WOMEN FOR SECURITY
PER LE SCUOLE
PROGETTO per le SCUOLE MEDIE e SUPERIORI

WOMEN for Security

CYBER-TIPS: GUIDA PER GLI INSEGNANTI

PER PARLARE DI CYBERSECURITY A SCUOLA

Sommario

1 Prefazione 7

2 Chi siamo 9

3 La cybersecurity 11

3.1 Definizione 11

3.2 Cenni di storia della sicurezza informatica 12

3.3 Dinamiche mutuate dal mondo reale 14

3.4 Categorie e ambiti della cybersecurity 15

3.5 Crescita dei dati e aumento della superficie di attacco e reati connessi 16

4 Il rischio informatico 19

4.1 Hacker o cybercrime S.p.A.? 21

4.2 Obiettivi e motivazioni 21

4.3 Attacchi 22

4.4 Anatomia e fasi di un attacco informatico 23

4.5 Cyberbullismo 31

4.6 Doxing 32

4.7 Sexstortion 32

4.8 Scheda didattica 1 - scuole di ogni ordine e grado 34

4.9 Scheda didattica 2 - scuole di ogni ordine e grado 35

4.10 Scheda didattica 3 - scuole di ogni ordine e grado 36

4.11 Scheda didattica 4 - scuole di ogni ordine e grado 37

5 Attacchi informatici 39

5.1 I principali tipi di attacchi informatici 41

5.2 Come possiamo proteggerci dagli attacchi informatici? 45

5.3 Scheda didattica - scuole secondarie di primo grado 48

6 Cyber Hygiene 49

6.1 Le misure di protezione 49

6.2 Gestione degli account e delle password 50

6.3 Ingegneria sociale 51

7 Condotte digitali e profili legali 55

7.1 Perché in rete, senso della legalità ed etica si attenuano? 55

7.2 Alcune condotte digitali che possono avere ripercussioni di tipo legale 56

8 La nostra impronta sul web 63
8.1 L'identità digitale 63
8.2 Web reputation (cosa gli altri pensano di noi) 64
8.3 Rischi 65
8.3.1 Furto identità digitale 65
8.3.2 Falsi profili 66
8.3.3 Come distinguere un profilo falso da uno vero 67
8.3.4 Come proteggere l'identità digitale 67
8.4 L'identità digitale degli altri 69
8.4.1 L'identità digitale è reale 69
8.5 Scheda didattica - scuole secondarie di primo grado 71
9 Comunicazione digitale 73
9.1 La Netiquette 73
9.2 Un linguaggio nuovo: il gergo di Internet 74
9.3 Strumenti di messaggistica 74
9.4 Parole_Ostili 75
9.5 WhatsApp 76
9.6 Gestione del tempo e relazioni personali 78
9.7 Regole condivise in famiglia 79
9.8 Scheda didattica (classi medie) 80
10 Disinformazione: non è vero, ma ci credo? 83
10.1 Cos'è una fake news? 83
10.2 Perché la disinformazione può diventare pericolosa? 84
10.3 Cosa serve nella lotta alle fake news? 85
10.4 Consigli utili per individuare una fake news 88
10.5 Cosa abbiamo capito? 89
10.6 Scheda didattica 1 - scuole di ogni ordine e grado 90
10.7 Scheda didattica 2 - scuole di ogni ordine e grado 91
10.8 Scheda didattica 3 - scuole di ogni ordine e grado 92
11 Gaming online: rischi e opportunità 93
11.1 Il linguaggio dei gamer 95
11.2 Il comportamento dei gamer 95
11.3 I rischi del gaming online 97
11.4 Come proteggersi 99

11.6 Cosa abbiamo capito 102
11.8 Scheda didattica - scuola secondaria di primo e secondo grado 105
12 Conclusioni 107
13 Approfondimenti 109

1 Prefazione

“Perché avevamo bisogno di una guida?”
“Perché bisogna parlare di cybersecurity a scuola?”

La **cybersecurity** è diventata un aspetto essenziale nella nostra vita quotidiana. Con l’aumento delle minacce informatiche e degli attacchi informatici, è fondamentale che le persone siano consapevoli dei rischi e sappiano come proteggere i propri dati e la propria privacy online.
In questo scenario in continua evoluzione, diventa prioritario fornire ai nostri ragazzi e alle nostre ragazze, gli strumenti necessari per utilizzare la tecnologia al meglio, sfruttandone le innumerevoli opportunità e proteggendosi dagli i rischi.
I/le giovani sono nativi/e digitali, con genitori ed educatori NON digitali: è l’equivalente di dare un’auto da corsa a un adolescente, senza spiegargli i rischi della velocità e il codice della strada.
Le conseguenze possono essere disastrose e terribili (come confermano dei tristi fatti della cronaca degli ultimi anni).

La Guida per insegnanti ai percorsi di cybersecurity nasce dall’esperienza fatta in alcune scuole italiane, da cui è risultato evidente che per garantire una certa continuità nel percorso di educazione al digitale e alla cybersecurity è necessaria la “complicità” di insegnanti e genitori.

I primi paragrafi sono comuni a tutti i percorsi.
Dopo una breve introduzione sulla Cybersecurity e qualche cenno di storia della sicurezza informatica, la guida si focalizza sulle fasi, sui principali tipi di attacchi informatici e sulle misure di protezione.
Non mancano i focus sui comportamenti digitali, i profili legali e i suggerimenti su come proteggere l’identità digitale.
Segue una panoramica sui maggiori sistemi di messaggistica istantanea, fino al delicato tema della Disinformazione e alcuni consigli utili per individuare una fake news.
Chiude la guida, il tema del Gaming online: rischi ed opportunità, il linguaggio dei gamer e il gaming online nella formazione scolastica.

Questo lavoro è frutto delle competenze, del tempo e della dedizione di alcune professioniste della cybersecurity: le nostre le Cyber Ladies che ringrazio, a nome di tutto il Comitato Direttivo.

Competenze, Condivisione e Crescita: da queste tre "C" nasce il progetto Women For Security che continuiamo a perseguire con la stessa passione sin dalla costituzione della community.
Noi continueremo ad impegnarci nella diffusione di una corretta cultura digitale con l'auspicio che le nuove generazioni abbiano tutte le informazioni necessarie per poter fare le scelte personali, professionali che sono sul campo, prive di divisioni di genere.
Stay tuned.

Cinzia Ercolano
Founder Women For Security

2 Chi siamo

Women For Security (WFS) è una community di professioniste che operano nel mondo della sicurezza informatica in Italia.
Nata nei primi mesi del 2020, WFS riunisce cyber lady con profili molto variegati: da ricercatrici e divulgatrici scientifiche a figure tecniche, da avvocati ed esperte di diritto dell'informatica a responsabili marketing e comunicazione, da profili di vendita a ruoli di country manager aziendali.

L'obiettivo primario di Women for Security è mettere a fattor comune le competenze delle professioniste della cybersecurity per fare squadra e crescere insieme. La community svolge inoltre attività di education e divulgazione sull'utilizzo sicuro del digitale, sensibilizzando su temi di attualità e favorendo un ruolo sempre più attivo della donna nella cyber società, abbracciando le discipline STEM per intraprendere una carriera in un settore in grande crescita.

La community è impegnata concretamente nell'organizzazione di eventi di formazione e aggiornamento per uno sviluppo professionale e personale, e in tavoli di lavoro su tematiche attinenti al mondo cyber.
Nel 2022 la community ha attivato un tavolo di lavoro dedicato alle scuole che mira a offrire agli Istituti che ne fanno richiesta un percorso di educazione all'uso sicuro del digitale, con particolare focalizzazione sugli aspetti della sicurezza informatica.

3 La cybersecurity

Alessia Valentini

Per conoscere la cybersecurity è necessario fornire una prima serie di definizioni formali e informazioni che consentano di comprendere il contesto digitale, alcune sue caratteristiche e soprattutto le motivazioni degli attaccanti, al fine di comprendere il rischio digitale per poi sapere come affrontarlo preventivamente.

3.1 Definizione

Il termine inglese "cybersecurity" (o Cyber Security), in italiano tradotto con sicurezza informatica, è l'insieme delle prassi, misure tecniche, tecnologie, processi e controlli per proteggere sistemi, reti, programmi, dispositivi e dati dagli attacchi informatici. La cybersecurity ha lo scopo di ridurre il rischio di attacchi informatici e proteggere dallo sfruttamento non autorizzato di sistemi, reti e tecnologie da parte di avversari (per lo più criminali) che vogliono sfruttare i dati sottratti a loro vantaggio.

Da un punto di vista tecnico digitale, la cybersecurity è la pratica di garantire la riservatezza, l'integrità e la disponibilità delle informazioni digitali, ovvero dei dati digitalizzati. Proteggere la **riservatezza** significa tutelare il grado di confidenzialità, preservare l'**integrità** significa garantire inalterabilità delle informazioni, mentre assicurare la **disponibilità** significa rendere fruibile l'informazione quando necessaria a chi ha diritto di accedervi. Globalmente queste tre caratteristiche sono indicate come la "**RID"** dei dati. È utile sapere che un dato digitale può avere anche la caratteristica di **autenticità** grazie alla quale è possibile verificare l'identità di chi ha dato origine all'informazione e il **non ripudio,** ovvero la qualità del dato di non poter essere ripudiato: chi lo ha creato non può negare di averlo fatto.

La cybersecurity è spesso confusa con la **sicurezza delle informazioni** che a sua volta è invece la **pratica** di proteggere i dati da qualsiasi forma di minaccia, indipendentemente dal fatto che sia analogica o digitale. La sicurezza delle informazioni è necessaria nel mondo analogico, e viene garantita da tutte quelle prassi che tutelano la RID delle informazioni su qualunque supporto esse siano: carta, microfiches, nastri, fotografie, video. Nel contesto digitale coincide con la cybersecurity perché la sicurezza delle informazioni si sovrappone alla protezione della RID digitale dei dati. Un esempio di sicurezza delle informazioni nel mondo analogico può essere la pratica di chiudere nei cassetti i documenti riservati senza lasciarli in giro sparsi o gli accorgimenti degli inchiostri speciali e la filigrana per evitare che certi documenti siano modificati.

La trasformazione digitale influenza la vita delle persone perché molti servizi e informazioni dipendono dai computer e da Internet: le comunicazioni (ad esempio e-mail, smartphone, tablet), l'intrattenimento (ad esempio videogiochi interattivi, social media, app), i trasporti (ad esempio sistemi di navigazione), gli acquisti (ad

esempio acquisti, carte di credito), le medicine (ad esempio attrezzature mediche, cartelle cliniche) e l'elenco potrebbe continuare. Quanto della vostra vita quotidiana utilizza la tecnologia? Quante delle vostre informazioni personali sono memorizzate sul computer, smartphone, tablet o sul sistema di qualcun altro? Questa impronta digitale (letteralmente digital footprint) è esattamente quello che vi caratterizza nel contesto digitale e che in una certa misura vi identifica. I criminali lo sanno, e puntano proprio a questo tipo di dati personali, sensibili, riservati. I dati nella loro forma digitale sono stati definiti il nuovo oro nero (petrolio) per i criminali perché attraverso il loro commercio nel "mercato nero" digitale (il dark web), lucrano e si finanziano. I dati digitali fanno gola anche ad avversari digitali motivati da attivismo e motivi geopolitici e in questo caso il vantaggio che deriva dal loro commercio può avere molteplici scopi per questo tipo di attaccanti.

3.2 Cenni di storia della sicurezza informatica

La sicurezza informatica e le minacce informatiche sono state costantemente presenti negli ultimi 60 anni di trasformazione digitale. Ma se negli anni '70 e '80, la sicurezza informatica era circoscritta al mondo accademico, dopo l'evoluzione di Internet e la maggiore connettività, si è assistito al progressivo decollo dei virus informatici e delle intrusioni di rete. Dopo la diffusione dei virus negli anni '90, gli anni 2000 hanno segnato la sistematizzazione delle campagne di attacco e la diffusione delle minacce informatiche, ma soprattutto si è assistito alla trasformazione degli attaccanti, dalla tipologia "LONE WOLF" (accezione inglese che caratterizzava il singolo esperto di sicurezza capace di attaccare interi sistemi da solo) alla tipologia criminalità organizzata, caratterizzata da gruppi di attacco con appartenenti suddivisi in specializzazioni multidisciplinari, budget consistenti e molto tempo da dedicare al crimine.

La storia delle minacce alla sicurezza informatica ha tenuto il passo con il progresso della tecnologia informatica e, senza conoscere la storia della sicurezza informatica, non è possibile comprenderne appieno l'importanza. Da quando i computer sono stati connessi a Internet e hanno iniziato a scambiarsi messaggi, il crimine informatico si è sostanzialmente evoluto e con esso la probabilità di rischio di essere attaccati, che è significativamente più alta oggi rispetto ad allora.

All'epoca dei primi computer, negli anni '40, solo piccoli gruppi di persone avevano accesso alle enormi macchine elettroniche e il rischio era inesistente. Tuttavia, il pioniere dei computer, John von Neumann, nel 1949, fu il primo a teorizzare programmi per computer capaci di comportamenti inattesi, il che di fatto fa da data di nascita della teoria alla base dei virus informatici, resa pubblica per la prima volta in quell'anno. A tutti gli effetti i primi incidenti possono risalire al phone phreaking, una tecnica degli anni '50 effettuata da coloro che avevano particolare interesse per il funzionamento dei telefoni, al fine di manomettere i protocolli, operare sulla rete da remoto e attuare chiamate gratuite evitando di pagare tariffe interurbane.

Gli anni '60 sono stati invece caratterizzati, per la maggior parte, da computer enormi, i mainframe, mantenuti in ambienti sicuri e a temperatura controllata. L'accesso era ancora limitato, tuttavia, la maggior parte dello sviluppo della parola "hacking" è avvenuta durante questo decennio. Infatti, in quegli anni, alcuni individui fecero irruzione in un set di treni ad alta tecnologia di proprietà del MIT Tech Model Railroad Club, perché desideravano modificare la loro funzionalità e questa idea fu poi trasferita ai computer. L'obiettivo di questi primi incidenti di hacking era solo quello di ottenere l'accesso ai sistemi. Tuttavia, non c'erano opportunità di guadagno politico o economico. I primi attacchi di hacking consistevano principalmente nel creare confusione per testare se fosse possibile modificare il funzionamento dei computer. Gli anni '70 in particolare hanno visto l'emersione di tecniche di hacking sempre più evolute, rapide ed efficaci grazie alle quali le case produttrici venivano a conoscenza delle vulnerabilità. Quindi, questo continuo binomio fra attacchi e correzioni permetteva di fortificare strumenti digitali, macchine e reti. È in questo periodo che si assiste alla nascita delle tecniche di difesa digitale e ai controlli di sicurezza informatica o strumenti deputati alla difesa delle reti e dei sistemi. Ma è sicuramente l'attacco alla ARPANET, l'antenata di Internet, l'inizio della storia attuale della cybersecurity: Bob Thomas, uno sviluppatore ARPANET, utilizzando PC connessi alla rete, aveva creato "I'm the creeper; catch me if you can!" ("Io sono il rampicante; prendimi se ci riesci!") il primo programma capace di passare da una macchina all'altra da solo. È possibile presumere che questo sia stato il primo worm informatico registrato nella storia della sicurezza informatica. Con gli anni '80 e l'estensione e diffusione dei virus, worm e trojan sono stati diffusi i programmi antivirus a difesa dei device, ma è solo con l'interconnessione globale degli anni '90 che la minaccia travalica frontiere e confini e si trasforma in una minaccia estesa. I virus diventano polimorfici (non sono più riconoscibili dagli antivirus), iniziano a distruggere porzioni di dischi e di dati e anche le misure di difesa si incrementano, introducendo connessioni protette con livelli di sicurezza, per impedire la diffusione dei dati in chiaro e l'intercettazione delle comunicazioni (nascono così i protocolli HyperText Transfer Protocol Secure- HTTPS, e Secure Sockets Layer- SSL).
Il carattere pandemico della minaccia digitale avviene a partire dal 2011, definito l'anno del security Breach per la grande quantità e gravità degli attacchi, e dalla trasformazione degli attaccanti in gruppi di criminalità organizzata. Ma da allora la scala di misura della qualità e gravità degli attacchi è stata modificata più volte per rendere i numeri confrontabili anno dopo anno a causa dell'incremento e persistenza degli attacchi digitali (si veda a tal proposito l'introduzione del Rapporto Clusit anno dopo anno dal 2011 a oggi).
Gli anni a cavallo del COVID e gli ultimi due, caratterizzati dal conflitto Russo-Ucraino, hanno ulteriormente aggravato il panorama della minaccia, che oggi ha superato per introiti qualsiasi altra attività illecita e criminale (compreso lo spaccio e la prostituzione, soliti mezzi di finanziamento illecito) nel contesto del Cybercrime,

ma di fatto il cyberspazio è diventato anche il luogo di scontro della contrapposizione geopolitica che a mezzo disinformazione e propaganda di fake news punta a destabilizzare o influenzare le correnti di pensiero della popolazione nelle varie culture. Il livello geopolitico della contrapposizione si sposta sulle culture diverse e mira alla affermazione di questo o quel gruppo politico per ogni nazione. Alcuni attacchi avvengono per destabilizzare la sicurezza, altri per spostare l'attenzione e attaccare altrove per guadagni finanziari, ma in generale si assiste sempre a dinamiche mutuate dal mondo reale. Cerchiamo quindi di capire come avviene questa trasformazione mutuata dal mondo reale ai contesti digitali.

3.3 Dinamiche mutuate dal mondo reale

Lo spazio digitale è un luogo spesso percepito in modo distorto da grandi e piccoli a causa dell'erronea percezione che quello che accade nell'universo digitale NON incida sul mondo analogico e nella nostra vita di tutti i giorni: ma è una percezione sbagliata. Infatti, diverse dinamiche del mondo reale sono state trasferite nel mondo digitale e quindi le attenzioni e le precauzioni tipiche del nostro day by day devono essere le stesse con cui affrontiamo gli spazi digitali: non parlare con gli sconosciuti, non accettare cose dagli sconosciuti (l'equivalente delle famose caramelle), non dare soldi a sconosciuti che si spacciano per conoscenze nostre o dei nostri familiari. Troppo spesso invece, complice l'intermediazione operata dai computer e dispositivi digitali smart, il criminale digitale mistifica la propria identità presentandosi in modo credibile e manipola o raggira la potenziale vittima. Nel mondo reale un truffatore si riconosce o almeno si impara a diffidare di lui, grazie ai racconti dei nonni e dei genitori, ma nei contesti digitali questa "esperienza" non viene trasferita (anche perché nonni e genitori non ce l'hanno) con il risultato che tutti più o meno sono vulnerabili alle truffe, cadono vittima di raggiri, o peggio di adescamenti digitali, di trappole che a vario titolo sfruttano le informazioni lasciate in modo incontrollato sui social, o sulle chat. Se sugli autobus e mezzi pubblici ci hanno insegnato che ci sono i borseggiatori e che quindi si deve fare attenzione alle borse e ai portafogli, lo stesso deve essere fatto quando si naviga in rete: occhio alle proprie password di accesso, occhio ai propri portafogli digitali, al conto in banca, alle operazioni creditizie o finanziarie e occhio soprattutto ai nuovi contatti che avvengono per le ragioni più disparate. Dubitate come fareste nella vita reale, perché il Digital Trust va bene, ovvero è positivo affidarsi alle nuove tecnologie che possono facilitare la vita, ma in questi contesti la guardia dovrebbe sempre essere mantenuta alta, per tutta quella serie di raggiri che dalla vita reale si sono spostati nel cyberspazio e da qui possono danneggiare sia i nostri luoghi digitali sia avere degli effetti dannosi nella vita reale e analogica.

Alcune prassi e misure di contrasto possono tuttavia aiutare nella prevenzione, esattamente come è avvenuto con il COVID. Durante la pandemia, infatti, abbiamo imparato a non contagiarci con tre misure preventive: l'uso delle mascherine, la

disinfezione delle mani e il metro di distanza. Le corrispondenti misure nel contesto digitale sono rispettivamente: navigare in modo anonimo per non lasciare traccia di navigazione (equivalente della mascherina), tenere puliti pc e device digitali da malware e quindi fare puntualmente gli aggiornamenti di sistema e installare un apposito software antivirus (equivalente della disinfezione delle mani) e come terza prassi tenere a distanza gli altri rispetto alla sfera della vostra privacy (equivalente del metro di distanza). Tutte le altre pratiche che troverete nel paragrafo della Cyberhygiene sono misure strettamente tecniche che implementano queste tre regole di base al fine di ridurre il rischio di essere oggetto e soggetto di attacco. Praticare queste buone regole significa saper proteggere la propria sfera personale digitale e significa soprattutto assumersi pienamente la responsabilità della protezione come parte della responsabilità di adottare nuove tecnologie. Questa responsabilizzazione è la stessa identica che nella vita analogica sosteniamo ogni volta che facciamo qualcosa di nuovo, ogni volta che affrontiamo una nuova sfida o progrediamo nel lavoro, nelle amicizie, negli affetti. Ogni passo della nostra crescita richiede di assumersi la responsabilità dei benefici e degli eventuali problemi che ne scaturiscono. Esattamente allo stesso modo, anche nei contesti digitali, adottare nuove tecnologie, device, app, social, dovrebbe comportare la medesima assunzione di responsabilità per le pratiche di sicurezza a propria tutela.

3.4 Categorie e ambiti della cybersecurity

Come visto nel paragrafo in cui si definisce cybersecurity, questo è un termine generale, ma per capire a cosa si applichi è necessario distinguere i diversi ambiti tecnologici in cui attuarla e saper comprendere le sue sottocategorie. La sicurezza informatica può essere quindi applicata a:

- Reti di dati e in questo caso si parla di NETWORK security
- Internet: WEB security
- Cloud: CLOUD Security
- Infrastrutture critiche: CRITICAL INFRASTRUCTURE PROTECTION
- Operation Technology (OT): OT security
- IoT (Internet of Things): IoT security
- Smartphone: MOBILE Security
- Ambienti di lavoro smart: SMART WORKING security
- Edge computing: EDGE security
- Applicazioni e programmi: APPLICATION Security

Sono poi importanti i concetti di AWARENESS E INFOSHARING che supportano la diffusione di prassi e misure di sicurezza per diffondere la consapevolezza e la diffusione della cultura alla sicurezza fra gli individui grandi e piccoli, in tutti i contesti e ambienti sociali, nelle famiglie, nei contesti lavorativi.

3.5 Crescita dei dati e aumento della superficie di attacco e reati connessi

La pervasività della trasformazione digitale ha generato un numero di dati digitalizzati con una progressione impressionante e non paragonabile ad altri fenomeni di innovazione. Questa crescita esponenziale delle tecnologie e l'adozione incontrollata e non pianificata di apparati hardware e software, app mobile, social media, infrastrutture in Cloud, strumenti IoT, ha generato foreste di tecnologie non sempre adeguatamente protette che, a loro volta, hanno attratto i criminali, consci del valore dei dati personali, sensibili, particolari e di proprietà intellettuale (spesso paragonato al nuovo oro nero digitale), per il commercio clandestino che porta loro lucro e ricchezza. Il crimine si è talmente orientato su questo tipo di reato, che il cybercrime come mezzo di finanziamento illecito sta uguagliando se non superando gli introiti da sfruttamento della prostituzione e spaccio di droghe (Fonte: bizjournals).
Anno dopo anno dal 2011 si è assistito a un incremento smisurato degli attacchi e la conta dei danni ha raggiunto proporzioni da piaga biblica. Secondo il report del Clusit 2023, lo scorso anno il numero di incidenti rilevati è cresciuto significativamente arrivando a un aumento del 527%. Tra quelli avvenuti In Italia, la categoria "Cybercrime" rappresenta il 93% del totale, +11% rispetto al resto del mondo (dove la percentuale è pari all'82%). Seguono con il 7% gli incidenti classificati come "attivismo"[1], mentre non rilevano in modo significativo gli attacchi nelle categorie "spionaggio/ sabotaggio" o "guerra dell'informazione".
Negli ultimi cinque anni la situazione è peggiorata nettamente, seguendo un trend pressoché costante. Confrontando i numeri del 2018 con quelli del 2022, la crescita del numero di attacchi rilevati è stata del 60% (da 1.554 a 2.489). Nel 2020 con il periodo del COVID la superficie di attacco[2] è repentinamente aumentata aggiungendo perimetri cloud e di smart working che hanno subìto attacchi specifici. Nel 2022 si è aggiunto il conflitto tra Russia e Ucraina, che ha peggiorato un panorama degli attacchi già gravoso. La ricerca 2022 dell'Osservatorio cybersecurity e Data Protection del Politecnico di Milano ha anche fatto emergere come il 67% delle grandi imprese abbia subito un aumento dei tentativi di attacco rispetto all'anno precedente e come il 14% delle grandi imprese abbia subito attacchi con conseguenze concrete. Oltre ai danni crescenti causati dal cybercrime e dalle "normali" attività di intelligence che osserviamo da anni, dal 2022 siamo entrati in una nuova fase di "guerra cibernetica diffusa", nel contesto di crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa. La relazione annuale del DIS sulla minaccia, che negli ultimi anni include anche la minaccia da parte di avversari digitali, ha fotografato gli obiettivi

---

1 Hacktivism (in italiano attivismo) è un termine che deriva dall'unione delle parole hacking e activism e indica una tipologia di attacchi informatici volti a sensibilizzare su temi sociali, etici, sui diritti civili e/o protestare contro chi non li rispetta o non li fa rispettare (https://it.wikipedia.org/wiki/Hacktivism)

2 L'insieme di tutti gli elementi digitali che possono essere attaccati.

delle operazioni cibernetiche condotte a danno del nostro Paese evidenziando come siano state coinvolte diverse tipologie di soggetti pubblici e privati, per mano sia di attori finanziati da stati, che di organizzazioni criminali e hacktivisti. Sono state impiegate svariate tecniche d'attacco, tra cui software e script malevoli, e perseguite diverse finalità, tra cui lo spionaggio, il ritorno economico e il discredito dei target. In particolare, è stato rilevato un significativo incremento delle azioni a danno di obiettivi privati e un aumento dell'impiego di malware, inclusi i ransomware e, in concomitanza con l'invasione russa dell'Ucraina, sono stati osservati ancora nuovi trend di attacco. (Fonte: Rapporto annuale intelligence italiana- 2023).
Ogni anno sono pubblicati studi e approfondimenti sul panorama della minaccia digitale da parte del CLUSIT, dell'Agenzia per la sicurezza Europea, del Dipartimento per le informazioni della Repubblica (DIS), per informare, rendere noti e preparare alla difesa tutti coloro che a vario titolo possano essere coinvolti da questi attacchi. Aziende PMI e Corporate ma anche le organizzazioni pubbliche e le istituzioni possono rientrare nel mirino degli avversari digitali che, in veste di criminali, attivisti o gruppi pagati da Stati, possono creare danni significativi ai sistemi informatici e alle reti di dati che li collegano alla Rete.

Un significativo elenco di minacce digitali è stato pubblicato dal Consiglio europeo nel 2022 unitamente a uno studio sulle minacce del 2022 dell'ENISA, ma l'ENISA aveva già iniziato ad analizzare il panorama delle minacce fra il 2019 e il 2020 pubblicando un documento in proposito.

4 Il rischio informatico

Stefania Iannelli

In sicurezza informatica, o cybersecurity, il rischio informatico è la probabilità che si verifichino eventi indesiderati o comportamenti illeciti moltiplicata per il danno generato, a cui viene assegnato un valore convenzionale in una scala da un minimo a un massimo.

Ad esempio da 1 a 4:
Probabilità:

1. Improbabile
2. Poco Probabile
3. Probabile
4. Altamente probabile

Gravità del danno:

1. Lieve
2. Medio
3. Grave
4. Gravissimo

Normalmente con tale termine ci si riferisce alla possibilità che malintenzionati possano sfruttare vulnerabilità e falle presenti nei sistemi informatici portando a conseguenze quali furto di dati, danno economico, interruzione delle attività o altro, compromettendo riservatezza, integrità e disponibilità dei dati.
Un paradigma, questo, denominato RID (Riservatezza, Integrità e Disponibilità) attorno a cui ruotano tutti i concetti legati alla sicurezza informatica.
La mancanza o la manomissione di uno di questi fattori può comportare una violazione con successivo danno/impatto. Per esemplificare, possiamo quindi considerare un incidente informatico:

- un dato che dovrebbe rimanere privato, reso pubblico;
- un dato modificato senza autorizzazione;
- un dato perso, e non più recuperabile.

Semplificando, si può calcolare il rischio usando la seguente formula con i valori esemplificati prima:

$$Rischio = Probabilità \times Impatto$$
$$R = PxI$$

La probabilità è la possibilità che si verifichi l'evento, mentre l'impatto è la conseguenza negativa derivante, la mole del danno.

Il rischio informatico riguarda tutte le persone che utilizzano dispositivi connessi a internet quali ad esempio smartphone, tablet, computer, IoT – Internet of Things (tra cui SmartTV, telecamere, elettrodomestici smart) e l'impatto può essere devastante non solo a livello economico ma anche mentale, arrivando a provocare ansia, depressione e pensieri suicidi.
È stato stimato che ogni giorno circa un milione di persone in più si collega a internet, che nel 2022 circa sei miliardi di persone erano connesse e che nel 2030 il 90% della popolazione umana di età pari o superiore ai sei anni sarà connessa.
Con il crescere dell'informatizzazione, della connettività persistente e dei progressi tecnologici, le minacce informatiche sono aumentate e continuano ad aumentare di anno in anno, evolvendosi per sfruttare queste tendenze a vantaggio degli attaccanti.
Volendo dare alcuni numeri che includono fatti e previsioni sul cybercrime, Cybersecurity Ventures ha pubblicato degli studi secondo i quali nel 2021 ogni 11 secondi un'azienda è stata vittima di un attacco ransomware, rispetto a una ogni 14 secondi nel 2019.
La previsione è che la frequenza degli attacchi ransomware contro Governi, aziende e persone continuerà ad aumentare fino a raggiungere una media di uno ogni 2 secondi nel 2031.
Un'altra previsione è che il costo del cybercrime nel mondo arriverà a 10.5 trilioni di dollari nel 2025.
Sono numeri impressionanti, e se il crimine informatico fosse paragonato a uno Stato, sarebbe la terza economia mondiale dopo Stati Uniti e Cina.
Così il cybercrime è entrato a far parte della lista dei 10 maggiori rischi mondiali per i prossimi 10 anni stilata dal World Economic Forum.
Diventa perciò fondamentale, per tutti, migliorare la comprensione dei rischi e delle minacce che ci si può trovare ad affrontare ogni giorno.
Questo vale in particolare per chi interagisce professionalmente con bambini e adolescenti che sono nati nell'era digitale e che hanno molta più familiarità con il mondo di internet e delle app rispetto agli adulti.
È quindi essenziale conoscere i rischi legati al mondo online, in modo da poter essere d'aiuto e rappresentare un punto di riferimento.
Esattamente come avviene nel mondo "reale", anche per il mondo digitale, i ragazzi vanno istruiti sui possibili pericoli che si nascondono in internet e nelle applicazioni che sono diventate parte della loro quotidianità (dalla scuola al tempo libero), evidenziando come, se è pur vero che ciò che avviene in un mondo virtuale non è reale, questo però può condizionare in maniera grave e significativa la vita reale; infatti nel mondo virtuale si trovano pericoli anche più insidiosi, perché più difficili da riconoscere.
Analizziamo ora questi pericoli, descrivendo chi sono gli attaccanti, quali sono le loro motivazioni, come avvengono gli attacchi e quali sono le conseguenze.

4.1 Hacker o cybercrime S.p.A.?

Nell'immaginario collettivo l'hacker è una persona solitaria, che vive davanti al computer, molto intelligente e abile sia nella programmazione che nella violazione di qualsiasi sistema informatico.
L'hacker può utilizzare le sue conoscenze per evidenziare le lacune legate alla sicurezza di aziende o Stati, per poi diffondere una maggiore consapevolezza oppure per intenti criminali.
Cinema e televisione hanno contribuito alla diffusione di questa immagine, un po' romantica (per esempio Matrix, Wargames, Mr. Robot), ma ad oggi questo tipo di figura non esiste più e sicuramente non è a loro che si riferiscono gli studi e le previsioni presentati in precedenza.

Immagini prese da internet che raffigurano gli hacker secondo l'immaginario collettivo.

In realtà sono gli "hacker" stessi che spesso si definiscono come uomini/donne d'affari, vantandosi di svolgere un servizio prezioso e curando la loro reputazione. Sono organizzati come piccole o grandi aziende e sono professionisti che si riuniscono portando ognuno le proprie capacità e ricoprendo ciascuno un ruolo specifico.
Le attitudini degli appartenenti a questi gruppi, che vengono anche definiti cyber gang, sono diverse e possono anche non essere legate a conoscenze informatiche.
Per esempio, nel caso di estorsioni via ransomware[3], ci sono specialisti delle negoziazioni, addetti al supporto, al riciclaggio del denaro estorto, e così via.
Queste persone lavorano insieme perseguendo lo stesso obiettivo.
Ovviamente, il fatto che si atteggino o pensino di essere lavoratori rispettabili non significa che non siano criminali, quali invece sono.

4.2 Obiettivi e motivazioni

Vediamo quali sono gli obiettivi e le motivazioni che muovono gli attaccanti, suddividendoli in quattro macrocategorie:

- **Cybercrime:** la motivazione principale è il guadagno economico;

[3] Il ransomware è un programma malevolo che oltre ad infettare un dispositivo, impedisce l'accesso ai dati al legittimo proprietario e chiede anche un riscatto, in cambio di dati sottratti e/o della decifratura del dispositivo infettato.

- **Cyber Spionaggio:** la motivazione in questo caso è legata al furto di segreti industriali, proprietà intellettuali, informazioni governative confidenziali;
- **Attivismo e Cyber terrorismo:** intimidazione per ragioni ideologiche, politiche, religiose o patriottiche;
- **Cyber Warfare:** l'utilizzo di attacchi informatici contro Stati nemici.

Queste motivazioni non sono mutuamente esclusive, infatti gli attaccanti possono far parte di un gruppo con una determinata finalità ma allo stesso tempo partecipare anche ad altre gang, oppure un gruppo può lavorare su diversi progetti, in base alla convenienza.
Ad esempio, un gruppo ransomware è spesso motivato da un guadagno economico ma a volte può anche agire sotto la guida di uno Stato aggiungendo così motivazioni più complesse.
A oggi la finalità principale è il cybercrime, anche se sono aumentati gli attacchi di tipo cyber warfare da quando la Russia ha invaso l'Ucraina.

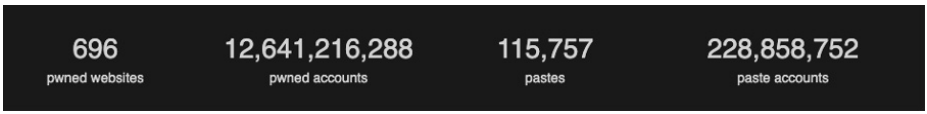
4.3 Attacchi

Come riportato, gli attacchi informatici continuano ad aumentare sempre di più diventando un fattore di preoccupazione mondiale.
Di seguito alcune delle violazioni più grandi e peggiori degli ultimi anni:

- **Yahoo**, agosto 2013 - Impatto: 3 miliardi di account. Questo è ancora ad oggi uno dei più grandi e noti incidenti informatici. Nonostante la violazione fosse avvenuta nel 2013, l'attacco è stato scoperto 3 anni dopo, nel 2016. È stato un attacco di tipo ATP (attacco di tipo avanzato e persistente) nel quale gli attaccanti sono riusciti a rubare informazioni sensibili, tra cui nomi, indirizzi e-mail, numeri di telefono, date di nascita e domande di sicurezza con relative risposte. Non sono note le finalità dell'attacco né i responsabili.
- **Aadhaar** (legato ad Alibaba), gennaio 2018 - Impatto: rivelate informazioni sull'identità/biometriche di 1,1 miliardi di cittadini indiani.
- **LinkedIn**, giugno 2021 - Impatto: 700 milioni di utenti.
- **Sina Weibo** (una delle maggiori piattaforme social cinese), marzo 2020 – Impatto 538 milioni di account.
- **Facebook**, aprile 2019 – Impatto 533 milioni di utenti. A causa di una vulnerabilità su API usate da Facebook e da Instagram alcuni sviluppatori di app di terze parti avevano avuto accesso non autorizzato a dati personali di utenti per cui è stato possibile esfiltrare e pubblicare dati sensibili degli utenti, tra cui numeri di telefono, ID, nomi, date di nascita, foto del profilo. Anche in questo caso l'accesso non autorizzato è avvenuto diversi mesi prima di venire scoperto.
- **SuperVPN, GeckoVPN e ChatVPN -** 2022 – Impatto 21 milioni di utenti. Una violazione che ha coinvolto diversi servizi VPN Android ampiamente utilizzati.

- **Twitter** – 2022 - Impatto 200 milioni di account. Gli indirizzi e-mail di più di 200 milioni di account Twitter sono stati pubblicati su un forum hacker includendo indirizzi e-mail, nomi, numero di follower, data di creazione.

Tutti i dati sottratti in questi e molti altri attacchi possono venire utilizzati per altri scopi criminali quali social engineering, doxing, furto di identità, tutti temi che tratteremo più avanti.
Basta fare una verifica sul sito haveibeenpwned.com, un sito web che permette di verificare se i propri dati personali sono stati rubati a seguito di una violazione, per capire l'entità del problema.



Verifica del furto dei propri dati

4.4 Anatomia e fasi di un attacco informatico

Per capire come avviene un attacco informatico dobbiamo comprenderne le varie fasi. Per descrivere queste fasi e le tecniche e tattiche usate dagli attaccanti, si utilizza spesso una terminologia militare.

Di solito vengono presi in considerazione diversi modelli, a seconda degli scopi. Qui utilizzeremo la Cyber Kill Chain che descrive gli stadi di un cyber attacco.
Lockheed Martin, una società internazionale di sicurezza e aerospaziale, è stata la prima a definire la "Cyber Kill Chain" per aiutare le aziende a comprendere meglio gli stage di un attacco informatico e creare difese contro di esso.

Le principali fasi di un attacco informatico descritte sono 7 (essendo un modello esemplificativo, un attacco non segue per forza sequenzialmente queste fasi ma una fase può essere ripetuta più volte, alcune fasi essere saltate):

1. **Ricognizione** (ricerca, identificazione e selezione del target). Questa fase si riferisce a quel momento di preparazione e strategia in cui un cybercriminale raccoglie quante più informazioni possibili sull'obiettivo prima di attaccare. Le tecniche di ricognizione possono essere categorizzate generalmente in ricognizione diretta e indiretta.
   a. **Indiretta.** Viene effettuata tramite ricerche avanzate sui motori di ricerca per trovare informazioni sensibili rimaste indicizzate oppure pubblicate sui social network, comprese le password rubate.
      Nelle violazioni di sistemi che avvengono quasi quotidianamente si hanno

spesso furti di account, informazioni personali che possono essere vendute e riutilizzate in altri attacchi.
Se gli utenti impiegano sempre le stesse credenziali per accedere a siti o app diverse, ecco che gli attaccanti possono avere accesso a più piattaforme.
Inoltre, è facile che le persone, specialmente i più giovani, condividano molte informazioni personali sui social media. Queste informazioni possono sembrare innocue, magari alcune vengono condivise rispondendo a sondaggi o partecipando a giochi proposti sui social, ma spesso di innocuo c'è ben poco.
Infatti, tanti giochi, sondaggi, quiz vengono creati per raccogliere informazioni sulle persone come ad esempio il colore preferito, il nome della via in cui si è cresciuti, il nome del proprio animale, e così via. Queste sono poi le informazioni che vengono richieste come domande di sicurezza per accedere agli account quando non si ha la password.
Un altro metodo di ricognizione è quello di cercare dispositivi esposti su internet e vulnerabili (webcam, router, ecc.). Questi dispositivi spesso dispongono di livelli di sicurezza inadeguati, non vengono aggiornati e possono diventare uno dei punti di accesso degli attaccanti.

b. **Diretta**. Viene fatta attivamente una scansione sulla rete alla ricerca di servizi esposti, vulnerabilità, password deboli del WiFi e così via. Questa tecnica porta spesso a ottenere informazioni più puntuali, e quindi più utili per un attacco, ma allo stesso tempo è più rumorosa e potrebbe attirare l'attenzione del target.

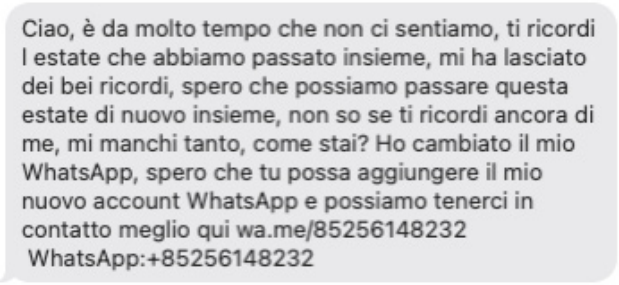
2. **Weaponization:** in questa fase l'attaccante decide come tentare l'attacco in base ai risultati della fase precedente (si arma e decide come agire).

3. **Delivery:** Nella fase tre avviene la consegna, cioè la trasmissione del malware. Per consegnarlo l'attaccante si serve di vettori di infezioni tra cui, il più utilizzato è il phishing nelle sue varie declinazioni. Perciò, prima di elencare i diversi vettori vediamo cosa si intende per phishing.
Il **phishing** è una forma di attacco informatico atta a ingannare le persone. Gli attaccanti impersonano organizzazioni legittime (la banca, il corriere da cui si aspetta un pacco, Amazon, Apple, Instagram o altri) o persone fidate (un amico, un conoscente, un collega, ecc.) con lo scopo di ottenere informazioni sensibili quali password, codici di accesso, dati finanziari, dati personali o di far installare alla vittima un malware (un programma malevolo).
La truffa può arrivare in diversi modi: via email, SMS, App, instant messenger o tramite una telefonata.
Oltre a ingannare la vittima il phishing spesso sfrutta altri aspetti emozionali dell'animo umano quali ad esempio paura o eccitazione.

Una delle caratteristiche comuni dei messaggi di phishing è l'urgenza dell'azione richiesta (se non si fa una determinata azione in risposta al messaggio ricevuto succederà qualcosa).
La fretta comunicata tramite questi messaggi sfrutta la psicologia umana cercando di indurre la persona ad agire impulsivamente senza fermarsi a riflettere. I cyber criminali sfruttano la paura, l'ansia, la preoccupazione per spingere le persone ad agire immediatamente (ad esempio impersonando la banca possono scrivere che la carta di credito verrà bloccata immediatamente se non si clicca sul link riportato e non si compilano le informazioni richieste, oppure che l'account Facebook, Instagram verrà sospeso se non si condividono i dati necessari). Questo tipo di pressione mira a ridurre la parte razionale facendo prevalere quella irrazionale con un'azione impulsiva (devo agire subito!).
Un'altra caratteristica tipica è la comunicazione di una vincita.
In questo caso gli attaccanti comunicano alla vittima una presunta vincita (denaro, premio, vacanza o altro). La manipolazione emotiva dietro questo tipo di messaggi può essere ancora una volta la fretta (se non si fa subito quello che viene richiesto la vincita scade) unita all'entusiasmo e all'emozione provati per aver vinto qualcosa.
Lo scopo è sempre lo stesso: ottenere informazioni, dati sensibili da condividere per ricevere quanto promesso (data di nascita, indirizzo, numero di telefono, informazioni bancarie su cui depositare i soldi vinti) oppure soldi (finte spese amministrative o tasse per ricevere il premio).
Ma tramite phishing i criminali informatici non prendono solo informazioni; questi messaggi possono contenere link a programmi malevoli che infettano il computer o il dispositivo dell'utente.
Per questo, nella Cyber Kill Chain il phishing rientra nella fase 4, cioè la consegna del malware che potrà infettare il dispositivo.

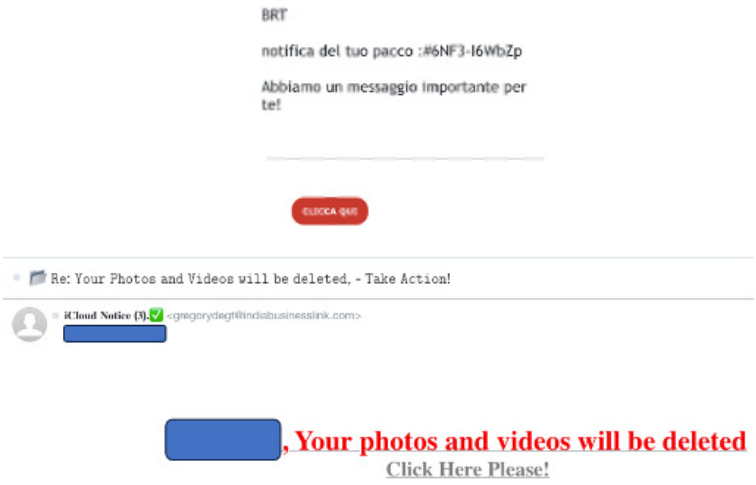
La consegna del malware viene spesso effettuata tramite:
- e-mail di phishing;
- smishing - link malevoli consegnati tramite SMS, instant messenger come WhatsApp, messaggi sui Social Network, sulle app, sui giochi online, sui forum;
- vishing - phishing effettuato tramite chiamate vocali;
- sfruttando le vulnerabilità sui dispositivi quali telefonini, tablet, PC, Mac, Smart Device (SamartTV, Telecamere, router Internet, ecc.);
- utilizzando credenziali rubate nella fase di ricognizione.

Di seguito alcuni esempi di smishing e phishing:



Esempio di smishing a carattere emotivo

Come si può vedere, in questo esempio l'attaccante tenta di sfruttare un fattore emotivo, quale l'amicizia, l'affetto, fingendosi qualcuno conosciuto dalla vittima e tentando di indurla a cliccare sul link riportato (cliccandoci si potrebbe scaricare un programma malevolo mettendo a rischio la sicurezza del telefonino e dei dati contenuti in esso). Oppure, la vittima potrebbe rispondere al messaggio per cercare di capire chi è l'interlocutore (il messaggio non è volutamente firmato per indurre il destinatario a rispondere) cadendo così nella seconda parte della trappola e instaurando un rapporto con i truffatori, che facilmente si evolverà con il tentativo di ottenere la fiducia della vittima o sfruttarne l'ingenuità e ricavarne qualcosa.

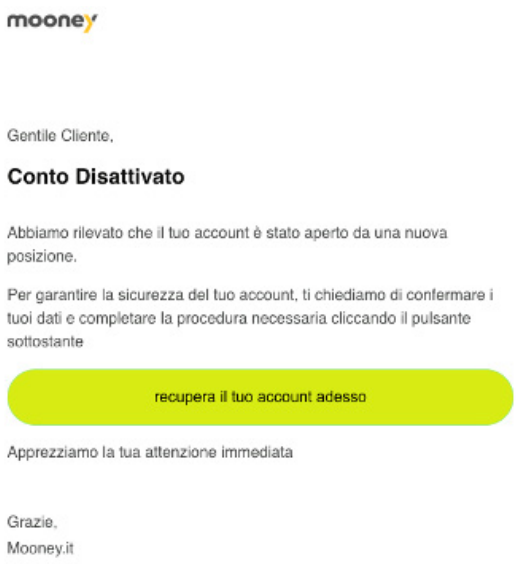


Esempio di smishing con carattere di urgenza

In questi due messaggi è molto chiaro il carattere di urgenza inserito dagli attaccanti: “messaggio importante”, “le tue foto e video verranno cancellati”, gli attaccanti hanno studiato i messaggi per mettere pressione alla vittima in modo che clicchi subito sul link senza riflettere.

Esempio di smishing di vincita

Qui un esempio di phishing della vincita. Come analizzato in precedenza, l’attaccante cerca di convincere il destinatario di aver vinto un premio cercando di sfruttare l’emozione della sorpresa inaspettata, seguita dalla fretta: “reclamalo prima che finisca” e inducendolo a cliccare subito sul link.



mooney

Gentile Cliente,

Conto Disattivato

Abbiamo rilevato che il tuo account è stato aperto da una nuova posizione.

Per garantire la sicurezza del tuo account, ti chiediamo di confermare i tuoi dati e completare la procedura necessaria cliccando il pulsante sottostante

recupera il tuo account adesso

Apprezziamo la tua attenzione immediata

Grazie,
Mooney.it

Esempio di smishing con carattere di ansia e allarme

Un altro esempio di mittente considerato legittimo con un contenuto che genera ansia e preoccupazione "il tuo account è stato aperto da una nuova posizione" e che spinge la vittima ad agire subito: "per garantire la sicurezza del tuo account" "recupera il tuo account adesso".
Fino a poco tempo fa, un messaggio di phishing poteva essere individuato (anche) perché presentava errori grammaticali grossolani o frasi troppo lunghe o non corrette, dato che spesso gli attaccanti non conoscono la lingua in cui stanno scrivendo (vedere l'esempio della vincita LIDL sopra riportato in cui è presente un errore grammaticale: "hai appena vinto **un grande sorpresa**").
Oggi, con il proliferare di strumenti di Generative AI, gli attaccanti si possono avvalere dell'intelligenza artificiale per creare messaggi di adescamento in qualsiasi lingua sempre più corretti semanticamente e grammaticalmente, rendendo difficile anche all'utente più attento la distinzione tra un messaggio legittimo e uno illegittimo.

La Generative AI o intelligenza artificiale generativa, tra cui la più nota è ChatGPT, è un tipo di tecnologia che utilizza algoritmi informatici per "generare" contenuti nuovi e originali, come immagini, video, musica o testo. L'intelligenza artificiale generativa viene istruita tramite grandi quantità di contenuti, che analizza per comprendere modelli, stili, relazioni e caratteristiche uniche all'interno dei dati.

Una volta che ha imparato, può iniziare a creare nuove cose da sola.
È uno strumento "neutro" e potente che può essere utilizzato per scopi nobili aprendo possibilità nuove in diversi campi ma è anche utilizzato dai criminali informatici.

4. 5. 6. **Exploitation, Installazione, Command and Control:** queste sono le fasi in cui l'attaccante sfrutta una vulnerabilità del sistema, installa il software malevolo e gestisce da remoto il dispositivo che ha violato.

Vale la pena spiegare brevemente cos'è una vulnerabilità e cos'è un exploit:

- **Vulnerabilità**: in sicurezza informatica, una vulnerabilità è una debolezza che riduce la sicurezza delle informazioni di un sistema e consente a un utente malintenzionato di accedervi.
  Una vulnerabilità potrebbe coincidere con un bug (un errore nel sistema), cioè un errore fatto non intenzionalmente dai programmatori nel codice che hanno scritto per creare il programma che si sta utilizzando.
  Tutte le app e i programmi che utilizziamo sono stati scritti da programmatori che si avvalgono di linguaggi appositi che vengono poi compresi dai sistemi su cui l'app viene eseguita (telefonini, computer, tablet, etc.).
  Nello scrivere un programma però si possono commettere degli errori che sfuggono alla revisione che di solito viene fatta prima di rilasciare un'applicazione o un sistema operativo (per esempio iOS, MacOS, Windows); per questo motivo vengono rilasciati gli aggiornamenti delle applicazioni e dei sistemi operativi, per correggere gli errori man mano che vengono trovati.
  Questi errori di programmazione vengono chiamati "bug". Non tutti i bug però implicano problemi di sicurezza e coincidono quindi con una vulnerabilità, infatti il bug di sicurezza è un concetto più ristretto.
  Quando un errore nella programmazione pregiudica la sicurezza del programma che si sta usando, siamo di fronte a un bug di sicurezza che può venire sfruttato dai criminali informatici.
  Le vulnerabilità però non sono solo bug di sicurezza nei programmi: possono anche essere hardware. In questo caso il difetto sarà sul dispositivo fisico o su una componente di esso (per esempio la memoria) oppure possono essere vulnerabilità legate all'agire umano (vedere paragrafo sul phishing).

- **Exploit**: dal verbo inglese sfruttare, che significa "usare qualcosa a proprio vantaggio": è un pezzo di software, un blocco di dati o una sequenza di comandi che sfrutta un bug (o una vulnerabilità) per causare eventi imprevisti o un comportamento imprevisto sul computer, sull'hardware o su qualcosa di elettronico (di solito computerizzato).

Per sintetizzare e riassumere le fasi di un attacco informatico sopra descritte: all'inizio i cyber criminali cercano informazioni, poi creano strumenti dannosi, li consegnano alle vittime spesso tramite l'inganno, arrivando in seguito a sfruttare delle vulnerabilità con il risultato di ottenere l'accesso al dispositivo della vittima, per controllarlo da remoto e ottenere privilegi di accesso anche a programmi o informazioni presenti su di esso .

7. **Azione sugli obiettivi:** in questa fase gli attaccanti portano a termine l'azione e concludono raggiungendo l'obiettivo che si erano prefissati (vedere le motivazioni riportate in precedenza).
   Alcuni esempi possono essere: esfiltrazione di dati, cifratura dei dati o del dispositivo con conseguente richiesta di soldi per sbloccarlo (ransomware), ricatti legati al furto di foto con la minaccia di diffonderle se non verranno inviate altre foto compromettenti (Sextortion), furto di carte di credito e così via.

Il **social engineering** merita una menzione a parte visto che può essere utilizzato in tutte le fasi della Cyber Kill Chain con scopi diversi.
Per social engineering si intende una tecnica utilizzata per manipolare o ingannare le persone in modo da ottenere informazioni riservate e accesso ai sistemi.
Non si avvale esclusivamente di capacità tecniche, ma anche psicologiche: sfruttando l'inganno l'attaccante raggira la vittima per ottenere il suo scopo.
Ad esempio, il phishing, vishing, smishing rientrano nel social engineering perché raggirano la persona solitamente con l'obiettivo di farle cliccare un link con contenuto malevolo.

Al termine di questa analisi sugli attacchi informatici va evidenziato che il malware, nello specifico il ransomware, è, ad oggi, la minaccia più diffusa.
L'industria del ransomware è un'industria multimiliardaria, composta da diversi gruppi che hanno come target aziende e persone.

Molto dipende dai soldi richiesti durante l'estorsione: se il target sono delle persone probabilmente ci sarà un numero maggiore di vittime con una richiesta di riscatto più bassa, in modo che possa essere evasa; al contrario se il target sono aziende, il riscatto richiesto sarà molto più oneroso ma il numero delle vittime minore.

Bambini e teenager possono essere target, come gli adulti, degli attacchi analizzati con finalità legate al furto di carte di credito, di dati sensibili, alla richiesta di soldi per un riscatto, ecc., ma possono anche essere vittime di abusi online tra cui:

- Cyberbullismo
- Cyberstalking

- Doxing
- Sextortion.

4.5 Cyberbullismo

Si tratta di un comportamento aggressivo e dannoso che coinvolge l'uso di tecnologie digitali per molestare, minacciare, intimidire o danneggiare emotivamente un individuo o un gruppo di persone. Comportamento che viene ripetuto nel tempo.
Parliamo, in pratica, della trasposizione dal mondo reale a quello virtuale del bullismo tradizionale con in più un'amplificazione legata al contesto (possibilità di diffusione maggiore), in cui gli aggressori possono nascondersi dietro l'anonimato e raggiungere un pubblico più vasto.

Il cyberbullismo può essere perpetrato da criminali informatici o da singoli individui. I criminali informatici utilizzano tattiche come l'invio di minacce o messaggi offensivi attraverso social network, mail, chat, sms, forum online, siti di giochi e qualsiasi tipo di social media, diffusione di informazioni dannose o false, creazione di siti web o profili falsi per diffamare le vittime, o sfruttamento di vulnerabilità informatiche per danneggiare i sistemi o rubare dati personali delle vittime.

È importante sottolineare che il cyberbullismo non è limitato ai criminali professionisti, ma può venire perpetrato da adulti o ragazzi con normali abilità informatiche che spesso conoscono la vittima. Tuttavia, le possibilità tecniche dei criminali informatici consentono loro di nascondere l'identità e sfuggire alle conseguenze legali, rendendo il loro comportamento ancora più dannoso e difficile da affrontare.
Secondo una ricerca rilasciata nel 2020 da Cyberbullying Research Center and Cartoon Network il 21% di giovani di età compresa tra i 9 e i 12 anni è stato vittima o testimone di cyberbullismo.

Alcune tattiche del cyberbullismo comprendono:

- insulti e offese online via social media, messaggi istantanei, forum e altri strumenti di comunicazione digitale;
- minacce e intimidazioni;
- diffamazione: possono venire diffuse informazioni false o dannose sulle vittime;
- divulgazione di informazioni personali: gli aggressori possono condividere informazioni private o immagini personali della vittima;
- incoraggiamento nell'intraprendere azioni autolesioniste: possono spingere la vittima a ferirsi o uccidersi;
- masquerade: i cyberbulli possono rubare l'identità della vittima con lo scopo di pubblicare a suo nome contenuti di ogni tipo.

Il cyberbullismo può portare a gravi conseguenze per chi lo subisce, tra cui problemi di salute mentale, ansia, depressione, isolamento sociale, ridotta autostima, problemi scolastici e, in alcuni casi, anche il suicidio.
Anche nel caso del cyberbullismo gli attaccanti iniziano ad avvalersi della Generative AI come vettore per perpetrare molestie e danni.
Grazie all'uso dell'intelligenza artificiale i cyberbulli possono creare automaticamente messaggi, e-mail, post o commenti molesti e minacciosi su un'ampia varietà di piattaforme agevolandone una diffusione più veloce grazie all'automazione, amplificando notevolmente l'impatto delle molestie, e arrivando a sopraffare le vittime.

4.6 Doxing

Un'altra forma di comportamento dannoso e abuso online è rappresentata dal doxing (o doxxing), abbreviazione di "dropping documents" o "document tracing".
Con questo metodo di attacco l'aggressore (singolo o gruppo) cerca e divulga informazioni personali e private di un'altra persona, spesso con l'intento di danneggiarne la reputazione o esercitare pressioni su di essa. Queste informazioni possono includere dettagli come il nome completo, l'indirizzo, il numero di telefono, l'indirizzo email, le informazioni di contatto dei familiari e altri dettagli personali (vedere paragrafo sui più gravi attacchi informatici).
Gli aggressori possono raccogliere e aggregare queste informazioni in modo da creare un profilo completo della vittima. Una volta ottenute le informazioni, gli attaccanti possono diffonderle pubblicamente attraverso vari canali online, inclusi forum, social media, siti web, chat e messaggi.
Gli obiettivi dietro il doxing possono essere: molestie, minacce, forme di vendetta, mezzo di pressione.

4.7 Sexstortion

Proseguendo, la "sextortion" è una forma di estorsione online in cui un individuo o un gruppo minacciano di diffondere immagini, video o informazioni sessualmente esplicite della vittima a meno che quest'ultima non soddisfi le richieste dell'aggressore.

Questo tipo di attacco sfrutta la vulnerabilità, la vergogna e la paura che possono derivare dalla diffusione di materiale intimo per costringere la vittima a pagare o fornire altro materiale. L'aggressore acquisisce materiale sessualmente esplicito della persona che decide di perseguitare. Il materiale può essere stato condiviso consensualmente in precedenza o ottenuto illegalmente attraverso metodi come il phishing, la violazione di account sui social media o la violazione di dispositivi.
La modalità più diffusa dai criminali informatici è quella di avvicinare online le vittime, con apprezzamenti per foto pubblicate, nascondendosi dietro a profili social di ragazze o ragazzi belli e gentili (social engineering).

Una volta agganciata la vittima la spingono a conversazioni sempre più intime fino ad arrivare alla condivisione di foto e video.
In caso di foto queste possono anche venire manipolate per una resa più umiliante (e anche in questo caso l'attaccante può farlo utilizzando la Generative AI).
L'aggressore, o le organizzazioni criminali che si celano dietro questo tipo di attacchi, minacciano di distribuire il materiale ottenuto a familiari, amici, colleghi o online, a meno che la vittima non assecondi le loro richieste.
Queste possono variare, ma spesso sono richieste finanziarie o di ulteriore materiale sessualmente esplicito.
La sextortion purtroppo è un fenomeno in crescita che colpisce anche minorenni. Solo nel mese di agosto 2023, in Italia, la Polizia postale ha dichiarato di aver ricevuto oltre un centinaio di segnalazioni.

4.8 Scheda didattica 1 - *scuole di ogni ordine e grado*

Titolo attività	**Approfondimento sul Cyberbullismo**
Obiettivo	Avere una comprensione approfondita di quali sono gli elementi che caratterizzano il cyberbullismo, in modo da poterlo identificare ed evitare.
Descrizione attività	Leggere con attenzione gli articoli forniti per approfondire le proprie conoscenze riguardo il cyberbullismo, con informazioni e consigli provenienti dalle fonti più attendibili e stimolare una discussione in calsse su questi temi.
Documentazione fornita	- Polizia Postale: cos'è il cyberbullismo? - Polizia Postale: consigli contro il cyberbullismo - Ministero dell'Istruzione e del Merito: bullismo e cyberbullismo - Ministero della salute: bullismo e cyberbullismo
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	30 minuti
Tipologia	Attività individuale
Contenuti propedeutici in ingresso	- Definizione di bullismo - Definizione di cyberbullismo
Conoscenze / Competenze / abilità in uscita	- Conoscenza dei termini bullismo e cyberbullismo - Capacità di riconoscere il cyberbullismo - Nozioni sulle conseguenze del cyberbullismo - Nozioni su dove ottenere aiuto in caso si diventi vittima o testimone di cyberbullismo
Documentazione di supporto aggiuntiva (URL o allegati)	

4.9 Scheda didattica 2 - *scuole di ogni ordine e grado*

Titolo attività	**Ricerca e identificazione di un messaggio di phishing**
Obiettivo	Essere in grado di identificare nel mondo reale messaggi o email sospetti, che possono essere riconducibili ad attacchi di tipo phishing.
Descrizione attività	In gruppi da 3 e con la supervisione dell'insegnante, cercare tra i propri messaggi di testo, whatsapp ed email dei messaggi che possano far pensare a phishing. Guardare tra i messaggi di testo di sconosciuti (per SMS e Whatsapp) e controllare la cartella spam dell'email. Identificare il tipo di phishing (vincita, allarme, etc.) e l'emozione che l'attaccante vuole suscitare (amicizia, preoccupazione, ecc.). **Attenzione:** non fare click su nessun link presente nei messaggi identificati.
Documentazione fornita	Nessuna documentazione fornita. Utilizzare i propri account di email, whatsapp, messaggi di testo, ecc.
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	60 minuti
Tipologia	Attività di gruppo - Min partecipanti: 2 - Max partecipanti: 4
Contenuti propedeutici in ingresso	Comprensione di cosa sia il phishing.
Conoscenze / Competenze / abilità in uscita	Capacità di identificare un messaggio di phishing. Capacità di osservare con attenzione i particolari che caratterizzano un messaggio di phishing. Esperienza reale in prima persona riguardante alcuni possibili attacchi di phishing.
Documentazione di supporto aggiuntiva (URL o allegati)	

4.10 Scheda didattica 3 - *scuole di ogni ordine e grado*

Titolo attività	**Creazione e individuazione di un messaggio di phishing**
Obiettivo	Acquisire ulteriore esperienza riguardo i messaggi di phishing, in modo da essere particolarmente abili nell'identificarli ed evitarli.
Descrizione attività	Ci si dividerà in gruppi, e il gioco avverà tra due squadre. Dividersi in un numero pari di gruppi. Ogni gruppo dovrà creare due messaggi: un messaggio legittimo e un messaggio di phishing. Il messaggio di phishing dovrà contenere almeno alcune delle caratteristiche comuni, come link camuffati o frasi che possano suscitare forti emozioni. Dopo aver creato i due messaggi, scambiarseli con un altro gruppo; analizzare i messaggi dell'altro gruppo per distinguere quello di phishing da quello legittimo. Per creare i messaggi, ci si potrà anche avvalere di strumenti di intelligenza artificiale, come quelli di Generative AI.
Documentazione fornita	Nessuna in particolare
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	60 minuti
Tipologia	Attività di gruppo - Min partecipanti: 2 - Max partecipanti: 6
Contenuti propedeutici in ingresso	- Comprensione di cosa sia il phishing - Esempi di email e messaggi di phishing
Conoscenze / Competenze / abilità in uscita	- Comprensione approfondita di cosa caratterizza un messaggio di phishing. - Esperienza reale in prima persona riguardante alcuni possibili attacchi di phishing.
Documentazione di supporto aggiuntiva (URL o allegati)	ChatGPT - *Nota bene: ChatGPT non genererà messaggi di phishing; parte dell'esercizio consiste nell'abilità di sfruttare tale strumento come aiuto alla generazione di un messaggio che possa anche essere usato per scopi di phishing.*

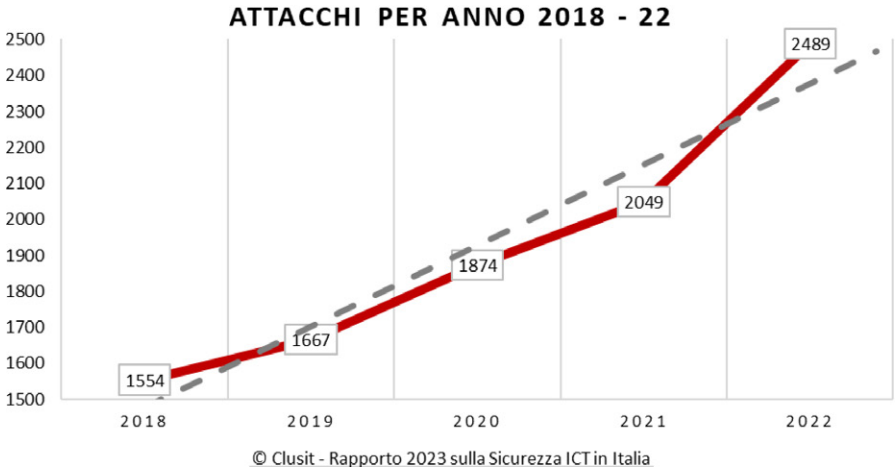
4.11 Scheda didattica 4 - *scuole di ogni ordine e grado*

Titolo attività	**Verificare se si è stati vittima di qualche data breach**
Obiettivo	Acquisire una maggiore sensibilità rispetto al rischio che i propri dati personali siano esposti in un data breach e rimediare dove possibile.
Descrizione attività	Visitare il sito https://haveibeenpwned.com/ e inserire un proprio indirizzo email. Il sito dirà se quell'email è stata oggetto di qualche data breach in passato, e darà alcune informazioni di dettaglio. Inoltre, per ogni data breach, ci dirà quali dati sono stati esposti. Se risultano email compromesse partire da quelle per concordare in una discussione aperta le contromisure da adottare (p.es. modificare la password dei servizi impattati da data breach). Analoga discussion può partire anche nel caso in cui non risultino indirizzi compromessi, ma facendo l'ipotesi che ce ne siano
Documentazione fornita	Nessuna in particolare
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	30 minuti
Tipologia	Attività individuale
Contenuti propedeutici in ingresso	- Comprensione del concetto di data breach - Comprensione del concetto di dato personale
Conoscenze / Competenze / abilità in uscita	- Capacità di verificare se la propria email è stata oggetto di qualche data breach in passato - Attenzione alla protezione dei propri dati personali
Documentazione di supporto aggiuntiva (URL o allegati)	- https://haveibeenpwned.com/ - Garante della Privacy: cosa sono i dati personali?

5 Attacchi informatici

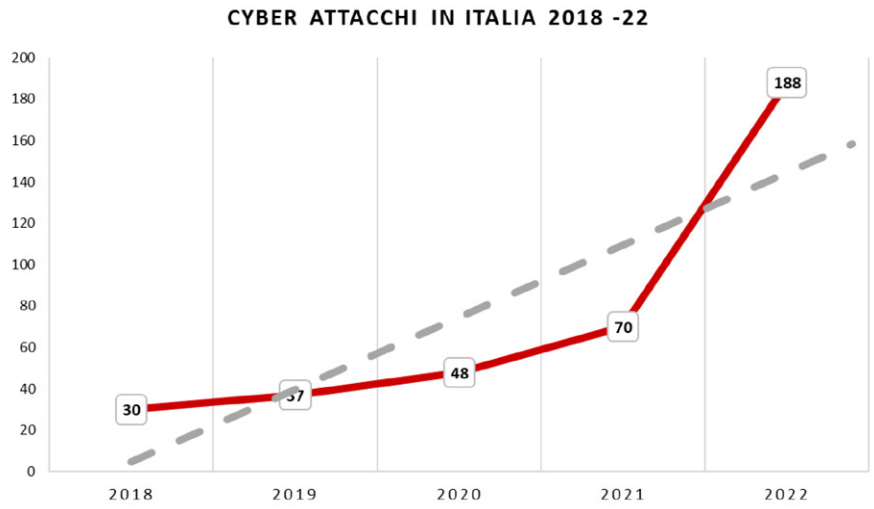
Lisa Da Re

Secondo il Rapporto Clusit 2023, se nel 2018 il numero di attacchi informatici era 1.554, nel 2022 si sono registrati 2.489 attacchi con un incremento del 60%.



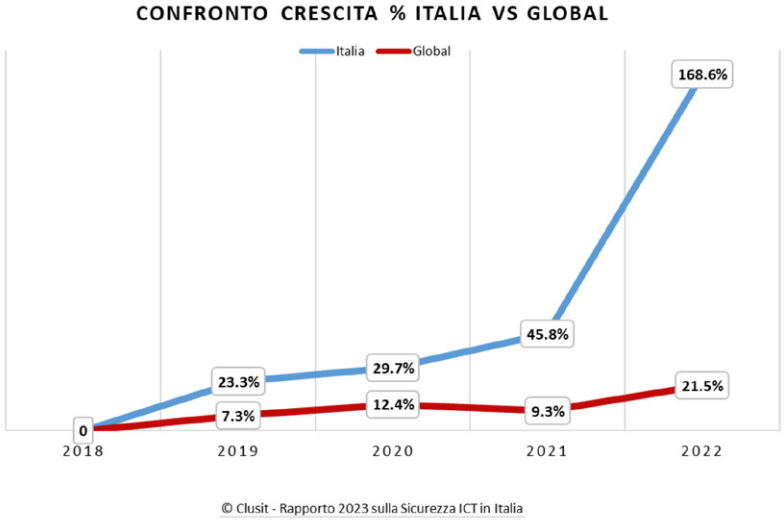
Andamento degli attacchi informatici

In questo scenario, il Clusit ha rilevato tra il 2018 e il 2022 un numero di attacchi di particolare gravità pari a 373.



Andamento degli attacchi informatici in Italia

Il nostro Paese dal 2022 riceve il 7,6% degli attacchi globali contro il 3,4% registrato nel 2021.

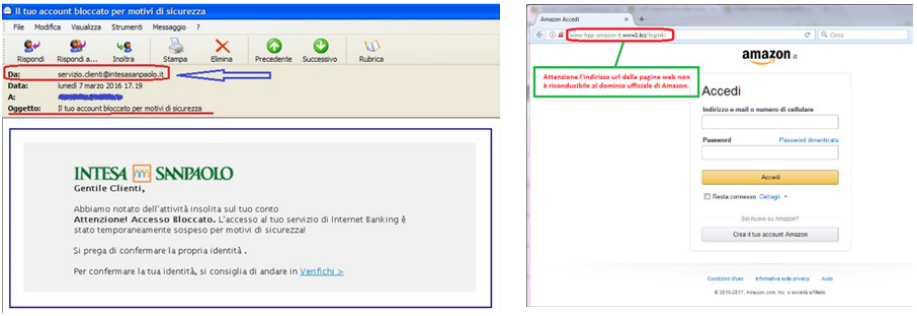


Andamento degli attacchi informatici in Italia versus gli attacchi globali

5.1 I principali tipi di attacchi informatici

Esistono diverse tipologie di attacchi informatici, vediamo insieme le principali.

1) **Attacchi di phishing**: consistono nel cercare di ingannare la vittima attraverso l'invio di messaggi o e-mail fraudolenti, convincendoli a fornire dati personali, finanziari, codici di accesso o password, fingendosi un interlocutore affidabile.



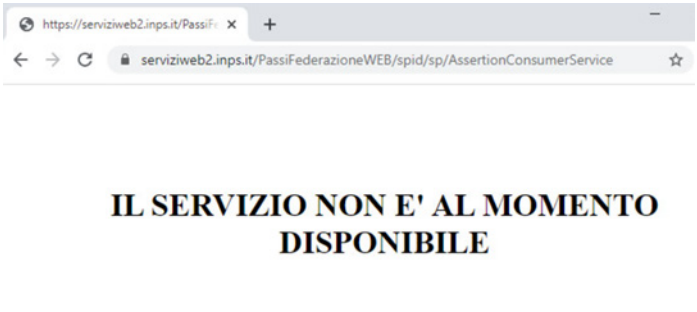
Esempi di attacchi informatici

In questi casi bisogna prestare attenzione alla e-mail del mittente e all'indirizzo URL della pagina web che devono entrambi essere quelli ufficiali.

2) **Attacchi di ingegneria sociale**: consistono in una manipolazione psicologica delle persone per ottenere accesso a informazioni riservate o per compiere azioni non autorizzate. Questi attacchi possono avvenire attraverso il telefono, e-mail, social media o incontri di persona. In questi casi l'hacker può collezionare informazioni relative alla vittima e ai suoi interessi semplicemente attraverso i social network (es. foto, commenti, gruppi di appartenenza, posto).

3) **Attacchi di forza bruta**: consistono nel tentativo di violare la sicurezza di un sistema tramite la generazione automatica di una vasta gamma di possibili combinazioni di password fino a trovare quella corretta. In questo caso è fondamentale utilizzare una password sicura.

4) **Attacchi di Denial of Service** (DoS): consistono nel sovraccaricare un sistema o una rete inviando un grande volume di richieste, al fine di renderli inaccessibili agli utenti legittimi.



Esempio di pagina non disponibile in seguito ad attacco DoS

5) **Attacchi di hacking**: consistono nello sfruttare vulnerabilità del sistema o delle applicazioni per ottenere accesso non autorizzato o per manipolare le funzionalità del sistema.

6) **Malware**: abbreviazione di software dannoso (Malicious Software), è un codice/software sviluppato con lo scopo di recare un danno a un dispositivo attraverso:
   - il furto dei dati
   - il bypass del controllo degli accessi
   - il danneggiamento dei dati
   - il controllo di un sistema a distanza
   - la compromissione di un sistema.

Esistono diverse tipologie di malware tra cui:

a) **Ransomware:** malware progettato per bloccare un sistema informatico o i dati in esso contenuti fino al pagamento di una somma di denaro (riscatto in inglese "ransom") per ripristinare l'accesso. Solitamente, il malware viene scaricato da un file e agisce crittografando i dati nel computer con una chiave sconosciuta all'utente.

Esempio di schermata in seguito al malware WannaCry

b) **Spyware:** malware progettato per tracciare e spiare l'utente (activity tracker, sequenze di tasti, acquisizione di dati). È di frequente associato a software legittimo o Trojan horse.
c) **Adware:** malware progettato per recapitare automaticamente pubblicità attraverso pop-up. Spesso viene installato con alcune versioni software, può contenere spyware.

Esempi di adware

d) **Virus:** programma/codice dannoso eseguibile, collegato spesso a programmi legittimi, che si diffonde duplicandosi. La maggior parte dei virus richiede l'attivazione da parte dell'utente. La sua diffusione avviene attraverso USB, condivisioni di rete o e-mail.
e) **Trojan:** malware che esegue operazioni dannose sotto forma di un'operazione desiderata, proprio come il cavallo di Troia. È presente in file di immagini, file audio o giochi. Differisce da un virus perché si associa a file non eseguibili.

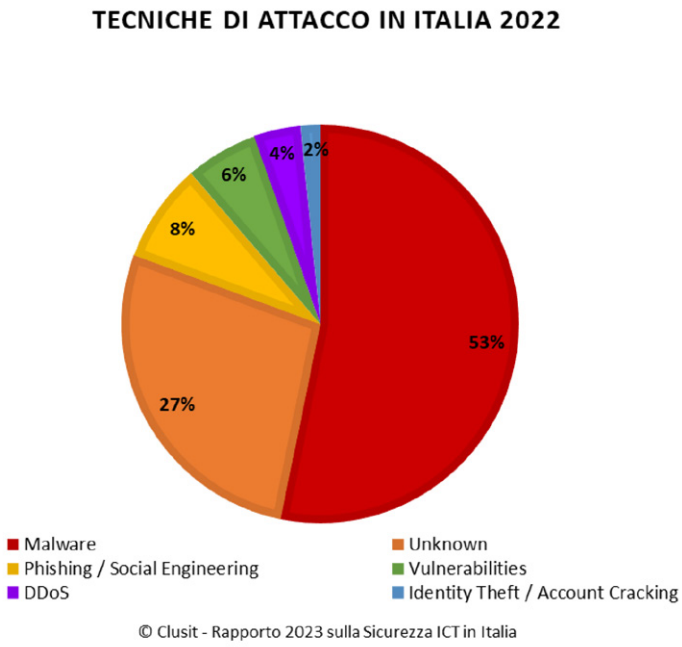
f) **Worm:** codice dannoso che si replica e diffonde in modo autonomo sfruttando le vulnerabilità nelle reti. Esauriscono le risorse di sistemi (memoria) o della rete (banda) creando dei rallentamenti. Sono responsabili di alcuni degli attacchi più devastanti di Internet come nel 2001 il worm *Code Red* che ha infettato 658 server e dopo 19 ore 300.000 server.

Rappresentazione della diffusione di Code Red

g) **Rootkit:** malware progettato per ottenere gli accessi di amministratore di sistema. Esso modifica il sistema operativo al fine di creare una backdoor attraverso cui accedere al computer in remoto e poter eseguire l'escalation dei privilegi.

In Italia tra le tecniche di attacco più utilizzate prevalgono:

- gli attacchi per mezzo di malware, pari al 53%,
- gli attacchi di phishing e di ingegneria sociale, pari al 27%.



Rappresentazione della tipologia di attacchi in Italia

5.2 Come possiamo proteggerci dagli attacchi informatici?

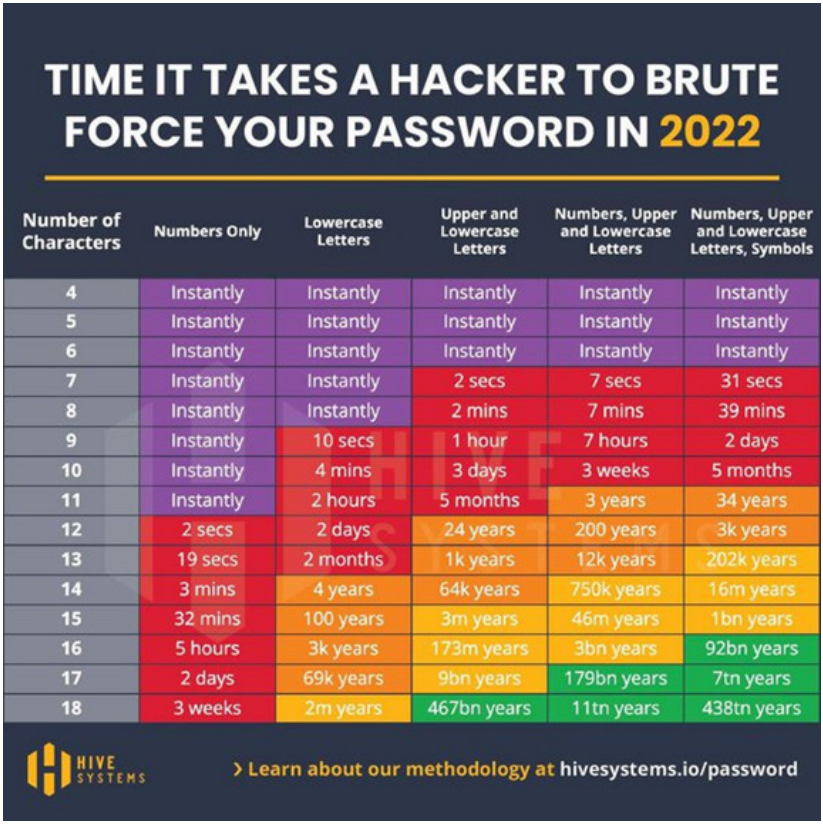
Gli attacchi informatici sono sempre più sofisticati e diffusi, minacciando la nostra privacy, la sicurezza finanziaria e persino la stabilità delle istituzioni.

In questo paragrafo, esploreremo alcune misure di sicurezza che ogni individuo e organizzazione dovrebbero adottare per proteggersi dagli attacchi informatici.

- Installare un software **antivirus** nel computer: gli antivirus sono software sviluppati per rintracciare la presenza di malware, rimuovere e proteggere il dispositivo;
- installare appena disponibili **aggiornamenti software e applicativi** nei nostri computer, tablet, cellulari: le vulnerabilità possono essere sfruttate dagli attaccanti per infiltrarsi nei nostri sistemi. Assicurarsi di installare regolarmente gli aggiornamenti di sistema e di applicazioni riduce le possibilità di sfruttare tali vulnerabilità;
- scaricare solo le **applicazioni** realmente **necessarie** nella vita quotidiana;
- scaricare applicazioni solo da **siti affidabili,** accertando che il sito in questione utilizzi il protocollo **HTTPS** (HyperText Transfer Protocol over Secure Socket Layer) che rende difficile intercettare i dati in transito. Per verificare che un sito sia protetto da HTTPS basta verificare se nella barra degli indirizzi del browser

ci sia un **lucchetto o uno scudo**. Inoltre, la parte iniziale del sito Web dovrebbe corrispondere alla dicitura https://

- usare **password robuste** composte da almeno 8 caratteri, da lettere minuscole/maiuscole/numeri/caratteri speciali. Inoltre, è importante utilizzare password diverse per ogni account.



Tempo necessario per un hacker di identificare una password a seconda della complessità

- utilizzare un **gestore di password** in modo da non doverle ricordare e non scriverle mai su fogli, documenti nel pc, rubrica telefonica;
- utilizzare **l'autenticazione a più fattori** (Multi factor authentication - MFA): gli account con accesso tradizionale (nome utente e password) sono facili da

penetrare. L'autenticazione a più fattori richiede che si forniscano almeno due fattori di autenticazione, o prove di identità, prima di poter accedere a dati protetti, creando così una seconda linea di difesa contro le attività criminali. L'attivazione del MFA rende molto più difficile per gli attaccanti accedere ai nostri account anche se riescono a ottenere la nostra password. I fattori che possono essere forniti per verificare un utente sono:

1. Conoscenza: un elemento che l'utente conosce (es. password)
2. Possesso: un elemento l'utente possiede (es. token)
3. Biometria: un elemento intrinseco all'utente (es. fingerprint).

Il MFA si ottiene combinando due di questi fattori: per esempio per il collegamento all'home banking si usa la password e il token che arriva su un cellulare autorizzato

- non condividere mai le proprie informazioni personali o password o pin;
- limitare l'utilizzo di chiavette USB;
- eseguire regolarmente il backup dei dati in modo che, in caso di attacco, sarà possibile recuperare i documenti o dati;
- fare attenzione a link e allegati provenienti da e-mail con mittente sconosciuto;
- essere consapevoli delle e-mail di phishing, che sono uno dei metodi più comuni utilizzati dagli attaccanti per ingannare le persone e ottenere accesso alle loro informazioni personali. Verificare sempre attentamente l'indirizzo email del mittente per rilevare eventuali incongruenze o errori ortografici anche nel testo della email;
- utilizzare solo reti sicure. Quando ci connettiamo a Internet, dobbiamo assicurarci che la nostra connessione sia sicura. Utilizzare reti Wi-Fi protette e criptate quando possibile, evitando le reti pubbliche non sicure. L'utilizzo di una connessione VPN (Virtual Private Network) può fornire un ulteriore strato di crittografia dei dati e protezione della privacy;
- Navigare solo in siti affidabili (es. con protocollo HTTPS).

Proteggersi dagli attacchi informatici richiede un approccio proattivo e una costante consapevolezza della sicurezza online. Adottare queste strategie essenziali può contribuire significativamente a ridurre le possibilità di subire un attacco informatico. Ricordiamo che la sicurezza online è una responsabilità condivisa, e dobbiamo fare la nostra parte per proteggere noi stessi, le nostre informazioni e la nostra comunità digitale.

5.3 Scheda didattica - *scuole secondarie di primo grado*

Titolo attività	**Attacchi informatici e come proteggerci**
Obiettivo	Avere consapevolezza delle principali tipologie di attacco e come riconoscerli e prevenirli.
Descrizione attività	- Valutare in piccoli gruppi: l'affidabilità di alcuni siti, l'affidabilità di alcune email e la sicurezza di alcune password. - Scrivere quali elementi hanno determinato la scarsa affidabilità di siti ed email e come si potrebbe migliorare la sicurezza delle password. - Produrre un documento finale, sintesi delle attività dei gruppi.
Documentazione fornita	Nessuna
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività di gruppo - Min partecipanti: 2 - Max partecipanti: 4
Contenuti propedeutici in ingresso	- Tecniche per costruire una password sicura - Valutazione di un sito sicuro
Conoscenze / Competenze / abilità in uscita	Capacità di riconoscere e prevenire alcuni attacchi informatici

6 Cyber Hygiene

Alessia Valentini

Con il termine Cyber hygiene si indica l'insieme delle buone prassi da seguire per ridurre al minimo i rischi derivanti dall'utilizzo di sistemi informatici, preservando così l'integrità e la sicurezza dei dati personali al fine di aumentare l'immunità dalle minacce.
Le raccomandazioni sono necessarie sia a livello di singoli utenti nel proprio ambito personale, sia in qualità di dipendenti o professionisti rispetto alla propria organizzazione/ambito di lavoro.

6.1 Le misure di protezione

Se consideriamo il contesto aziendale/scolastico la pubblicazione ENISA «Review of Cyber Hygiene practices» suggerisce 5 maggiori aree di intervento:

1. Protezione del "perimetro" ovvero la protezione di tutti i propri ambienti digitali (applicazioni, dispositivi, tutto l'Hardware e il software che si usa) che potrebbero essere soggetti a un attacco;
2. Protezione della rete, ovvero la protezione dei collegamenti digitali utilizzati per accedere, gestire e lavorare con hardware e software;
3. Protezione dei singoli dispositivi, ovvero protezione mediante software di sicurezza installato su ogni dispositivo digitale smart (dispositivo connesso in rete e con funzionalità digitali);
4. Uso del cloud in modo sicuro, ovvero impostazione della protezione a doppio fattore per l'accesso e le impostazioni di crittografia per mantenere i dati memorizzati in modo che non siano immediatamente intellegibili da un potenziale attaccante che riuscisse a sottrarli dal cloud;
5. Protezione della catena di approvvigionamento, ovvero garantire che anche i propri fornitori adottino misure di sicurezza per i prodotti e servizi che forniscono a voi e/o alla organizzazione in cui lavorate.

Per poter implementare correttamente le pratiche di Cyber Hygiene è opportuno almeno effettuare queste attività, che dovrebbero essere curate dalla scuola:

1. Tenere un registro di tutto l'hardware per avere sempre un inventario aggiornato dei dispositivi da proteggere;
2. Tenere un registro di tutto il software per assicurarsi di aggiornare per tutti sempre e puntualmente le patch di sicurezza;
3. Utilizzare guide di configurazione/hardening (la pratica di chiusura delle vulnerabilità per rafforzare il dispositivo e impedirne la violazione) per tutti i dispositivi (pc, cellulari, altri dispositivi smart...);

4. Gestire i dati in entrata e in uscita dalla propria rete LAN dell'organizzazione o la rete che si usa a casa, in caso di attività svolta in smartworking;
5. Scansionare tutte le e-mail in arrivo mediante adozione di software appositi che possano controllare gli allegati e valutare se siano stati alterati con codice malevolo;
6. impostare il privilegio minimo per gli account amministrativi che eventualmente si avessero nella propria organizzazione (o chiedere questa minima configurazione a coloro che si occupano dei servizi IT)
7. Eseguire regolarmente il backup dei dati e testare che possono essere effettivamente ripristinati;
8. Stabilire un piano di risposta agli incidenti, ovvero un processo di precise azioni da fare e persone da chiamare in caso si verifichi una violazione informatica;
9. Applicare livelli di sicurezza simili lungo tutta la catena di approvvigionamento con i fornitori (questa prassi rientra nella cosiddetta supply chain security)
10. Garantire controlli di sicurezza adeguati in qualsiasi contratto di servizio (inclusi i servizi erogati o adottati in ambiente cloud);
11. Garantire sempre la formazione per le persone (la cosiddetta awareness sulla sicurezza) in materia di pratiche truffaldine come il phishing, lo smishing e il Vhishing;
12. Garantire sempre attività di addestramento per mettere in pratica quanto imparato.

6.2 Gestione degli account e delle password

È importante gestire correttamente gli account sui nostri dispositivi oltre che sui social e sui vari siti a cui accediamo, senza dimenticare l'attenzione alla creazione e protezione delle password. Alcuni consigli di sicurezza suggeriti dalla Polizia postale sono:

- Non salvare sui dispositivi credenziali di accesso;
- Disconnettere i profili personali al termine della navigazione effettuando il logout.

Nell'ambito della protezione dei dispositivi è consigliabile seguire le prassi di:

1. Aggiornamento automatico dei dispositivi: configurare i propri dispositivi per aggiornare e installare le patch per app e sistema operativo;
2. Antivirus: sono da installare sempre sui dispositivi digitali con l'accorgimento di modifica delle impostazioni per interrompere le connessioni automatiche al Wi-Fi pubblico ed evitare così intercettazioni di dati non autorizzate;
3. Uso della crittografia per tutti dispositivi portatili, per evitare la lettura di

dati riservati dopo violazione informatica. Si consiglia l'uso della crittografia anche durante le trasmissioni di dati;
4. Uso di password complesse (lunghe, univoche composte di caratteri maiuscoli, minuscoli e speciali o formate da frasi) oppure, e preferibilmente, adozione di autenticazione a doppio fattore per attuare una maggiore sicurezza informatica;
5. Attivare l'autenticazione a più fattori alle aree digitali che custodiscono i propri dati (ambienti cloud);
6. Eliminazione definitiva: utilizzare software di cancellazione profonda per eliminare definitivamente i dati da vecchi computer, dispositivi mobili, smartphone, fotocopiatrici digitali e unità disco prima di darli via, buttarli, venderli o regalarli.

6.3 Ingegneria sociale

Un ulteriore e importante pratica di Cyber Hygiene è conoscere e attuare azioni contro l'ingegneria sociale. Si definisce ingegneria sociale la pratica di manipolare consapevolmente delle persone per ottenere informazioni senza dar loro modo di rendersi conto che si sta verificando una violazione della sicurezza (vedi anche il paragrafo sugli attacchi informatici). Gli accorgimenti e le contromisure di sicurezza sono strettamente legate alla formazione e all'educazione, che permettono di rendersi conto per tempo di tali comportamenti truffaldini.
Oltre il 90% degli attacchi informatici si verifica a seguito di errori umani evitabili. Questi errori umani si verificano a causa della mancanza di conoscenza, di attenzione o di preoccupazione per queste dinamiche di attacco. L'aggressore che utilizza gli attacchi di ingegneria sociale sfrutta le tre precedenti debolezze della natura umana per indurre la sua vittima a rilasciare informazioni sensibili, che gli consentono di lucrare a discapito della vittima. L'ingegneria sociale è in effetti un approccio per ottenere l'accesso alle informazioni attraverso false dichiarazioni. Può consistere in una impersonificazione di qualche forma di addetto amministrativo o manutentore che per telefono o per e-mail convince la potenziale vittima a dare quello che chiede (informazioni, credenziali, soldi). Alcune e-mail invitano il destinatario ad aprire un allegato che attiva un virus o un programma dannoso nel computer. L'attaccante può presentarsi in vari contesti insospettabili (luoghi pubblici, lavoro, casa, ufficio) mistificando la sua identità e facendo credere di essere qualcun altro, usando persuasione e manipolazione, per carpire informazioni altrimenti riservate e usarle a danno delle persone e a suo vantaggio. Tipicamente al telefono si subisce la simulazione di un amministratore di rete, che chiede password o credenziali o informazioni sensibili apparentemente per motivi leciti. Altri mezzi di ingegneria sociale sono le esche che sfruttano l'avidità della vittima nel volersi accaparrare qualche tool digitale lasciato incustodito ma di fatto infetto e capace di diffondere

l'infezione a tutti i contesti digitali della vittima.
Metodologie di ingegneria sociale non basate sulla tecnologia sono correlate alle pratiche di:

- ricerca nei cestini fisici per carpire enormi quantità di informazioni dai rifiuti e dai residui delle persone di una casa o di un ufficio: documenti riservati bollette, fatture, e ogni altro documento che possa contenere dati sensibili dovrebbe essere distrutto in molti pezzi prima di essere cestinato (dati interessanti per gli attaccanti riguardano: date di nascita, numeri di previdenza sociale e codice fiscale, indirizzo di residenza o domicilio, età, orari scolastici, date delle ferie e dati simili).
- Un'altra nota pratica non tecnologica è servirsi di bugie e false affermazioni, per costringere la vittima a un comportamento in emergenza o a seguito di imbarazzo o preoccupazione (questa metodologia è alla base di tutte le tipologie di truffe).
- In ultimo, il pretexting è l'atto di creare e utilizzare uno scenario immaginario per coinvolgere una vittima mirata in un modo che aumenta la possibilità che la vittima riveli informazioni o compia azioni che sarebbero improbabili in circostanze ordinarie (atti pretestuosi). È più di una semplice bugia.

Bisogna essere cauti in questi casi e dubitare sempre della veridicità delle informazioni ricevute, cercando conferme mediante altri canali informativi per reagire concretamente alle tecniche di ingegneria sociale

Per evitare di essere raggirati è consigliabile:

1. diffidare di telefonate, visite o messaggi e-mail non richiesti da persone che chiedono informazioni sui dipendenti o altre informazioni interne. Se un individuo sconosciuto afferma di appartenere a un'organizzazione legittima, provate a verificare la sua identità direttamente con l'azienda.
2. Evitare di parlare a voce alta dei fatti propri in luoghi pubblici perché si puo' essere ascoltati molto facilmente.
3. Non pubblicare tutto sui social, che diventano una fonte inesauribile di informazioni personali per gli attaccanti e rendono voi una vittima papabile.
4. Non fornire informazioni personali o informazioni sulla propria vita, lavoro, o ambito familiare, a meno di avere la certezza provata che chi lo richiede sia davvero una persona autorizzata a farlo.
5. Non rivelare informazioni personali o finanziarie nelle e-mail e non rispondere alle richieste via e-mail per queste informazioni.
6. Non inviare informazioni riservate su Internet prima di aver verificato la sicurezza di un sito web. Prestare attenzione all'URL di un sito web. I siti web dannosi possono sembrare identici a un sito legittimo, ma l'URL potrebbe utilizzare una variazione ortografica o un dominio diverso.
7. Se non si è sicuri che una richiesta via email sia legittima, è necessario provare a verificarla direttamente senza ricorrere alle informazioni di contatto

fornite su un sito web collegato alla richiesta; inoltre si può verificare se campagne di phishing siano in corso sul sito del CSIRT dell'ACN, l'Agenzia Nazionale per la Cybersecurity

8. Installare e mantenere aggiornati software antivirus, firewall e filtri e-mail per ridurre parte di questo traffico.
9. Sfruttare tutte le funzionalità anti-phishing offerte dal proprio client di posta elettronica e dal browser web.

7 Condotte digitali e profili legali

Anna Italiano

Nell'era digitale in cui viviamo, l'utilizzo delle tecnologie per finalità di svago, di apprendimento, di comunicazione e di conoscenza del mondo è diventato parte integrante della quotidianità degli adulti e, a maggior ragione, delle nuove generazioni.

È innegabile come la tecnologia sia diventata una compagna insostituibile, tanto nelle nostre incombenze quotidiane, quanto nei nostri momenti di svago. E, sotto questo profilo, possiamo affermare con certezza che l'evoluzione tecnologica sia un processo inarrestabile: occorre prenderne atto, senza demonizzarla, ma con la consapevolezza che anche il progresso tecnologico espone chi ne fruisce a rischi.

Il nostro compito di educatori, genitori e insegnanti è quello di trasmettere ai nostri ragazzi la consapevolezza di questi rischi e le regole fondamentali di un utilizzo sicuro delle tecnologie, che quei rischi aiutano a prevenire.
Infatti, l'onnipresenza delle tecnologie nella vita di tutti i giorni se, da un lato, ha facilitato l'accesso a informazioni e servizi, semplificandoci la vita in moltissimi aspetti, dall'altro, stante la pervasività con cui le stesse tecnologie sono in grado di plasmare le attività umane, fino ad arrivare a condizionare le abitudini e le scelte delle persone, può esporre i minori a situazioni spiacevoli, a contenuti inappropriati o disturbanti, fino ad arrivare alla messa a rischio alcuni diritti fondamentali della persona. Primo tra tutti: il diritto alla riservatezza. Senza contare che talune condotte adottate in Rete, per quanto attuate in una realtà virtuale, sono suscettibili di produrre effetti - e, non di rado, di avere impatti di tipo legale - anche nella realtà.

7.1 Perché in rete, senso della legalità ed etica si attenuano?

Partiamo da un dato di fatto: è provato da una serie di studi di psicologia e sociologia che il disvalore sociale percepito e attribuito a talune condotte attuate mediante l'utilizzo delle tecnologie sia minore rispetto a condotte equivalenti attuate nella sola realtà fisica e con modalità tradizionali. Un esempio per tutti: scaricare illegittimamente da Internet musica o libri o film in violazione dei rispettivi diritti d'autore è una condotta molto più diffusa e, come tale, percepita come "meno grave" rispetto a entrare in un media store o in una libreria fisica, occultare della merce e uscire senza averla pagata.

In altre parole, sembrerebbe che la mediazione dello schermo di un computer o di un tablet o di uno smartphone possano indurci una percezione alterata della liceità delle nostre condotte, allentando i nostri freni inibitori e provocando un abbassamento della soglia di ciò che è lecito, etico e morale.

Ma perché questo avviene?

Anzitutto, perché è diffusa la (falsa) convinzione che il mondo digitale possa sempre e comunque garantire l'anonimato. In secondo luogo, perché in Rete tutto appare "alla portata di un click" e ottenibile velocemente e senza eccessivo sforzo. Infine, perché le interazioni online spesso mancano del contatto diretto e immediato con le persone coinvolte: in questo modo, la distanza fisica può tradursi in distanza emotiva, con conseguente impatto sulla percezione degli impatti negativi che le condotte lesive ed offensive possono avere.

Come genitori, insegnanti ed educatori, non possiamo, quindi, ignorare questo effetto potenzialmente distorsivo dei valori etici e morali che l'utilizzo del digitale può ingenerare, specialmente in soggetti come i ragazzi, che sono tendenzialmente resi più vulnerabili dalle dinamiche di identificazione e riconoscimento da parte del "branco" tipiche dell'età adolescenziale. Occorre piuttosto insegnare ai ragazzi che anche le condotte digitali, poste in essere mediante l'utilizzo di tecnologie come internet, smartphone, social media, applicazioni di messaggistica istantanea e via dicendo, possono non solo avere delle ripercussioni anche nella vita reale, esattamente come avviene con le condotte fisiche, ma che, talvolta, tali ripercussioni possono essere particolarmente gravi, poiché amplificate dalla diffusione della tecnologia, dalla capacità di un contenuto pubblicato in Rete di raggiungere un altissimo numero di soggetti in tempi brevissimi e dalla circostanza che Internet non conosce barriere fisiche o confini territoriali e spaziali.
Nel contesto scolastico, è, dunque, compito dell'insegnante far comprendere ai ragazzi che taluni atteggiamenti e condotte adottate in rete possono avere conseguenze nocive e, in alcuni casi, persino integrare dei reati ed essere perseguibili per legge.

7.2 Alcune condotte digitali che possono avere ripercussioni di tipo legale

Vengono di seguito trattati – con taglio pratico e senza pretesa di esaustività – alcuni fenomeni particolarmente preoccupanti di cui i ragazzi possono rimanere vittime o di cui, in taluni casi, possono, specularmente, rendersi autori.

- Il cyberbullismo
Mentre, come sappiamo, il bullismo è quell'insieme di condotte di sopraffazione e prevaricazione, volte a umiliare, vessare e isolare la vittima, il cyberbullismo consiste nell'attuazione di quelle stesse condotte mediante l'utilizzo di mezzi elettronici e tecnologie digitali.
Una definizione di questo fenomeno viene data per la prima volta, nel nostro ordinamento, con la legge n. 71/2017, che definisce il cyberbullismo come "*Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione,*

diffamazione, furto di identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali, di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

Un atto di cyberbullismo può esporre sia a conseguenze penali che a conseguenze civili.
Sotto il primo profilo, sebbene il nostro ordinamento non preveda un reato specifico di cyberbullismo, le condotte poste in essere dal cyberbullo sono suscettibili di essere ricondotte, a seconda dei casi, a una serie di fattispecie incriminatrici, tra cui: lesioni personali (art. 582 c.p.), diffamazione (art. 595 c.p.), violenza privata (art. 610 c.p.), minacce (art. 612 c.p.), stalking (art. 612-bis c.p.), molestia o disturbo alla persona (art. 660 c.p.), ecc.
Sotto il secondo profilo, invece, gli atti di cyberbullismo, quand'anche non rilevanti penalmente, possono dar luogo al diritto della vittima a ottenere un risarcimento in sede civile, ai sensi di quanto disposto dall'art. 2043 c.c., per cui, qualunque fatto doloso o colposo che cagioni ad altri un danno ingiusto obbliga colui che l'ha commesso a risarcire il danno.

È importante sottolineare che, a differenza della responsabilità penale – che ha sempre e immancabilmente carattere personale – sul piano civile, le conseguenze dei fatti illeciti di una persona minorenne possono ricadere anche su coloro che hanno il compito di educare il minore e vigilare su di esso al fine di prevenire condotte anomale e dannose.
Più in particolare, l'art. 2048 sancisce un'ipotesi di responsabilità per "*culpa in vigilando*" a carico di genitori ed educatori. Infatti, salvo che non provino di essere stati impossibilitati a impedire il fatto, i primi sono sempre responsabili del fatto illecito commesso dai figli minori, mentre anche gli insegnanti e l'istituto scolastico potrebbero essere chiamati a risarcire i danni che siano derivati da condotte commesse nell'ambito del contesto scolastico, qualora sia accertato che abbiano omesso di esercitare la dovuta vigilanza sui minori a essi affidati.

- La pornografia non consensuale
Il reato di pornografia non consensuale (o, come viene definito dal codice penale, di "diffusione illecita di immagini o video sessualmente espliciti") è un reato introdotto in Italia nel luglio 2019, proprio per far fronte al fenomeno sempre più dilagante della diffusione di immagini e video intimi attuata senza il consenso della persona ritratta.
Nel linguaggio mediatico, per indicare tale condotta, si parla spesso anche di

"revenge porn", anche se, in realtà, tale espressione risulta impropria, poiché la fattispecie perseguibile penalmente è molto più ampia e ricomprende ogni ipotesi di diffusione illecita di materiale intimo, qualunque sia il motivo per cui essa viene effettuata (dunque, non solo la condivisione di materiali intimi attuata per finalità di vendetta). Le ragioni che stanno alla base di un simile abuso possono essere le più varie: dall'ottenere un profitto economico (per esempio, dietro ricatto, dopo aver sottratto il materiale a seguito di hacking di dispositivi o di spazio cloud), al vantarsi delle proprie conquiste o della propria vita sessuale; dall'attuare una forma crudele di bullismo fomentata dalle dinamiche del branco al porre in essere condotte superficiali e leggere, come la ri-condivisione di materiale intimo ricevuto, che contribuisce ad aggravare la portata del reato commesso dal colpevole originario e, con essa, le sofferenze della vittima.
Probabilmente è abbastanza noto che diffondere immagini o video sessualmente espliciti e destinati a rimanere privati, dopo averli realizzati (anche con il consenso della vittima, come può accadere durante un rapporto sessuale o a seguito di sexting) o trafugati costituisce un reato. Forse, però, non tutti sanno che commette reato anche chi, dopo avere ricevuto quelle immagini o quei video, a propria volta li ri-condivide, contribuendo alla loro diffusione e ad aggravare la portata del reato commesso dal colpevole originario.
Il modo più efficace per contrastare questo triste fenomeno è sicuramente agire sotto il profilo della prevenzione, anziché sotto quello della repressione, perché, sebbene le Forze dell'Ordine abbiano i mezzi tecnici e giuridici per limitare la diffusione dei materiali incriminati e individuare i colpevoli, nel momento stesso in cui si verifica anche solo una condivisione di un video o una foto destinata a rimanere riservata, l'intimità della vittima viene lesa irreparabilmente.

Come educatori, dovremmo quindi educare e sensibilizzare i ragazzi:
- al rispetto dell'intimità altrui e all'esistenza di una sfera intima e personalissima che riguarda ciascuno di noi e che nessuno ha diritto di valicare senza il consenso della persona alla quale tale sfera si riferisce;
- al fatto che esistano aspetti del vissuto – come quelli relativi all'intimità e alla sessualità – talmente preziosi che non dovrebbero essere indiscriminatamente "messi in piazza", nonostante la realtà in cui viviamo ci spinga sempre di più verso la condivisione di contenuti e verso relazioni "social";
- circa le condotte che, oltre che essere moralmente riprovevoli, costituiscono reato e vengono, pertanto, perseguite penalmente;
- al prestare molta attenzione ai contenuti che si ricevono, ma anche a come, a propria volta, li si utilizza (evitando, per esempio, qualsiasi ulteriore ricondivisione, onde evitare di porre in essere, magari inconsapevolmente, delle condotte penalmente rilevanti);
- alle modalità con le quali reagire a condotte illecite come quella considerata.

Sotto questo punto di vista, è bene ricordare che la pornografia non consensuale è un reato procedibile solo a querela della persona offesa, che può essere presentata nel termine di 6 mesi. Questo vuol dire che chi ha commesso il reato può essere perseguito dalle Forze dell'Ordine e dall'Autorità Giudiziaria solo se la vittima ha sporto denuncia;

- infine, a non colpevolizzare coloro che rimangono vittime di pornografia non consensuale, visto che molto spesso le vittime tendono a sottacere il reato e non denunciare proprio perché si colpevolizzano o, addirittura, vengono colpevolizzate, per aver condiviso proprie foto o video intimi sottostimando i rischi che ne potevano derivare. Quand'anche abbia avuto comportamenti imprudenti o leggeri, la vittima rimane pur sempre una vittima e nulla ci autorizza a ritenere che ci possa essere una condivisione di responsabilità con il suo carnefice.

- *Violazione della privacy e adescamento online*

La protezione della privacy digitale dei minori è un compito fondamentale di genitori ed educatori.
I preadolescenti di età compresa tra 10 e 13 anni sono particolarmente esposti ai rischi derivanti da ingerenze alla propria sfera di riservatezza e alle dinamiche più patologiche che possono manifestarsi nell'ambito delle relazioni online.
Infatti, è proprio in questa fascia d'età che i ragazzi – spesso non avendo nemmeno l'età minima richiesta dalla normativa vigente per poter fruire di servizi digitali – aprono i primi profili social o iniziano a utilizzare app di messaggistica istantanea o piattaforme di interazione online.

Sotto il profilo delle minacce alla sua sfera di riservatezza, i rischi cui un minore può andare incontro per effetto di un utilizzo incontrollato e poco consapevole delle tecnologie sono fondamentalmente riassumibili in:

- rischi per la privacy e condivisione incontrollata di informazioni personali: i minori spesso non comprendono appieno le implicazioni della condivisione incontrollata di informazioni personali online. La pubblicazione di foto, indirizzi, scuole frequentate o dettagli sulla propria vita può mettere a rischio la loro sicurezza e privacy, rendendoli vulnerabili ad abusi, furti di identità o monitoraggio indesiderato.
- Tracciamento delle attività online e raccolta di dati personali: le nuove tecnologie e le piattaforme che offrono servizi digitali consentono alle aziende di raccogliere una vasta quantità di dati personali sui minori, inclusi interessi, abitudini di navigazione e posizione geografica. In mancanza di un'impostazione consapevole delle impostazioni privacy di app e servizi online e una gestione oculata dei consensi espressi in sede di registrazione e iscrizione alle piattaforme, questi dati possono essere utilizzati per scopi di marketing mirato o venduti a terze parti senza il consenso dei genitori;
- Possibilità di contatto con estranei e rischio di adescamento online: pedofili e

adulti abusanti – detti anche "groomer" – possono sfruttare i social network, le piattaforme di gioco online o le chat room per avvicinare bambini e adolescenti per scopi sessuali, cercando di vincerne le resistenze e conquistandone gradualmente la fiducia, con la finalità di instaurare una relazione sessuale o sessualizzata. È bene sottolineare che la manipolazione su cui si fonda l'adescamento è facilitata spesso dalla mole di informazioni di sé che i ragazzi condividono spontaneamente in rete e che costituiscono, per gli adescatori, un punto di partenza fondamentale per agganciare il minore. Spesso il minore ignora che dall'altra parte dello schermo potrebbe trovarsi un adulto: il linguaggio utilizzato, la comunanza dichiarata di interessi e gli atteggiamenti adottati possono facilmente indurlo a credere di rapportarsi con un coetaneo. In alcuni casi, invece, la differenza d'età è nota fin dall'inizio, ma la lontananza e la mediazione dello schermo facilitano le confidenze e la sottovalutazione del pericolo.

In Italia, ogni condotta volta a carpire la fiducia di un minore di 16 anni attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete Internet o di altri mezzi di comunicazione, al fine di perseguire scopi sessuali, è un reato fin dal 2012 e viene punito con la pena della reclusione da uno a tre anni (art. 609-undecies c.p.).

Dati i numeri preoccupanti di fenomeni di abuso perpetrati anche a danno di minori tramite l'utilizzo della rete, fare prevenzione nelle scuole è non solo opportuno ma anche necessario e fondamentale. Ferma la necessità di collaborazione e stretta sinergia educativa tra le famiglie e la scuola, gli insegnanti potrebbero:

- parlare di privacy in classe per far comprendere ai ragazzi che cosa sia un dato personale (erroneamente, infatti, si ritengono tali solo nome, cognome e poco altro, mentre lo è anche l'immagine - e, quindi, costituiscono dati personali anche le foto o i video che ritraggono il minore, così come tutte le informazioni che, direttamente o indirettamente, possono essere ricondotte a una persona fisica e che ci rivelano dettagli anche molto personali di un individuo, tra cui, per esempio, la nazionalità, le convinzioni religiose, lo stato di salute, ecc.);
- educare i ragazzi a distinguere la sfera di ciò che può essere reso pubblico da quella di ciò che è meglio rimanga privato, insegnando loro a valutare attentamente prima di affidare informazioni personali alla rete e, comunque, a non condividere con persone che non conoscono bene anche "offline" informazioni di carattere personale, come l'indirizzo di casa, la scuola frequentata o i propri interessi personali;
- invitare i ragazzi a informarsi sulle impostazioni privacy e sui meccanismi di sicurezza di app, tecnologie e servizi, suggerendo loro di condividere con i propri genitori le scelte circa i contenuti da rendere aperti a un pubblico indifferenziato e la gestione dei consensi per il trattamento dei dati personali;
- diffondere consapevolezza circa l'età minima richiesta per legge perché una

persona possa validamente fornire il consenso al trattamento dei propri dati personali. In Italia, tale soglia minima è rappresentata dai 14 anni, mentre l'iscrizione a servizi digitali nella fascia d'età compresa tra i 13 e i 14 anni è consentita a condizione che vi sia il consenso dei genitori;

- parlare apertamente ai ragazzi, scegliendo modalità compatibili con la loro età, dei rischi di abuso perpetrati attraverso gli strumenti tecnologici, come la pornografia non consensuale o l'adescamento online, e spesso favoriti da comportamenti imprudenti della vittima, che viene manipolata e indotta a fidarsi;
- favorire un dialogo scuola-famiglia sui rischi del digitale e sull'uso consapevole delle tecnologie, sensibilizzando i genitori sull'importanza della formazione su queste tematiche, sul dialogo e sulla creazione di un ambiente di ascolto dei propri figli, sull'importanza di regole che disciplinino l'utilizzo delle tecnologie (per esempio riguardo alla durata giornaliera, ai siti e/o alle app consentite, ecc.) nonché della condivisione delle motivazioni che stanno alla base di tali regole.

8 La nostra impronta sul web

Anna Vaccarelli

Nel mondo interconnesso e digitale di oggi, l'identità digitale e la web reputation hanno acquisito un ruolo di fondamentale importanza per ciascuno di noi. La nostra vita scorre sia online che offline e le due modalità sono strettamente intrecciate, tanto che nel 2014 Luciano Floridi ha coniato il termine "onlife", una crasi tra online e life (vita), per sottolineare che c'è una continua interazione tra la digitale e "materiale".
È quindi importante imparare a gestire la propria presenza online, visto che può influenzare significativamente quella offline. Nella vita offline siamo istintivamente abituati a curare l'immagine che vogliamo dare di noi agli altri, sia nel comportamento che nell'aspetto, cercando di essere coerenti con noi stessi e di mandare su di noi un messaggio univoco. Generalmente cerchiamo di fare in modo che gli altri abbiano di noi una impressione positiva e che la comunità in cui viviamo ci accetti facilmente. Ma potremmo anche voler dare di noi una immagine non "conforme" agli standard, magari ribelle o anticonformista: anche in questo caso mandiamo messaggi coerenti con questo schema, perché gli altri ci percepiscano con queste caratteristiche.
Nella vita online succede esattamente la stessa cosa, anche se la percezione che ne abbiamo è molto meno immediata. Anche online i nostri comportamenti, i nostri commenti, i contenuti che pubblichiamo contribuiscono a creare negli altri un'immagine di noi e questa immagine si intreccia inevitabilmente con quella che abbiamo offline (a meno che con conduciamo online una doppia vita con uno pseudonimo!)
L'avvento della tecnologia ha aperto nuove opportunità di comunicazione e connessione, ma ha anche reso essenziale gestire attentamente la propria presenza online e la percezione che gli altri hanno di noi.
Per molti sviluppare questa attenzione non è immediato e questo può portare delle conseguenze nella nostra vita reale: dobbiamo perciò imparare a gestire la nostra identità digitale e prendercene cura.

8.1 L'identità digitale

L'identità digitale è l'insieme di informazioni personali che ci definiscono in modo esclusivo su Internet: quelle che condividiamo sui social media, sui siti web personali o professionali, e su altre piattaforme online, ma anche il nome e cognome, l'indirizzo di posta elettronica, le password di accesso, il codice fiscale, i numeri delle carte di credito o le copie digitali di documenti cartacei (per esempio foto o scansioni). Per estensione, il concetto include anche gli strumenti come lo SPID (Sistema Pubblico di Identità Digitale), la CIE (Carta di Identità Elettronica) e la

CNS (Carta Nazionale dei Servizi) che permettono l'accesso a diversi servizi online in maniera più sicura. Dell'identità digitale fanno parte anche la nostra professione, i nostri interessi, le nostre opinioni e molto altro. È ciò che gli altri possono trovare e conoscere di noi tramite una ricerca online.
L'identità digitale è diventata una parte integrante della nostra vita: quando qualcuno cerca il nostro nome su Internet, l'identità digitale che emerge avrà un impatto significativo sulla impressione che si forma di noi. Spesso quando veniamo in contatto via rete con una persona che non conosciamo, la prima cosa che facciamo è cercare online una foto e delle informazioni per farcene un'idea. Idea che sarà basata su quello che la persona ha lasciato in Rete, non necessariamente su quello che ha fatto o detto nella vita reale e che può essere diverso dalla sua personalità in Rete. Ma quello che conta è che noi ci siamo fatti un'idea basata su quello che abbiamo trovato in Rete e fino a che non avremo occasione di incontrare quella persona quell'idea non verrà cambiata.
Ci sono diverse situazioni in cui l'opinione che gli altri si fanno di noi attraverso la nostra identità digitale può avere effetti "reali", per esempio può influenzare le opportunità di lavoro, le relazioni personali, le partnership commerciali e la nostra reputazione online. Gestire attentamente la propria identità digitale è essenziale per presentarsi in modo positivo e coerente con ciò che vogliamo rappresentare e far conoscere di noi.

8.2 Web reputation (cosa gli altri pensano di noi)

Associato al concetto di identità digitale c'è quello di reputazione online (*web reputation*). Per ciascuno di noi la *web reputation* è la **percezione** che gli utenti del web hanno di noi, è l'idea che si fanno dalle "tracce" che lasciamo in Rete, dai commenti che facciamo sui social, dai post, in generale dai nostri comportamenti online.
Ogni azione che compiamo online contribuisce a costruire la nostra web reputation e influenza il nostro "pubblico", in modo da creare su di noi un giudizio, come accade nella vita reale alle persone che frequentiamo.
A differenza della vita reale, però, dove alcune situazioni, comportamenti, affermazioni, commenti, magari inopportuni o spiacevoli, possono essere dimenticati, la Rete ha una memoria lunghissima ed è possibile ritrovare cose scritte, dette, pubblicate molto tempo prima. È importante quindi riflettere bene su cosa pubblichiamo, commentiamo e condividiamo perché in futuro potremmo dover fare i conti con le tracce che abbiamo lasciato.
Per i ragazzi questo problema è ancora maggiore, perché rispetto agli adulti, hanno una storia online che sarà molto più lunga di quelli che sono adulti oggi e sarà fonte di molte più informazioni su di loro, influenzerà significativamente la loro reputazione e non solo quella online. Basti pensare che da adulti, magari alla ricerca di un lavoro, potrebbe venire fuori qualche commento o post pubblicato da ragazzi che può rivelarsi imbarazzante e compromettere la valutazione che il potenziale datore

di lavoro si sta formando sul giovane aspirante. Bisogna anche tenere presente che, se ci accorgiamo di avere scritto o pubblicato un post "sbagliato", rimuoverlo non è detto ci garantisca dalle conseguenze perché qualcuno potrebbe averlo memorizzato in uno screenshot e potrebbe ripubblicarlo in un secondo momento, dandogli nuova vita. Il rischio può essere evitato solo pensando molto bene prima di pubblicare qualunque contenuto o commento. Se ci accorgiamo di avere scritto o pubblicato un post "sbagliato" può convenire scusarsi, rimuoverlo, proprio per il fatto che potrebbe essere ripubblicato in un secondo momento, ripescandolo, appunto, nella memoria della Rete.
Se vogliamo dare di noi un'immagine positiva dobbiamo sforzarci di costruirla con coerenza, cercando di essere attenti a ciò che pubblichiamo online e come comunichiamo con gli altri, utilizzando con saggezza la privacy e le impostazioni di sicurezza per proteggere le informazioni personali.
Nel gestire la nostra presenza online, inoltre, è opportuno monitorare le informazioni che si possono trovare online su di noi, rimuovere info e contatti non desiderati.

8.3 Rischi

Per ogni utente della Rete potenzialmente esistono dei rischi, che è bene conoscere soprattutto per riuscire a evitarli. Esistono anche nel caso dell'identità digitale e possono riguardare la nostra o quella degli altri.

8.3.1 Furto identità digitale

Il primo tra tutti i rischi è il furto di identità, che è un reato a tutti gli effetti e, formalmente, si verifica quando un cyber criminale accede illegalmente e senza autorizzazione alle informazioni personali di un altro individuo. Se, per esempio, viene a conoscenza delle credenziali di accesso agli account social può sostituirsi al legittimo proprietario e pubblicare contenuti che appaiono scritti e prodotti dalla vittima del furto, con il rischio di danneggiarne la reputazione. Il danno è tanto maggiore se la vittima è un soggetto pubblico come per esempio un politico, una persona di spettacolo ecc. la cui immagine online viene costruita accuratamente in base a una specifica strategia, per accattivare il suo pubblico o i suoi elettori. Spesso questo tipo di attacco è fatto apposta per danneggiare pubblicamente la vittima. Ancora più pericoloso è il caso in cui il malintenzionato acceda alle credenziali delle carte di credito, dove il danno immediato è direttamente di tipo economico.
Se il furto di credenziali è "massivo" cioè le vittime contemporaneamente attaccate sono moltissime, è possibile che questi dati vengano rivenduti a terzi.
Il furto di identità che porta a una "sostituzione" di persona (p.es. qualcuno si appropria di un account social non suo) ci deve far riflettere sulla necessità di osservare sempre con spirito critico i contenuti pubblicati da persone/profili che seguiamo, tenendo presente che, se sono particolarmente anomali, può essersi verificato un furto di identità.

Il criminale può arrivare a conoscere le credenziali della vittima attraverso diverse tecniche (per le quali vi rimandiamo agli altri capitoli):

- **phishing;**
- **malware;**
- intercettazione dei dati **durante la navigazione in Rete;**
- furto dei dati direttamente **dai dispositivi elettronici** spiandoli mentre li digitiamo o rubando i dispositivi;
- **social engineering.**

In generale è buona norma controllare i nostri account regolarmente. Per monitorare quelli social, oltre a presidiarli, può essere utile cercare il proprio nome con un motore di ricerca e verificare i risultati.
Nel caso dell'accesso alla banca o alle carte di credito è prudente impostare dei messaggi che arrivino sul cellulare nel momento in cui venga effettuata una spesa oltre una soglia fissata e controllare regolarmente i resoconti di spesa.

8.3.2 Falsi profili

Un aspetto diverso dell'identità online è la possibilità di imbattersi in profili falsi.
Sono diverse le ragioni per cui qualcuno decide di creare un falso profilo:

- spiare l'attività di altri profili rimanendo in incognito;
- aggirare i blocchi che il social ha messo sull'account personale;
- ingannare i contatti con l'obiettivo di:
  - instaurare una relazione sentimentale: in questo caso si parla anche di profilo "catfish" e, spesso, il falso profilo è solo il primo di una serie di altri reati, perché tipicamente in queste situazioni vengono chieste foto "osé" con le quali la vittima viene poi ricattata (sextortion);
  - attuare una truffa: si approfitta dell'ingenuità della vittima per portarla a dare informazioni personali o per ottenere benefici economici. Queste truffe, come metodo, non sono una novità: quante volte abbiamo sentito di falsi tecnici, per esempio, di reti telefoniche che si introducono in casa e dicono di dover riscuotere improbabili bollette o di sedicenti nipoti che telefonano ad anziane signore per convincerle a ricevere e pagare (centinaia di euro) per conto loro per un pacco di importanza strategica? Il metodo è lo stesso, è il mezzo, il tramite, che cambia e ciascuno di noi deve essere pronto a riconoscere questi rischi anche online;
- pubblicare false recensioni, molto positive per promuovere un prodotto o un servizio o molto negative per affossarlo, a volte dietro compenso;
- inserirsi nelle discussioni online per orientarle (e questo si verifica soprattutto in prossimità di elezioni politiche o di decisioni importanti) o disturbarle (trolling).

Solo su Facebook, si stima che 87 milioni di profili siano falsi. Il furto di identità si configura come un reato, con sfumature diverse a seconda dell'obiettivo che il criminale vuole raggiungere o delle tecniche che utilizza.

8.3.3 Come distinguere un profilo falso da uno vero

In genere, a meno che non si tratti di "professionisti" di questo tipo di crimine, è possibile verificare se un profilo è falso o almeno farsi venire dei dubbi.
Possiamo fare alcuni semplici controlli:

- verificare che le info nel profilo siano complete, coerenti e abbastanza specifiche;
- verificare se ha un'attività regolare nel pubblicare contenuti;
- verificare se la creazione dell'account è molto recente;
- verificare se il numero di "follower" (qualunque sia il social) ha un andamento di crescita regolare e, se ha numeri molto alti, cercare di capire se è giustificato rispetto ai contenuti pubblicati e agli hashtag;
- immagine del profilo: si può scaricarla e chiedere informazioni a Google immagini. Se è associata a più persone, molto probabilmente non corrisponde all'identità di nessuna di esse;
- controllare se l'account viene taggato da amici e conoscenti e se abbiamo amici in comune;
- verificare la regolarità di pubblicazione: se una persona non condivide contenuti e sta su un social può destare qualche sospetto.

Naturalmente il malintenzionato ha maggiori possibilità di agganciarci se ha sufficienti informazioni su di noi, perché può interagire con noi su argomenti che sa che ci interessano e su episodi e situazioni che ci riguardano direttamente. E le informazioni le altre persone le possono trovare grazie a tutte le "tracce" che volontariamente o solo per superficialità lasciamo in Rete.

8.3.4 Come proteggere l'identità digitale

Quello che ci deve preoccupare non è solo proteggere la nostra reputazione quanto tutti i dati che vanno a comporre la nostra identità digitale: i dati anagrafici (se rendiamo pubblico nome, cognome e soprattutto data e luogo di nascita rendiamo immediatamente disponibile in nostro codice fiscale), le credenziali di accesso per esempio all'home banking, alle carte di credito, le password, spesso troppo banali (1234 è la password più diffusa) o memorizzate in chiaro o in vista e così via. Si richiede attenzione e consapevolezza nell'attuare una serie di contromisure, anche preventive, per evitare di essere danneggiati.
In Europa, l'identità digitale è protetta dal GDPR (General Data Protection Regulation), adottato nel 2016 dal Parlamento europeo e reso operativo anche in Italia dal 2018. Il GDPR obbliga le organizzazioni che raccolgono dati personali online a garantire che siano protetti, ma questo obbligo, purtroppo, non è rispettato da tutti,

volontariamente o anche solo per ignoranza e superficialità. In questo scenario, è opportuno che prestiamo attenzione in prima persona a:

- rendere privati i nostri profili: in questo modo ciò che pubblichiamo potrà essere visto solo dalle persone che abbiamo autorizzato personalmente. Come corollario ne discende che dovremmo aver valutato bene prima di accettare tra gli "amici" o i "follower" nuovi soggetti che magari non conosciamo direttamente. Il fatto che abbiamo un contatto o un'amicizia in comune non è necessariamente una garanzia: anche creare contatti comuni può far parte della tecnica di "avvicinamento" da parte di un malintenzionato.
- Rimuovere o limitare i permessi che concediamo alle app di terze parti che possono accedere ai nostri dati: molte app chiedono di accedere per esempio alla geolocalizzazione o alla rubrica. Questi permessi vanno limitati allo stretto indispensabile e, possibilmente, scegliendo l'opzione "solo quando l'app è in uso".
- Negare il consenso ai cookie non rilevanti: spesso è noioso dover smarcare uno a uno tutti i permessi, ma, se rinunciamo a questa possibilità, una infinità di dati relativi alla nostra navigazione online, alle nostre preferenze, abitudini e acquisti possono essere condivise da terze parti sconosciute. È come se affiggessimo alle nostre finestre i nostri scontrini, le liste della spesa ed esponessimo a tutti gli acquisti che abbiamo fatto. Nel mondo reale ci sembra un'assurdità ma lo è anche in quello digitale, anche se le modalità in cui si realizza sono diverse.
- Condividere il minor numero possibile di dati personali sul nostro profilo per impedire ai criminali di rubare la nostra identità: se pubblichiamo la data di nascita, l'indirizzo e il numero di telefono e, magari quando partiamo per le vacanze, postiamo la foto del biglietto aereo, abbiamo dato ai criminali una esatta informazione per venire a rubare indisturbati in casa nostra.
- Aggiornare regolarmente le app e il software di sistema: ci può apparire noioso interrompere la nostra attività online per aggiornare l'applicazione quando ci arriva la notifica, o magari rimandiamo perché stiamo facendo altro, ma l'aggiornamento costante evita di lasciare aperte falle (i cosiddetti bug) che potrebbero facilitare l'accesso a cybercriminali.
- Utilizzare password uniche e sicure: la password più gettonate sono il nome dei figli, del gatto o del cane, la data di nascita e, prima fra tutte, 1234… Queste password possono essere facilmente indovinate se abbiamo postato la foto di compleanno di nostro figlio, con il suo nome ovviamente, o quella del gatto o abbiamo reso pubblica la nostra data di nascita. La password deve essere complessa per evitare al cybercriminale di accedere facilmente ai nostri account, ma non va memorizzata in chiaro, magari sul mitico post-it in bella vista. Esistono app che gestiscono tutte le password, per cui

diventa sufficiente ricordarne solo una, quella dell'app (e diventa indispensabile non dimenticarla).
- Utilizzare l'autenticazione a due fattori, quando possibile (ad esempio per accedere alla posta elettronica o al conto in banca): questa tecnica si basa sul fatto che l'autenticazione avviene su una cosa che sappiamo (un pin o una password) e una cosa che siamo (per esempio l'impronta digitale) o che abbiamo, generalmente il cellulare che abbiamo autorizzato per quel servizio e su cui ci arriva il cosiddetto token o OTP (One Time Password, la password che si usa una volta sola) che nessun altro può conoscere perché esiste solo sul nostro telefono.
- Utilizzare una rete privata virtuale (VPN), specialmente quando ci connettiamo a una rete WiFi pubblica: esistono tecniche per intercettare i dati che viaggiano sulle reti Wi-Fi non protette. L'uso di una VPN (Virtual Private Network) garantisce la cifratura di tutta la comunicazione, così che nessun malintenzionato che stia spiando il traffico può leggere niente di ciò che inviamo.
- Non effettuare mai operazioni finanziarie quando siamo connessi a siti non sicuri, cioè quelli che non hanno il simbolo del lucchetto nella barra dell'indirizzo.

In generale è utile applicare le cautele di cybersecurity di base ed essere sempre attenti e ragionevolmente diffidenti, come nella vita "reale".

8.4 L'identità digitale degli altri

Come gli altri si fanno di noi un'idea in base a quello che facciamo o pubblichiamo in Rete, così noi possiamo farci un'idea dei soggetti che frequentiamo in Rete. Questo esercizio è molto utile quando veniamo contattati da persone sconosciute: prima di accettare un collegamento è bene studiare i loro profili, verificare che siano veri e poi capire se i contenuti che pubblicano, i commenti che fanno, le idee che manifestano sono coerenti con le nostre, con il nostro modo di affrontare le situazioni, per non rischiare di trovarsi coinvolti in situazioni spiacevoli. Può essere una scelta quella di frequentare profili "lontani" dal nostro ma deve essere consapevole, come quando decidiamo di frequentare persone che ci sono poco affini ma magari, per qualche motivo ci interessano.

8.4.1 L'identità digitale è reale

Spesso di fronte a un account, a un profilo, ci dimentichiamo che dietro quell'account (quasi certamente) c'è una persona "vera" con tutte le implicazioni connesse: una persona che ha la sua dignità, la sua reputazione, il suo orgoglio e quindi dobbiamo rapportarci a lei come faremmo nel mondo reale, con educazione, con rispetto, con gentilezza.

Purtroppo, accade spesso, invece, che nell'interazione con le persone attraverso la Rete cadano molti freni, molte riserve e dimentichiamo che quello che diciamo o scriviamo può offendere o ferire chi è dall'altra parte, come se fosse un'entità impersonale ed eterea.
Questo può portare al diffondersi di fenomeni violenti, come ad esempio:

- L'odio in Rete: si arriva ad insultare una persona, usando termini, comportamenti e parole che probabilmente in un confronto diretto, "in presenza" non useremmo. Ciò di cui non si tiene conto è che la diffamazione, l'offesa, il vilipendio e via dicendo sono reati tanto online che offline. A maggior ragione se l'odio è manifestato con intenti di discriminazione razziale o di religione o omofobi.
- Il body shaming: quante volte assistiamo in Rete a offese, insulti e prese in giro ad alcune persone per il loro aspetto fisico, in qualche modo sbagliato o sgradevole secondo i nostri canoni? Le persone che ne sono bersaglio ne soffrono tanto quanto se le stesse offese e insulti le ricevessero "di persona", con l'aggravante che online la quantità può diventare incontrollata e incontrollabile, andando a compromettere l'equilibrio psicologico della vittima.
- Il (cyber)bullismo: non può mancare nell'elenco di comportamenti violenti contro le persone. È tanto più grave perché di solito è rivolto a bambini e ragazzi più vulnerabili e indifesi rispetto agli adulti, proprio a causa della giovane età e della mancanza di esperienza. Il termine "cyber" è tra parentesi perché questi comportamenti non sono che l'evoluzione del "vecchio" bullismo praticato di persona maggiormente nei decenni passati (ma mai scomparso), solo che oggi viene amplificato dalla Rete e reca più danni alle vittime.

In tutti questi casi (e in altri simili, l'elenco potrebbe continuare) si tratta di offese verso una persona con la sua identità digitale e reale e molti di questi comportamenti, soprattutto se ripetuti e esasperati, costituiscono un reato. Qualunque sia l'aspetto di chi abbiamo davanti in Rete o le sue convinzioni bisogna sempre comportarsi secondo le regole del "vivere civile" alla base delle quali c'è prima di tutto il rispetto dell'altro. Questa dimensione è spesso sottovalutata non solo dai ragazzi, forse più inesperti e impulsivi, ma anche da molti adulti. Tutti si sentono in qualche modo "protetti" dalla tastiera, come se questa potesse garantirgli anonimato e impunità.
In alcuni casi chi ha questi comportamenti, quando si rende conto delle conseguenze (magari penali) in cui può incorrere prova a cancellare il commento o il post, ma quasi sempre questi "riaffiorano" dai computer di qualcuno che ha fotografato lo schermo e che ripubblica tutto, perché la Rete non dimentica.

8.5 Scheda didattica - *scuole secondarie di primo grado*

Titolo attività	**Identità digitale e web reputation**
Obiettivo	Avere consapevolezza della propria presenza in Rete e dei suoi effetti nella vita reale
Descrizione attività	- Cercare se stessi in Rete e verificare le notizie che appaiono su di noi, confrontandole con i fatti "reali" e cercando di capire perché appaiono certe informazioni, soprattutto se ci sorprendono. - Analizzare reciprocamente i risultati in un piccolo gruppo. - Scrivere alcune regole per gestire correttamente la propria identità online. - Produzione di un documento finale, sintesi delle attività dei gruppi
Documentazione fornita	Nessuna perché si tratta solo di fare una ricerca
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 4
Contenuti propedeutici in ingresso	- Definizione di Identità digitale e web reputation. - Tecniche per costruire la propria presenza online. - Rischi per il furto della propria identità e per la possibilità che quella dei nostri interlocutori sia falsa.
Conoscenze / Competenze / abilità in uscita	- Capacità di valutare e analizzare la propria presenza online. - Capacità di valutare i segnali di una possibile falsa identità di un interlocutore. - Ricadute della presenza online sulla vita "offline".
Documentazione di supporto aggiuntiva (URL o allegati)	Cos'è l'Identità Digitale e perché è importante per cittadini e imprese (EP 1).

9 Comunicazione digitale

Samanta Fumagalli

Quando parliamo di comunicazione digitale ci riferiamo a qualsiasi contenuto testuale, visivo o audio che viene prodotto con le tecnologie digitali (Pc, tablet, smartphone ecc.) e diffuso tramite web. Ciò che distingue la comunicazione analogica o tradizionale da quella digitale è il mezzo: il digitale.
I contenuti digitali possono essere testi (post sui social network, articoli di un blog o di un magazine online, email), immagini (foto su Instagram o Facebook), video (contenuti visivi pubblicati su Youtube o TikTok), audio (podcast).

La comunicazione digitale differisce dalla comunicazione tradizionale perché è inclusiva (chiunque può comunicare digitalmente) e bidirezionale (il ricevente partecipa attivamente interagendo con il mittente).
Ogni volta che produciamo un contenuto digitale lasciamo una traccia sul web, composta dalla serie di dati memorizzati derivanti da tutte le nostre attività online. Più consistente è l'uso che viene fatto di Internet, più ampia sarà l'impronta digitale (digital footprint) che lasciamo sul web. E di pari passo aumenterà anche il rischio correlato alla sicurezza dei nostri dati.

9.1 La Netiquette

In Rete esiste un cosiddetto galateo di Internet che prende il nome di "Netiquette"[4]. Si tratta di un neologismo che nasce dall'unione del termine inglese "net" (Rete) e del termine francese "etiquette" (buona educazione) e racchiude le regole di condotta per comunicare in Internet in modo rispettoso e appropriato, un insieme di norme non scritte che ci aiutano a rispettare gli altri.
Si tratta di regole di buon senso, che dovrebbero essere adottate anche nella vita "analogica". Vediamone alcune:

- evitare di scrivere usando solo lettere maiuscole perché può essere percepita come una comunicazione aggressiva: viene ritenuto equivalente a urlare qualcosa nella vita reale;
- richiedere il permesso di condividere foto o materiale in cui sono presenti anche altre persone;
- non usare termini offensivi;
- dichiarare la fonte quando si condividono contenuti realizzati da altri, possibilmente inserendo il link al contenuto originale;
- evitare le catene di Sant'Antonio;

[4] Il galateo di Internet | Comunicazione e linguaggio | Videopillola (Fonte: Telefono Azzurro) https://www.youtube.com/watch?v=vxqoofKdAlo

- evitare qualsiasi forma di bullismo digitale;
- non violare il copyright dei contenuti fruibili in Rete.

9.2 Un linguaggio nuovo: il gergo di Internet

La comunicazione digitale ha rivoluzionato il nostro linguaggio, introducendo nuovi termini e nuovi slang. Gli adolescenti prendono in prestito moltissime parole e acronimi dall'inglese americano, la vera culla dello slang di Internet, come le espressioni LOL (per esprimere divertimento - significa "laughing out loud", cioè "ridere rumorosamente" oppure "tante risate", se si intende "lot of laughs"), OMG (che sta per Oh My God, per esprimere stupore), BRO (abbreviazione di "brother") o BTW (abbreviazione di by the way, "a proposito"). La principale finalità di questo nuovo gergo giovanile di Internet non è quella di diffonderlo al resto della popolazione, anzi, è vero il contrario. Lo slang e i neologismi dei giovani nascono innanzitutto per differenziarsi dalla massa, per esprimere l'appartenenza a un gruppo selezionato, una cerchia ristretta da cui sono esclusi gli adulti, definiti "boomer".

Conoscere questi termini significa comprendere le conversazioni dei ragazzi, avvicinarci a loro, e in alcuni casi intercettare sigle e termini che i giovanissimi utilizzano appositamente per non farsi capire dai genitori o che hanno un significato legato ad ambiti intimi o illegali, come sesso e droga. Vediamone alcuni: KPC (Keep Parents Clueless, significa non dirlo ai tuoi genitori), NEK (dall'inglese neck, collo, è inteso come il collo della bottiglia ed è legato alle sfide online in cui un ragazzo ne nomina un altro sfidandolo a bere grandi quantità di alcol mentre viene ripreso), RU/18 (Are you 18, sigla utilizzata per chiedere all'altra persona se è maggiorenne… spesso dall'altra parte dello schermo potrebbe esserci un malintenzionato). Conoscere questi termini e sigle può aiutare gli adulti a individuare e intuire situazioni di pericolo.

9.3 Strumenti di messaggistica

WhatsApp, Facebook, Messenger, Instagram, Snapchat, Telegram, Signal, Skype, Slack, e anche i semplici SMS sono alcuni degli strumenti di messaggistica digitale più utilizzati a cui si aggiungono le chat dei videogiochi online come Twitch e Discord. Dai dati delle rilevazioni Audiweb di Nielsen su un'audience di età compresa tra i 18 e i 74 anni emerge che in Italia WhatsApp è leader indiscusso tra le app di messaggistica, seguito da Facebook Messenger e Telegram. Discord è in crescita grazie al popolo dei videogamer.
Ma i messaggi di testo e le foto e i video che inviamo e riceviamo sono al sicuro? Possono essere intercettati da malintenzionati? Quali di queste app sono le più sicure?
Gli esperti di sicurezza sono d'accordo nel considerare Signal come l'app di messaggistica più sicura, anche se oggi tutti i sistemi di Instant Messaging implementano nativamente la crittografia end-to-end ("da un estremo all'altro") che indica un

sistema di comunicazione cifrata nel quale solo le persone che stanno comunicando (mittente e destinatario) possono leggere i messaggi. I messaggi inviati vengono crittografati con la chiave pubblica e possono essere aperti solo da chi possiede la chiave privata. Tutti gli altri, comprese le società sviluppatrici dell'app, vedranno contenuti indecifrabili. Serve a impedire l'attacco "man in the middle" (MITM) che mira a rubare dati e informazioni personali, intercettando "in the middle" la comunicazione tra due utenti.

Ma non è l'unico metodo per proteggere i propri messaggi dagli hacker. Le app di messaggistica hanno infatti funzionalità studiate appositamente per garantire maggiore sicurezza. Ci sono app che permettono di impostare i messaggi in modo tale che trascorso un certo periodo di tempo si autodistruggono; altre consentono l'invio di messaggi in forma anonima.

Discorso a parte meritano i metadati, quindi tutte le informazioni che non sono "testi, video o foto" ma dati che registrano le nostre attività: ad esempio, quando scattiamo una foto con lo smartphone vengono registrati dati quali il luogo e l'ora dello scatto, il nome del dispositivo utilizzato, l'apertura del diaframma, ecc. Se parliamo di un messaggio, i metadati sono la data e l'ora di invio, il numero di telefono del mittente e del destinatario, la localizzazione di mittente e destinatario, ecc. I metadati fanno parte dell'impronta digitale che lasciamo sul web e possono fornire a un soggetto terzo informazioni importanti per profilarci. La gestione dei metadati è molto diversa tra le varie applicazioni di messaggistica, con scelte che possono penalizzare la sicurezza per avvantaggiare la praticità d'uso.
Quindi, il suggerimento è verificare nelle impostazioni delle app utilizzate quali funzionalità di sicurezza sono già attivate di default e quali devono essere attivate dall'utente. In ogni caso la sicurezza totale non esiste. Una persona che riceve un messaggio, foto o video, potrebbe fare uno screenshot e tutte le precauzioni prese dal mittente non hanno più alcuna efficacia. Importante è quindi fare sempre un uso consapevole di questi strumenti.

9.4 Parole_Ostili

Comunicare online richiede responsabilità. La scelta delle parole online è ancora più importante che nella lingua parlata per l'eco e la diffusione che possono avere.

Uno strumento educativo per un uso responsabile delle parole in Rete è il *Manifesto della comunicazione non ostile*[5], creato dall'associazione no-profit Parole O_Stili. Come si legge sul sito https://paroleostili.it si tratta di "Un progetto sociale di sensibilizzazione contro la violenza delle parole". Il Manifesto elenca dieci principi utili

[5] Video del Manifesto Parole Ostili: https://youtu.be/QATKI1I-79Y

a migliorare lo stile e il comportamento di chi sta in Rete, invitando a "scegliere le parole con cura e la consapevolezza che le parole sono importanti".

Le parole e le azioni in Rete hanno un peso e, una volta pubblicate, sono difficilmente cancellabili. Con l'avvento di Internet e degli smartphone in particolare ognuno di noi si è creato una identità digitale online e se c'è chi ne fa buon uso, c'è anche chi la usa per dare libero sfogo alle proprie insicurezze riempiendo social e chat di parole d'odio, violente, offensive e spesso diffamatorie.
Questi comportamenti "ostili" sono passibili di condanne. Le più recenti sentenze della Corte di Cassazione che si sono succedute negli ultimi anni hanno rilevato quanto i social network siano mezzi idonei per realizzare la pubblicizzazione e la circolazione, tra un numero indeterminato di soggetti, di commenti, opinioni e informazioni, che, se offensivi, comportano l'integrazione del reato di diffamazione, aggravata dall'utilizzo di un mezzo di pubblicità.

L'azione più naturale di tutte, cioè l'esprimere un proprio pensiero o una propria opinione, racchiude quindi insidie e conseguenze: occorre prestare attenzione quando si pubblica un commento o un post online e usare il buon senso.

9.5 WhatsApp

Lo strumento di messaggistica più usato al mondo (e anche in Italia) per comunicare è WhatsApp. Semplice, immediato, a prova di boomer, lo usano anche le persone più anziane.

Nella sezione "Informazioni sull'età minima per usare WhatsApp" si legge che "Chi risiede in un Paese dello Spazio economico europeo (che include l'Unione europea) e in qualsiasi altro Paese o territorio incluso (collettivamente Regione europea) deve avere almeno 16 anni (o un'età superiore in base ai requisiti per il suo Paese) per registrarsi e utilizzare WhatsApp. Chi risiede in un Paese diverso da quelli inclusi nella Regione europea deve avere almeno 13 anni (o un'età superiore in base ai requisiti per il suo Paese) per registrarsi e utilizzare WhatsApp."
Quindi, in Italia, l'utilizzo di WhatsApp non è consentito ai minori di 16 anni. Esiste però nelle clausole di Whatsapp la possibilità che prevede che i genitori si assumano la responsabilità e forniscano il consenso al trattamento dei dati personali del minore se il figlio/a ha meno di 16 anni.
Ma quali rischi si corrono usando WhatsApp? A cosa bisogna prestare attenzione?
Anche WhatsApp, come tutti gli strumenti di messaggistica e chat online, va usato con consapevolezza e buon senso. Esistono diversi comportamenti che sono vietati, alcuni possono sfociare in un reato:

- Divieto di inviare messaggi di natura razzista, offensiva, minacciosa, diffamatoria (anche tramite stickers)

- Divieto di perseguitare una persona con messaggi continui (stalking)
- Divieto di offendere insegnanti, professori, istruttori nei gruppi di WhatsApp (diffamazione)
- Divieto di pubblicare foto altrui in gruppi di WhatsApp senza il consenso dell'interessato
- Divieto di inserire una persona in un Gruppo WhatsApp senza il suo consenso

Un approfondimento più puntuale va fatto per i casi di sexting e di cyberbullismo, troppo frequenti su WhatsApp.

Sexting deriva alla fusione delle parole inglesi sex (sesso) e texting (inviare messaggi elettronici): è un termine utilizzato per indicare l'invio di messaggi, testi, video, immagini sessualmente espliciti, principalmente tramite il telefono cellulare o tramite internet. In breve, ogni volta che una persona condivide con altri utenti contenuti sessualmente espliciti (propri o che ritraggono altri individui) sta facendo sexting.
Il sexting in quanto tale non è reato, ma lo diventa quando coinvolge minori (pedopornografia) e/o la condivisione avviene senza il consenso del diretto interessato. Si arriva poi ai casi di **sextorsion** quando ne segue un'estorsione di denaro mediante il ricatto, basata sulla minaccia di diffusione dei contenuti a sfondo sessuale. Si parla invece di **revenge porn** quando i contenuti sessualmente espliciti vengono diffusi da parte di ex partner a scopo diffamatorio.

Come proteggersi da questi fenomeni?
Sul sito del Garante della Privacy si legge che "la prima e più importante forma di difesa sono sempre la consapevolezza e la prudenza". Ricordiamo che nel momento in cui una foto o un video lascia il proprio telefono e raggiunge quello di un'altra persona, se ne perde il controllo. Anche se inizialmente questo tipo di attività può nascere da intenzioni innocue, può ritorcersi contro in futuro.
Questo tipo di contenuti però possono anche essere sottratti dai nostri dispositivi e usati per ricattarci. Per proteggere i dati personali presenti nei dispositivi (smartphone, pc o tablet) occorre utilizzare sempre adeguate misure di sicurezza: ad esempio, password che proteggono i dispositivi e/o le cartelle in cui sono conservati i file, sistemi di crittografia per rendere illeggibili i file agli altri, sistemi antivirus e dove possibile l'autenticazione multi-fattore.
È importante sottolineare che anche chi riceve foto e immagini a contenuto sessualmente esplicito che riguardano altre persone e le ricondivide diventa complice di comportamenti illeciti nei confronti di quelle stesse persone: quindi, se si ricevono, non vanno diffuse ma cancellate ed eventualmente si può fare una segnalazione alla Polizia postale (https://www.commissariatodips.it/).

Il **cyberbullismo** è un altro fenomeno che si verifica con frequenza nella chat di gruppo su WhatsApp. Il primo passo per chi ne è vittima è non subire in silenzio questa violenza psicologica, ma reagire parlandone con persone di fiducia: un adulto, un amico, un professore o un referente del cyberbullismo a scuola. Si può anche ricorrere alla denuncia alle autorità. Se nella chat WhatsApp di classe si verificano episodi di cyberbullismo, anche chi è a conoscenza (ossia tutti coloro che sono nella chat) ha il dovere di denunciare e segnalare ciò che sta accadendo.

Su WhatsApp valgono poi alcune regole di base che valgono in generale su Internet: occorre prestare attenzione alle informazioni personali che condividiamo, a chi accettiamo come contatto, alle truffe (phishing) e ai virus e ai malware, sempre più diffusi tramite questi strumenti di messaggistica.

9.6 Gestione del tempo e relazioni personali

Se il progresso tecnologico da un lato ha permesso di comunicare di più e più velocemente, fornendo mezzi e maggiori opportunità per entrare in contatto "virtuale" con altre persone, dall'altro ha creato sempre più distanza "fisica" tra le persone. Questo sta generando, soprattutto nelle giovani generazioni, un isolamento sociale, a causa di una riduzione delle relazioni personali, fino a sfociare nei casi più gravi nel fenomeno chiamato "hikikomori" (dal giapponese "stare in disparte"). Con questo termine si fa riferimento a giovani di età compresa tra i 14 e i 30 anni che passano molto del proprio tempo davanti alla tv e ai videogiochi riducendo lo spazio dedicato alle relazioni interpersonali, spesso sottraendo ore al sonno o invertendo il ritmo sonno-veglia, fino a interrompere qualsiasi altra attività, che sia il percorso di studi o il lavoro. Tutto il loro mondo inizia e finisce all'interno della loro stanza, evitando qualsiasi contatto con il mondo esterno, a volte anche con i familiari.

La dipendenza dal digitale, ossia l'incapacità di moderare l'uso che una persona fa di Internet o di altri dispositivi digitali, è una tendenza che riguarda sia i giovani adolescenti, che i preadolescenti e i bambini in età prescolare. Il mondo adulto deve prestare attenzione a questi comportamenti cercando di ristabilire un sano equilibrio tra vita online e vita offline, proponendo ai ragazzi attività diversificate: lo sport in questo aiuta molto, favorendo non solo le relazioni ma anche un sano sviluppo fisico e psicomotorio; anche attività che prevedono di trascorrere tempo all'aria aperta o attività manuali (l'offerta di laboratori è vastissima) o momenti di incontro con amici o di studio con i compagni di scuola sono attività che possono aiutare a ristabilire un sano equilibrio tra vita reale e vita virtuale.

Anche la tecnologia può venire in aiuto: esistono applicazioni che permettono di rilevare la quantità di tempo trascorsa online, mostrando quali sono le attività che assorbono l'attenzione del ragazzo. L'utilizzo di queste applicazioni consente di

tracciare le abitudini digitali così da poter intervenire per modificare un comportamento che sta causando disagi al ragazzo o alla ragazza.

9.7 Regole condivise in famiglia

Abbiamo visto come la comunicazione digitale sia ormai parte integrante della nostra vita. Offre innumerevoli opportunità - nello studio, nel lavoro e in generale nella vita quotidiana - ma anche rischi, sia per quanto riguarda la sicurezza dei dati e dell'identità digitale che per quanto riguarda la salute psico-fisica.

In famiglia, per far sì che sulla bilancia dei "rischi/benefici" il peso maggiore sia sul piatto dei "benefici" occorre lavorare in squadra e stabilire alcune regole condivise che sia i genitori che i ragazzi dovranno osservare.

Ogni famiglia stabilirà le sue regole che dovranno essere condivise, ben visibili e molto chiare a tutti i componenti della famiglia. La "gamification" in questo caso può aiutare molto: assegnare delle stelline o dei punteggi a chi rispetta ogni regola quotidianamente permetterà di stabilire ogni fine mese chi sarà il vincitore e stimolerà l'osservanza di queste regole.

Da dove partire? Ecco qualche regola a cui se ne possono aggiungere molte altre.

- A tavola non si usano i dispositivi digitali (smartphone, tablet, ecc).
- Prima di andare a letto, lasciare il telefono fuori dalla camera.
- Stabilire una mezza giornata "senza cellulari".
- Niente cellulari mentre si fanno i compiti (se non per uso di ricerca).
- Attivare insieme le impostazioni di sicurezza sui dispositivi e sui profili di nuove app/giochi scaricati.
- Condividere almeno una esperienza che si è avuta online nella giornata.

9.8 Scheda didattica - *classi medie*

Regole condivise per il gruppo WhatsApp di classe

Titolo attività	**Scriviamo la Netiquette del gruppo WhatsApp di classe**
Obiettivo	Creare un elenco di regole che ogni studente deve rispettare nella chat WhatsApp di classe
Descrizione attività	La classe viene suddivisa in gruppi di 3 o 5 persone. Ogni gruppo scrive 8 regole per una corretta comunicazione sul gruppo WhatsApp di classe (focalizzando l'attenzione su ciò che non va fatto). In tutto 8 Post It che verranno attaccati sul foglio grande fornito a ogni gruppo in ordine di importanza. Ogni gruppo inventa anche 1 titolo da dare a questo elenco di regole. Quando tutti i gruppi hanno terminato, ogni gruppo presenta alla classe le regole che ha inventato. Il "Galateo" del gruppo WhatsApp dell'intera classe verrà formato dalle regole più votate dall'intera classe: se tutti i gruppi o la maggior parte hanno scritto la stessa regola, quella andrà sicuramente nell'elenco finale. Per le altre si procede con la votazione della classe. Al termine l'elenco finale di regole, che avrà il "titolo" più votato dalla classe, verrà appeso in classe e verrà eletto un responsabile del gruppo WhatsApp – un Garante - che ogni settimana, a turno, dovrà richiamare all'ordine chi non rispetta le regole.
Documentazione fornita	Un foglio grande bianco e Post It (possibilmente grandi) oppure strisce di carta che si possano attaccare e staccare
Strumentazione necessaria (HW/SW)	Nessuna in particolare
Impegno (durata stimata)	1/2 ora
Tipologia	Attività di gruppo - Min partecipanti: 3 - Max partecipanti: 5

Contenuti propedeutici in ingresso	- Strumenti di messaggistica e rischi online. - WhatsApp: semplice, immediato, ma sappiamo cosa è vietato fare? - Cyberbullismo: cosa fare se per fermarlo? - Regole di sicurezza sulla condivisione di contenuti digitali.
Conoscenze / Competenze / abilità in uscita	- Conoscenza delle regole di comunicazione e sicurezza sugli strumenti di messaggistica online (e su Internet in generale). - Conoscenza dei comportamenti vietati su WhatsApp. - Capacità di identificare un episodio di cyberbullismo e di denunciarlo. - Conoscenza delle regole per esprimersi online nel rispetto dell'altro.
Documentazione di supporto aggiuntiva (URL o allegati)	- Il Manifesto di Parole Ostili: https://youtu.be/QATKI1I-79Y - Netiquette: Il galateo di Internet (Fonte: Telefono Azzurro) https://www.youtube.com/watch?v=vxqoofKdAIo

10 Disinformazione: non è vero, ma ci credo?

Sonia Montegiove

È davvero necessario oggi difendersi dalle cosiddette fake news, ovvero dalle notizie false che circolano in Rete? È doveroso accompagnare ragazze e ragazzi nel costruire nel migliore dei modi possibili la propria "dieta informativa", ovvero nello scegliere le notizie che consentano loro di informarsi nel modo corretto? La risposta è sicuramente sì, soprattutto se pensiamo non solo all'abbondanza delle notizie disponibili, ma al fatto che quasi mai scegliamo noi cosa leggere, visto che a farlo ci pensano gli algoritmi dei social network che consultiamo in ogni istante della giornata. Come scrive Kevin Kelly, in "L'inevitabile", "la vastità della "Biblioteca del Tutto" travolge velocemente le nostre consuetudini limitate e le nostre abitudini logoranti; ci serve un aiuto per districarci in questa matassa. La vita è breve e ci sono troppi libri da leggere: qualcuno o qualcosa deve scegliere, o bisbigliarci alle orecchie per aiutarci nella decisione. Abbiamo bisogno di un metodo di smistamento, e la nostra unica scelta è farci assistere nel prendere decisioni".

Il problema, pertanto, non è certo l'abbondanza dell'informazione, come qualcuno a volte afferma. Il problema è il dovere e saper scegliere in autonomia in mezzo a tanta abbondanza le cose di qualità, affidabili, curate, correttamente elaborate, che consentono di farci crescere dal punto di vista culturale e professionale. Come sottolinea il rapporto AgCom "L'informazione alla prova dei giovani" del 2020" in sostanza, vi è un paradosso: internet si presenta potenzialmente capace di assicurare l'auspicato pluralismo informativo, in virtù dell'attitudine a diffondere e aggregare idee/orientamenti diversi, a stimolare il confronto, il dibattito e l'apertura mentale; dall'altra parte, vi sono forze che a contrario tendono a chiudere i cittadini all'interno di ambienti chiusi, spesso, popolati da informazioni manipolate, false, o comunque di bassa qualità".

10.1 Cos'è una fake news?

Volendo partire dalla definizione, Treccani descrive le fake news così: "locuzione inglese, entrata in uso nel primo decennio del XXI secolo per designare un'informazione in parte o del tutto non corrispondente al vero, divulgata intenzionalmente o inintenzionalmente attraverso il Web, i media o le tecnologie digitali di comunicazione, e caratterizzata da un'apparente plausibilità, quest'ultima alimentata da un sistema distorto di aspettative dell'opinione pubblica e da un'amplificazione dei pregiudizi che ne sono alla base, ciò che ne agevola la condivisione e la diffusione pur in assenza di una verifica delle fonti".
Se è vero che il termine è stato coniato di recente, è altrettanto vero che le notizie false non nascono certo con Internet. Sappiamo tutti, infatti, quanto antiche possa-

no essere le “fake news” e quanto la disinformazione sia stata utilizzata nella storia per cercare di spostare l’opinione pubblica, fin dai tempi più antichi. È sbagliato pensare che la disinformazione nasca con Internet. La Rete e i social media sono solo un potente strumento di diffusione, indispensabili per raggiungere una grande quantità di persone in tempi molto rapidi. Non per questo si devono demonizzare Internet o i social network. Come sottolinea Francesco Nicodemo in “Disinformazia, la comunicazione al tempo dei social media”, “Disinformazione e cattiva informazione, bufale e complottismo, notizie inesatte, incomplete e strumentalizzate sono perennemente in agguato sulla rete e rischiano di scorrerci davanti agli occhi come palline impazzite di un flipper attivato dal meccanismo perverso del clickbaiting. Il fatto che navigare in rete sia diventata un’abitudine non deve farci perdere di vista i suoi innumerevoli pericoli, ma anche le sue potenzialità, in parte ancora inespresse e inesplorate”. Per poter massimizzare le potenzialità e minimizzare i rischi, è importante tornare al punto di partenza di questa breve riflessione sulla disinformazione: servono conoscenze e competenze digitali che aiutano a sciogliere la complessità e utilizzare al meglio le tante informazioni che abbiamo a disposizione in Rete.

Uno degli esperimenti che si possono fare in classe - come suggerito nelle schede didattiche - è sicuramente quello di cercare delle famose fake news storiche e analizzare il modo con cui queste sono state divulgate per confrontarlo con le possibilità che la Rete ci mette a disposizione oggi.

10.2 Perché la disinformazione può diventare pericolosa?

Il tema della diffusione delle fake news è ritenuto pericoloso anche per la democrazia, tanto da imporre una riflessione anche a livello europeo. Tra le iniziative proposte, per esempio, c’è quella della pubblicazione di uno spazio in cui raccogliere notizie false circa il ruolo e le opportunità legate al far parte dell’Unione Europa: la Rappresentanza in Italia della Commissione europea ha deciso di fare chiarezza pubblicando dati, fatti e informazioni che guidano le persone nel capire cosa è fake e cosa no.

Le fake news non sono da considerare qualcosa di divertente, di cui poter ridere o sorridere, visto che la diffusione della disinformazione è quasi sempre finalizzata a spostare l’opinione pubblica per ragioni di potere e quindi ragioni legate alla politica e all’economia. “La disinformazione minaccia il cuore delle nostre democrazie, ostacolando la capacità dei cittadini di prendere decisioni basate su fatti corretti. Per questo la Commissione Europea continua la sua azione di contrasto alla disinformazione tramite azioni di regolamentazione, sorveglianza e di promozione delle competenze digitali, e richiama tutti a fare la propria parte” - ha affermato qualche tempo fa Antonio Parenti, Direttore Rappresentanza Commissione Europea in Italia.

Visto che diversi studi dimostrano come i giovani (e non solo) sempre più si informino attraverso Internet e i social media, occorre una riflessione - come sottolinea il rapporto AgCom sull'informazione e i giovani - "sul ruolo delle piattaforme online (e dei relativi algoritmi), nell'indirizzare i ragazzi verso punti di vista nuovi ovvero verso fonti che confermano le loro convinzioni. È oramai dimostrato da una solida letteratura scientifica come l'uso dei social media sia spesso legato alla formazione di eco-chambers, ossia di gruppi chiusi che amplificano, attraverso una ripetitiva trasmissione e ritrasmissione (tramite post, condivisioni,...) di informazioni, idee o credenze più o meno veritiere, in cui visioni e interpretazioni divergenti finiscono per non trovare spazio né considerazione. Peraltro, questi processi di chiusura culturale e social(e) sfociano di frequente in fenomeni di incitamento all'odio (hate speech) nei confronti di soggetti portatori di idee, valori, culture, diverse".

Altro aspetto sul quale riflettere quello che disinformazione, cattiva e falsa informazione potrebbero diffondersi con ancora maggiore velocità e potenza grazie alla diffusione del Large Language Modeling, ovvero per esempio di chat basate su intelligenza artificiale generativa come ChatGPT di OpenAI o Bard di Google. Un invito, in questo senso, è arrivato dalla vicepresidente della Commissione europea Vera Jourova che, nel sottolineare come l'intelligenza artificiale ponga nuove sfide per la lotta alla disinformazione, ha invitato la grandi piattaforme online come Google, Meta, Microsoft, TikTok e altre società tecnologiche che hanno aderito all'accordo volontario sottoscritto nei Paesi UE sulla lotta alla disinformazione a creare tutele per impedire che "attori malintenzionati" generino disinformazione.

Uno studio pubblicato a giugno 2023 da Science rivela che la disinformazione generata dall'intelligenza artificiale potrebbe essere più convincente di quella prodotta dalle persone. La ricerca - che si è focalizzata sulla piattaforma Twitter - ha messo in evidenza che le persone avevano il 3% in meno di probabilità di individuare falsi tweet generati dal sistema di intelligenza artificiale GPT-3 rispetto a quelli scritti da esseri umani. Questa percentuale, apparentemente poco significativa, è preoccupante, in quanto la disinformazione generata dall'intelligenza artificiale è più economica e, pertanto, destinata a crescere - secondo lo stesso studio - in modo significativo nei prossimi anni.

10.3 Cosa serve nella lotta alle fake news?

Il contrasto alla disinformazione non può risolversi - purtroppo o per fortuna - solo attraverso la tecnologia o nuove leggi come a volte viene chiesto con forza: c'è bisogno di una grande consapevolezza e di un'operazione di diffusione dell'information literacy e di una cultura digitale che possa favorire un uso consapevole della Rete e dei social media. Se è vero che c'è bisogno di formazione, è anche vero che molto ce n'è bisogno a favore dei giovani: lo stesso report AgCom citato sopra, infatti,

mostra come a non saper distinguere una notizia vera da una falsa siano proprio le persone della fascia giovane 14-17 anni.

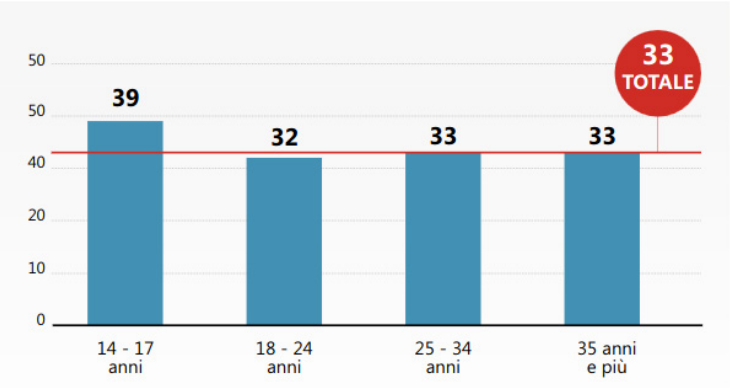


FIGURA 11.
Probabilità di scambiare notizie false per vere

Chi crede nelle fake news (dati in %)

"Se la disinformazione o la dispercezione - si legge nel documento AgCom - è per la società un "male" poiché fa diminuire la soddisfazione del consumatore, conduce a visioni distorte e, quindi, a decisioni non informate, il fenomeno è ancora più degno di attenzione quando interessa la popolazione giovanile, soprattutto i minori, per i quali le capacità cognitive sono, come detto, ancora in via di sviluppo".

Un manifesto di qualche anno fa, pubblicato dal Digital Transformation Institute, cercò di animare il dibattito proprio su questo punto: la disinformazione non si combatte con divieti o sanzioni o peggio ancora con la censura delle notizie, ma attraverso la formazione e l'educazione.

Alcuni dei punti contenuti in questo manifesto spiegano bene il fenomeno e individuano ciò che serve a contenerlo. Per esempio un punto particolarmente significativo è il terzo, dove si ricorda come l'istantaneità della condivisione batta la necessità della riflessione: con le fake news il coinvolgimento emotivo supera la dimensione dell'approfondimento ed enfatizza il meccanismo della post verità, ovvero quando sui social network leggo qualcosa di cui sono già convinto ci credo al di là che questo sia vero o meno.

Il quinto punto sottolinea come la censura delle fake news non solo sia inefficace, ma anche pericolosa per gli utenti, soprattutto se basata su meccanismi top down ovvero quando un unico soggetto (per esempio una piattaforma social) esercita un potere sulla scelta del cosa è utile leggere e cosa no, decidendo se una notizia è falsa e oscurandola. Questo punto fa riflettere su quanto sia invece indispensabile aiutare le persone a riconoscere la buona informazione e a sceglierla ogni giorno.

L'ultimo punto riprende un tema molto dibattuto: manca forse una legge ad hoc contro le fake news? Il manifesto ricorda che una norma da sola non risolverà il problema: servono cultura, educazione e consapevolezza degli utenti.

10.4 Consigli utili per individuare una fake news

Controllare le fonti. Il primo consiglio è vecchio come il mondo: dobbiamo ritrovare il piacere e il desiderio, oltre alla curiosità, di verificare l'attendibilità (e l'autorevolezza) delle fonti. Grazie alla disponibilità di tante fonti di informazione in Rete, nel momento in cui leggiamo una notizia abbiamo tutti gli strumenti per poter verificare da quale fonte proviene la notizia, mettere a confronto fonti differenti per capire se tutte stiano dando la stessa informazione e quale lettura stiano dando della cosa. In generale, non è mai consigliabile fermarsi alla prima cosa letta (o magari al primo titolo in cui inciampiamo consultando un social).

Controllare la data di pubblicazione. Prima di cedere alla fretta di condividere una certa notizia, è opportuno risalire alla data di pubblicazione. Una cosa semplice, sempre possibile in Internet e sui social. Se vogliamo banale, ma molto utile. Diversi sono i casi in cui le persone contribuiscono alla diffusione di cattiva informazione, scambiando per recente per esempio una notizia vecchia o che nel tempo si è dimostrata non vera.

Controllare l'URL. L'indirizzo di pubblicazione delle notizie a volte può rivelare molto del tipo di informazione data: esistono alcune finte testate giornalistiche, per esempio, che volutamente usano nomi simili a quelli di giornali conosciuti e ritenuti affidabili. È il caso del Fatto Quotidaino che richiama la nota testata giornalistica giocando sul fatto che, leggendo in fretta magari da smartphone, può sfuggirci una lettera di troppo contenuta nell'URL. Una selezione di finte testate che diffondono fake news è contenuta in Bufalopedia o in altri siti che fanno lavoro di debunking, andando a spiegare perché una certa notizia è una bufala per fare corretta informazione.

Controllare l'immagine associata alla notizia. È capitato spesso che a fare disinformazione non siano stati solo i testi delle notizie, ma anche le immagini associate, magari riferiti a fatti differenti rispetto a quanto raccontato. Per fare una verifica sulle immagini può essere sufficiente una ricerca per immagini sul motore di ricerca per capire dove una certa immagine è già stata pubblicata e a quale evento è stata associata. Esistono anche siti e servizi online che, data l'immagine, consentono di vederne la data in cui è stata scattata, la provenienza, ovvero i cosiddetti dati exif, dati associati che descrivono e caratterizzano la foto (latitudine e longitudine del posto in cui è scattata, tipo di device usato per lo scatto, dimensioni, ecc.). Altri strumenti ancora consentono in modo semplice di capire se una immagine è stata ritoccata o se sono stati aggiunti degli elementi: molte bufale sono state scoperte proprio grazie a semplici analisi come queste.

Ricorrere a tecniche OSINT. Alcuni dei consigli sopra descritti possono essere ricompresi in alcune tecniche OSINT, open source intelligence, ovvero ricerche di informazioni da fonte aperta, pubblica, consultabile a chiunque. Queste tecniche sono particolarmente efficaci anche per individuare la cattiva informazione, oltre che per allenarsi nell'usare in modo corretto e consapevole Internet e social.

Fare attenzione ai fake data. Quando leggiamo una notizia che riporta numeri, dati, molto spesso siamo portati a ritenere vero quanto leggiamo. "Il dato parla chiaro, i numeri parlano chiaro, i numeri non possono tradirci", pensiamo d'istinto. Eppure, non solo i numeri da soli non necessariamente possono darci informazioni, ma occorre avere una grande attenzione alla qualità di quei numeri. Da dove provengono? Qual è il campione di riferimento? Chi ha fatto una certa indagine e perché? Quanto sono attendibili e statisticamente significativi i numeri che stiamo leggendo? Queste sono le domande che tutti dovremmo farci. Stessa attenzione dovrebbe esserci anche nel caso dei grafici che a seconda di come sono realizzati possono indurre le persone a interpretare in modo distorto alcuni dati.

Avere un approccio critico, sempre. Ultimo, più importante consiglio che li racchiude tutti: dovremo fare attenzione ad avere un approccio critico all'informazione. Sempre, anche quando andiamo di fretta e vorremmo condividere una cosa che abbiamo visto e ci sembra curiosa. Soltanto in questo modo, dubitando, mettendo in discussione, approfondendo ci abitueremo a "mangiare" in modo migliore per informarci in modo sano, senza eccessi ed evitando "cibo" nocivo per la salute.

10.5 Cosa abbiamo capito?

- Dobbiamo sempre controllare la fonte. Mai fidarsi.
- Non dobbiamo cedere alla fretta di condividere una notizia prima di averla verificata.
- Dobbiamo leggere, leggere, leggere, consultando media e fonti differenti, per approfondire le nostre conoscenze.

10.6 Scheda didattica 1 - *scuole di ogni ordine e grado*

Titolo attività	**È una fake news?**
Obiettivo	Comprendere se una notizia sia o meno una fake news e, in caso negativo, descrivere il metodo usato per smascherare la notizia falsa
Descrizione attività	- Analizzare l'immagine ricevuta utilizzando strumenti online utili a verificarne l'attendibilità. - Descrivere in un documento o in una presentazione multimediale i metodi e gli strumenti utilizzati e lo scopo delle azioni intraprese. - Scrivere l'esito dell'analisi descrivendo perché una immagine risulta essere vera oppure falsa.
Documentazione fornita	Una immagine vera o fake (anche cercata online)
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 3
Contenuti propedeutici in ingresso	- Definizione di Fake news. - Le regole per riconoscere una Fake news. - Le regole per analizzare un'immagine e comprenderne l'autenticità.
Conoscenze / Competenze / abilità in uscita	- Capacità di distinguere un contenuto affidabile da una fake news. - Competenza di base nell'analisi delle immagini per determinarne l'autenticità. - Capacità di identificare una fonte.
Documentazione di supporto aggiuntiva (URL o allegati)	

10.7 Scheda didattica 2 - *scuole di ogni ordine e grado*

Titolo attività	**Cerca una fake news in Rete**
Obiettivo	Comprendere se una notizia sia o meno una fake news e, in caso negativo, fornire una stima motivata dell'attendibilità.
Descrizione attività	Cercare una notizia falsa in Rete, indicarla con un link e scrivere in un documento il metodo usato per individuarla e quello o quelli usati per avere certezza del fatto che sia una notizia fake.
Documentazione fornita	Una immagine vera o fake (anche cercata online)
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 3
Contenuti propedeutici in ingresso	- Definizione di Fake news. - Le regole per riconoscere una Fake news. - Le regole per analizzare un'immagine e comprenderne l'autenticità.
Conoscenze / Competenze / abilità in uscita	- Capacità di distinguere un contenuto affidabile da una fake news - Competenza di base nell'analisi delle immagini per determinarne l'autenticità - Capacità di identificare una fonte
Documentazione di supporto aggiuntiva (URL o allegati)	

10.8 Scheda didattica 3 - *scuole di ogni ordine e grado*

Titolo attività	**Cerca una notizia falsa quando Internet non c'era**
Obiettivo	Comprendere i diversi meccanismi di diffusione delle notizie false in momenti storici diversi.
Descrizione attività	- Cercare una notizia falsa che si è diffusa in momento storico precedente a quello in cui era presente Internet e i social network. - In un documento riportare la notizia e descrivere le modalità di diffusione per poi ipotizzare di poter disporre di Internet e social network e descrivere come si sarebbe potuta diffondere.
Documentazione fornita	Esempio di notizia falsa e degli effetti che ha prodotto
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 3
Contenuti propedeutici in ingresso	- Definizione di Fake news - Le regole per riconoscere una Fake news
Conoscenze / Competenze / abilità in uscita	- Capacità di distinguere un contenuto affidabile da una fake news. - Competenza di base nell'analisi delle immagini per determinarne l'autenticità. - Capacità di identificare una fonte.
Documentazione di supporto aggiuntiva (URL o allegati)	

11 Gaming online: rischi e opportunità

Manuela Santini

Il punto di partenza per comprendere il contesto di cui tratteremo nel presente capitolo è la definizione di "videogioco". I videogiochi sono "*opere audiovisive che simulano situazioni ambientate in mondi virtuali o reali di diversa natura e costruiti intorno a un percorso di base che si sviluppa in funzione dell'interazione ludica con uno o più giocatori*", essi "*possono essere fruiti mediante appositi dispositivi elettronici, computer o altri apparecchi, anche portatili e possono prevedere una fruizione online*". Questa è la definizione proposta dal Decreto Ingiuntivo del Ministro della Cultura (MiC) e Ministro dell'Economia e delle Finanze del 12 maggio 2021 REP 187 - "Disposizioni applicative in materia di credito di imposta per le imprese di produzione di videogiochi di cui all'articolo 15 della legge 14 novembre 2016, n.220".

[6]Come riportato nel documento "European Parliament resolution of 10 November 2022 on esports and video games"[7] nel 2020, l'industria europea dei videogiochi impiegava circa 98.000 persone, ma solo il 20% di esse erano donne. Ciò riflette uno squilibrio di genere e l'ingresso di un maggior numero di donne nell'industria dei videogame e negli esport[8] una priorità strategica.

L'industria dei videogiochi richiede una vasta gamma di competenze e know-how in scrittura, design, creazione artistica, sviluppo digitale, pubblicazione, distribuzione e localizzazione. I videogiochi rappresentano delle vere e proprie opere di proprietà intellettuale e la questione della proprietà e del controllo dell'IP[9] presenta sfide legali per streamer, sviluppatori, editori e detentori di contenuti terzi.

Il gaming online può quindi rappresentare un'opportunità economica per coloro che desiderano perseguire una carriera nel settore. Esistono professioni legate al gaming online come streamer, pro player, sviluppatori di giochi, animatori e commentatori. Attraverso piattaforme di streaming e tornei online, è possibile guadagnare denaro e costruire una reputazione nella comunità di gaming.

L'industria degli esports, come quella dei videogame, è in rapida crescita e offre numerose opportunità di carriera. Oltre ai giocatori professionisti, ci sono ruoli di supporto come allenatori, manager di squadra, organizzatori di eventi, commentatori,

---

6 D.I. MiC e MEF del 12 maggio 2021 REP 187 - "Disposizioni applicative in materia di credito di imposta per le imprese di produzione di videogiochi di cui all'articolo 15 della legge 14 novembre 2016, n.220" https://cinema.cultura.gov.it/cosa-facciamo/sostegni-economici/linee-di-sostegno/tax-credit/produzione-videogiochi/

7 Texts adopted - Esports and video games - Thursday, 10 November 2022 (europa.eu)

8 Videogiochi utilizzati nell'ambito professionistico dove i videogiocatori, gamer professionisti, sono considerati degli atleti che partecipano a tornei, sia in Italia che nel resto del mondo.

9 Intellectual Property

streamer e molti altri. Gli esports possono aprire porte per lavorare nell'industria dei giochi, dello streaming, del marketing e della produzione di contenuti digitali.
Nel medesimo documento viene riportato come la metà degli europei si considera videogiocatore, e quasi la metà di loro sono donne. L'età media dei videogiocatori in Europa è di 31,3 anni, e oltre il 70% dei giovani tra i 6 e i 24 anni nell'UE gioca ai videogiochi, anche se la maggioranza dei giocatori ha più di 18 anni.
Nonostante l'UE sia un attore importante nell'ecosistema dei videogiochi e degli esports , l'industria è dominata principalmente da attori extra-UE. Molti giochi europei vengono distribuiti in tutto il mondo attraverso piattaforme extra-UE che raccolgono dati personali dei propri utenti e che potrebbero non offrire le stesse garanzie di tutela richieste per le piattaforme UE.
Entrando più nel merito del fenomeno scopriamo che i videogiochi e gli esports utilizzano tecnologie avanzate come l'intelligenza artificiale e la realtà virtuale, dando vita a spazi virtuali alternativi come i metaversi dove è possibile vivere esperienze concrete in modo virtuali ma che si avvicinano a quelle reali.
"*La prima volta che giocai a un videogioco online provai una sensazione di pace e libertà. Trovai un luogo dove sfogarsi dalla rabbia e dalla tristezza e da tutte le emozioni negative che provai in quella giornata*" racconta una giovanissima giocatrice. "*Preferisco giocare online perché posso giocare con i miei amici che non vedo da tanto tempo, fare nuove amicizie, allenarmi e provare vite diverse con i role-play game*[10]."

Questa testimonianza evidenzia come i videogiochi possano offrire una piattaforma sociale, di connessione e di esplorazione per i giovani giocatori, oltre a essere una forma di intrattenimento.
Gli esports, in particolare, offrono diversi vantaggi sia per i giocatori che per la comunità in generale. Promuovono la competizione sana e stimolante tra i giocatori in cui è richiesta abilità, strategia, concentrazione e collaborazione di squadra. Richiedendo un elevato livello di pensiero strategico, risoluzione dei problemi in tempo reale e reattività, i giocatori si vedono costretti a prendere decisioni rapide e tattiche, migliorando così le loro abilità cognitive, come la pianificazione, l'analisi e la presa di decisioni sotto pressione. A questi si aggiungono soft skill come lavoro di squadra, leadership e la gestione dei conflitti.

Le competenze digitali acquisite dai gamer possono essere trasferite in altri ambiti, come l'istruzione, il lavoro e l'innovazione tecnologica.
In generale, i videogame online e gli esport promuovono lo sviluppo personale, le competenze sociali e le opportunità di carriera. Giocare online consente di osservare e interagire con i videogiocatori, conoscere nuove persone, creare un ambiente in

[10] Gioco di ruolo - Wikipedia

cui i giocatori condividono i propri valori e idee e sviluppare hard e soft skill come quelle viste precedentemente ma favoriscono anche l'apprendimento di nuove lingue o la creazione di neologismi.

11.1 Il linguaggio dei gamer

Il linguaggio dei gamer è in continua evoluzione e si adatta alle nuove tendenze e ai nuovi giochi. Si tratta di un gergo unico e specifico che comprende termini, abbreviazioni e acronimi che consente ai giocatori di connettersi, condividere esperienze e creare un senso di comunità all'interno del mondo del gaming.
Ad esempio, "GG" (Good Game) è un'espressione comune utilizzata per complimentarsi alla fine di una partita ed è indicativo di fair play e rispetto reciproco.
I gamer dimostrano spesso una grande creatività nel creare nuovi termini e modi di esprimersi. Possono modificare o combinare parole esistenti per adattarle al contesto del gioco o inventare nuovi termini per descrivere situazioni uniche o fenomeni di gioco.
Lo slang videoludico spesso incorpora termini e frasi derivate da giochi popolari. Ad esempio, "leeroy Jenkins" è un termine coniato da un video virale di World of Warcraft, che descrive un giocatore che si lancia senza pensarci in una situazione rischiosa.
Espressioni emotive come "OMG" (Oh My God) o "WTF" (What The F**k) sono utilizzati per esprimere sorpresa o incredulità ed espressioni tattiche per facilitare la comunicazione e il coordinamento tra i membri della squadra sono spesso oggetto di un linguaggio specifico utilizzato dai giocatori.
Purtroppo, il contesto e l'intenzione dietro l'uso di questi linguaggi possono variare. Alcuni termini, sebbene usati in modo scherzoso, possono essere indicativi di situazioni problematiche da monitorare. È il caso di "Noob", termine che indica un giocatore inesperto o poco abile. Questo termine potrebbe essere utilizzato per intimidire o denigrare altri giocatori e quindi essere indicativo di una situazione di bullismo o comportamento aggressivo.
L'uso frequente di linguaggi dispregiativi, aggressivi o dannosi potrebbe richiedere l'intervento di un adulto per promuovere un ambiente di gioco positivo e sicuro.
Oltre alla creazione di nuovi linguaggi, i giocatori sono noti per creare e condividere meme e inside jokes[11] all'interno delle comunità di gioco. Questi possono essere basati su eventi, personaggi o situazioni specifiche di un gioco e servono ad accrescere il senso di appartenenza e l'umorismo condiviso tra i giocatori.

11.2 Il comportamento dei gamer

Come in ogni comunità, esistono comportamenti che possono influenzare positivamente o negativamente l'esperienza di gioco degli altri.

[11] Inside joke - Wikipedia

Ad esempio è solito per un gamer avvisare gli altri giocatori che si sta allontanando dal gioco per un periodo di tempo, spesso per motivi personali tramite l'acronimo **AFK (Away From Keyboard)**. Tuttavia se un giocatore è spesso AFK, o utilizza questo termine come pretesto per evitare interazioni o responsabilità nel gioco di squadra, potrebbe essere motivo di monitoraggio per valutare il coinvolgimento o l'impegno del giocatore. La collaborazione e la coordinazione con gli altri membri del team per raggiungere obiettivi comuni (**Teamwork**), il rispetto delle regole e del codice etico del gioco (**Fair Play**) senza ricorrere a trucchi o scorciatoie non consentite (**Hacking/Cheating**) così come il mostrare un comportamento leale e rispettoso nei confronti degli avversari, anche in caso di sconfitta **(Sportsmanship)** sono infatti alcuni dei comportamenti che possono influenzare positivamente l'esperienza di gioco degli altri giocatori.

Purtroppo, ci sono anche fenomeni diffusi che minano l'esperienza di gioco e l'ambiente virtuale in cui i giocatori si ritrovano. Sono comportamenti che vanno oltre le semplici divergenze di opinione o di stile di gioco, ma che si manifestano attraverso l'uso di linguaggio offensivo, discriminatorio e provocatorio. Ne sono esempi i discorsi di odio (**Hate speech**) commenti razzisti, misogini, antisemiti e omofobi, che si propagano nelle chat, all'interno di forum e gruppi online. Accanto a queste forme di espressione negativa, si trovano anche altre pratiche dannose come il **Flaming**, l'invio di messaggi violenti e volgari per scatenare battaglie verbali, l'**Harassment**, ovvero l'invio ripetuto di messaggi offensivi e molesti a una persona specifica, il **Denigration**, che si manifesta attraverso la diffusione di pettegolezzi, calunnie e offese al fine di danneggiare la reputazione della vittima, e infine il **Trolling**, una pratica di disturbo che si materializza attraverso messaggi provocatori, irritanti, fuori tema o senza senso, con l'intento di disturbare o irritare gli altri giocatori. Questi comportamenti, purtroppo, sono molto comuni e richiedono l'attenzione di tutta la comunità dei giocatori per creare un ambiente di gioco sano, rispettoso e inclusivo.

Altro comportamento che può creare un ambiente di gioco tossico e danneggiare l'esperienza degli altri giocatori è il **Griefing**, che si riferisce all'atto intenzionale di disturbare, infastidire o danneggiare deliberatamente altri giocatori all'interno di un gioco tramite sabotaggio, uccisione ripetuta degli alleati o distruzione di oggetti di gioco. Il Griefing rientra a pieno titolo tra quei comportamenti che si distinguono per la loro intenzionalità nel causare danni e nel creare un clima di esclusione. Tra questi troviamo anche l'**Exclusion**, che consiste nell'escludere deliberatamente una persona da un gruppo online con l'obiettivo di suscitare in essa un sentimento di emarginazione.
Inoltre, ci sono pratiche come l'**Outing and Trickery**, che prevedono la pubblicazione e la diffusione di informazioni riservate e/o imbarazzanti estorte alla vittima con l'inganno, e il **Doxing**, che consiste nella diffusione pubblica via internet di dati

personali e sensibili a completare il quadro delle possibili dinamiche negative che possono essere essere viste come vere e proprie forme di bullismo online (cyberbullismo[12]).

11.3 I rischi del gaming online

Nel film "Ready Player One", diretto da Steven Spielberg, il protagonista Wade Watts, conosciuto all'interno del mondo virtuale di OASIS (acronimo di Ontologically Anthropocentric Sensory Immersive Simulation) con il nome di Parzival, descrive come i giocatori prendono parte a numerose attività per lavoro, istruzione e intrattenimento. In particolare cita tre espressioni "è qui che si conosce, che si fa amicizia", "è il mio migliore amico anche se non ci siamo mai incontrati nel mondo reale", "*perdere tutto vuol dire sclerare*" che ben si prestano a introdurre i rischi del gaming online.

Per poter giocare online è necessario creare un account, coppia ID Utente (username) e password, correlato di tutte quelle informazioni che, all'interno di un determinato sistema informatico, definiscono una persona fisica. Oltre all'account è necessario creare un avatar, cioè la "personificazione" di un'idea o di un tipo di persona che si vuole associare al proprio personaggio virtuale.

L'avatar può essere espressione di se stessi, e può fornire informazioni utili per identificare gli individui.

L'accesso ai dati personali può compromettere la privacy e la sicurezza dei giocatori con relative truffe e frodi con conseguente perdita di dati personali, informazioni finanziarie o accesso ai propri giochi.

Sono migliaia le applicazioni e i giochi gratuiti che recuperano a vario titolo informazioni sugli utenti, dalla navigazione alla posizione, dalle chiamate ai contatti, per poi monetizzare, grazie appunto alla vendita delle informazioni degli utenti.

I dati personali sono quindi la nuova moneta del mondo digitale e possono essere usati per comprare contenuti e servizi digitali. Tra questi vi possono essere contenuti premium o periodi di prova gratuiti che molte piattaforme offrono previo, appunto, inserimento di dati personali, come l'indirizzo email, l'età, o le preferenze di visualizzazione o acquisto.

Proprio perché i dati personali possono essere monetizzati, i tentativi di acquisizione di tali dati, anche fraudolenti, diventano un fenomeno diffuso per gli utilizzatori di internet, non solo durante la navigazione online ma anche durante il gaming online.

Alcuni giocatori possono essere vittime di phishing, hacking o furto di account.

Il furto d'identità di soggetti minori è definito come digital kidnapping e rappresenta

[12] Si ricorda che il cyberbullismo ha le stesse caratteristiche del bullismo tradizionale, con la particolarità che questo si manifesta attraverso la rete internet, in diverse forme e con conseguenze potenzialmente più gravi del bullismo offline.

una sfida emergente nell'era digitale richiedendo una risposta educativa e consapevole.
Il **digital kidnapping** si riferisce quindi alla pratica di creare un falso profilo online o di manipolare l'identità digitale di un minore al fine di appropriarsi delle sue informazioni personali per i fini più disparati come creare personaggi finti per giochi di ruolo o utilizzare l'identità digitale del minore per adescarne altri: "è qui che si conosce, che si fa amicizia".
I giovani potrebbero voler entrare in contatto, nel mondo reale, con utenti sconosciuti: "è il mio migliore amico anche se non ci siamo mai incontrati nel mondo reale". Talvolta questi incontri potrebbero sfociare in situazioni rischiose come l'adescamento di un minore su internet (**grooming**), che può portare a situazioni ad alto rischio per l'incolumità fisica e mentale, come l'abuso o sfruttamento sessuale.
Le vittime di digital kidnapping possono essere anche oggetto di cyberbullismo, persecuzione, estorsione o ricatti sulla base di immagini o filmati a sfondo sessuale (**sextortion**) o produzione e scambio di materiale su abusi sessuali su minori.
È essenziale che i ragazzi siano consapevoli dei rischi connessi all'uso delle piattaforme digitali e siano in grado di identificare segnali di avvertimento, come le richieste di spostarsi a parlare su chat private.
Tra i principali rischi del gaming online troviamo la dipendenza da videogame, il "**Gaming Disorder**"[13] . La disponibilità costante dei giochi online, l'esperienza coinvolgente e la competizione possono creare una forte attrazione, portando alcuni giocatori a dedicare troppo tempo e risorse al gioco. La dipendenza dal gaming può influire negativamente sulla salute mentale, sulle relazioni interpersonali e sul rendimento scolastico o lavorativo: "*perdere tutto vuol dire sclerare*".
Il disturbo comportamentale da gaming online, riconosciuto anche dall'Organizzazione Mondiale della Sanità (OMS) come una nuova forma di malattia mentale, è definito come "*una serie di comportamenti persistenti o ricorrenti legati al gioco, sia online che offline, manifestati da: un mancato controllo sul gioco; una sempre maggiore priorità data al gioco, al punto che questo diventa più importante delle attività quotidiane e degli interessi nella vita; una continua escalation del gaming nonostante conseguenze negative personali, familiari, sociali, educazionali, occupazionali o in altre aree importanti*".

È importante, tuttavia, distinguere tra una passione sana per il gioco e il Gaming Disorder. La maggior parte delle persone che giocano ai videogiochi non sviluppa alcun disturbo. Il Gaming Disorder, come abbiamo visto nella definizione, si riferisce a una condizione in cui il gioco diventa compulsivo, interferisce con la vita quotidiana e provoca disagio significativo.

[13] Diagnostic and Statistical Manual of mental disorder

Segnali da non sottovalutare sono l'isolamento per trascorrere molte ore ai videogiochi, restare svegli per chattare o giocare online fino a notte inoltrata con conseguente privazione delle ore di sonno necessarie.
La diagnosi del Gaming Disorder richiede una valutazione approfondita da parte di un professionista della salute mentale qualificato, che nel caso dei più giovani si tratta di un neuropsichiatra infantile. Il trattamento può includere interventi psicoterapeutici, supporto familiare, educazione sulle abitudini di gioco salutari, gestione dello stress e dell'ansia, sviluppo di abilità sociali alternative.
I giocatori possono sperimentare anche frustrazione, rabbia o senso di fallimento quando incontrano sfide nel gioco o subiscono sconfitte ripetute. In alcuni casi estremi, può verificarsi il fenomeno del "**rage quitting**" in cui i giocatori reagiscono in modo aggressivo o violento a causa di una situazione di gioco negativa e abbandonano la partita in modo brusco, in preda alla rabbia e alla frustrazione, anche prima che sia conclusa, perché si sta subendo una sconfitta totale.

Un altro rischio da considerare sono i potenziali effetti sulla salute fisica. I giocatori online possono trascorrere lunghe ore seduti davanti allo schermo, esponendosi a uno stile di vita sedentario. Questo può portare a problemi di postura e muscoloscheletrici oltre all'aumento del rischio di obesità.
Alcuni giochi online possono esporre i giocatori più giovani a contenuti inappropriati come violenza esplicita, linguaggio offensivo o temi per adulti. Ciò può influenzare il comportamento degli individui, aumentando il rischio di adottare atteggiamenti aggressivi, bullismo o comportamenti antisociali.

11.4 Come proteggersi

È importante tenere presente che i rischi di cui abbiamo parlato non si applicano a tutti i giocatori e che la gestione consapevole del tempo, l'equilibrio tra vita online e offline, e una buona igiene digitale possono contribuire a mitigare tali rischi.
Diventa importante stabilire limiti di tempo ragionevoli per il gioco online e rispettarli. L'utilizzo di timer o allarmi può aiutare a controllare il tempo trascorso a giocare.
Dedicare tempo anche ad altre attività fuori dal mondo del gaming, come lo sport, l'hobby, lo studio o il tempo trascorso con amici e familiari favorisce un equilibrio tra la vita online e offline e un benessere generale.
I genitori possono utilizzare strumenti di controllo parentale e limitazioni di accesso per proteggere i propri figli da contenuti inappropriati e limitare il tempo di gioco.

Tuttavia, il solo monitoraggio delle attività online non è sufficiente. Indispensabile è parlare con i giovani dei rischi associati al gaming online e sulla necessità di una buona igiene digitale:

- evitare di condividere informazioni personali sensibili con sconosciuti online o su forum di gioco.
- Usare password complesse e cambiarle regolarmente. L'utilizzo di gestori password può essere un valido alleato.
- Installare e mantenere attivo e aggiornato un buon software antivirus.
- Provvedere a effettuare gli aggiornamenti periodici del sistema operativo del computer o dispositivo utilizzato.
- Controllare e modificare le impostazioni di privacy sugli account di gioco online per limitare l'accesso alle tue informazioni personali e per controllare le interazioni con altri giocatori.
- Giocare su piattaforme e siti affidabili e legali. Evitare di scaricare giochi da fonti non ufficiali o di accedere a siti web sospetti.

Infine, prima di giocare a un nuovo gioco online, controllare la classificazione e leggere le recensioni per essere sicuri che sia adatto alla propria età e alle proprie preferenze. Esiste la possibilità di giocare a demo o versioni di prova per valutare il contenuto prima di impegnarsi nell'acquisto o nel gioco completo.
Per controllare la classificazione dei videogiochi è utile il PEGI (Pan European Game Information)[14], un sistema di classificazione dei giochi utilizzato in Europa per informare i consumatori sul contenuto e sulla fascia d'età appropriata per ciascun gioco. Come è possibile leggere sul sito, la classificazione PEGI esamina l'idoneità di un gioco sulla base dell'età e non del livello di difficoltà.
A titolo esemplificativo, i videogiochi con etichetta PEGI 3 non hanno contenuti inappropriati, ma a volte potrebbero essere un po' troppo complicati per i bambini più piccoli. Al contrario, ci sono giochi con etichetta PEGI 18 molto facili da capire, ma che contengono elementi non adatti a un pubblico più giovane.
Le etichette dell'età PEGI sono così suddivise:

A. 3+: il gioco è adatto a tutti i bambini di età superiore a 3 anni. I giochi in questa categoria presentano contenuti adatti anche ai bambini più piccoli e non contengono elementi che possano spaventarli o confonderli.
B. 7+: il gioco è adatto ai bambini di età superiore a 7 anni. I giochi in questa categoria possono contenere un po' più di violenza fantasiosa o di suspense, ma non devono contenere scene o immagini spaventose.
C. 12+: il gioco è adatto a persone di età superiore a 12 anni. I giochi in questa categoria possono contenere violenza leggera, linguaggio moderato o contenuti che potrebbero essere inappropriati per bambini più piccoli.
D. 16+: il gioco è adatto a persone di età superiore a 16 anni. I giochi in questa categoria possono includere violenza più intensa, linguaggio forte,

[14] Pegi Public Site

temi adulti o contenuti che richiedono una maturità emotiva e mentale superiore.

E. 18+: il gioco è adatto solo a persone adulte di età superiore a 18 anni. I giochi in questa categoria possono contenere violenza estrema, scene di sesso, droga o contenuti altamente disturbanti.

Oltre alle etichette dell'età PEGI, vengono forniti dei descrittori di contenuto. Queste descrizioni possono riguardare la presenza di violenza, linguaggio non adatto, paura, sesso, droga nel gioco, gioco d'azzardo, acquisti in-game, discriminazione. Verificare oltre all'età anche il tipo di contenuto permette di scegliere il videogioco in base anche alla sensibilità del giocatore.

11.5 Il gaming online nella formazione scolastica

Il gaming online può essere utilizzato come strumento di supporto per la formazione scolastica e per la formazione nella cybersecurity in quanto può offrire un'esperienza interattiva e coinvolgente per gli studenti, consentendo loro di apprendere in modo pratico e divertente.

I giochi possono essere progettati per insegnare concetti scientifici, tecnologici, ingegneristici e matematici in modo interattivo. Ne è un esempio il sito dell'organizzazione no-profit per l'innovazione dell'istruzione Code.org[15] che offre l'opportunità di apprendere l'informatica con semplici giochi in percorsi messi a disposizione delle scuole, con profili insegnanti o studenti.
Inoltre, i giochi possono essere utilizzati per insegnare nuove lingue, storia e cultura, offrendo un'esperienza immersiva in un contesto di apprendimento virtuale che permette esplorare periodi storici o culture diverse attraverso scenari, personaggi e missioni.
Il gaming online può anche essere utilizzato per la formazione nella cybersecurity, un ambito in rapida crescita e di fondamentale importanza. I giochi possono offrire simulazioni di attacchi informatici, consentendo agli studenti di mettersi nei panni di un hacker o di un difensore e sperimentare situazioni reali di sicurezza informatica. Oppure presentare scenari in cui gli studenti devono identificare e risolvere vulnerabilità di sicurezza in un sistema o in un'applicazione aiutandoli a sviluppare una mentalità critica e a comprendere le principali minacce e i punti deboli che possono essere sfruttati dagli attaccanti. Ne sono un esempio, analogamente agli esport, le piattaforme per competizioni di hacking etico, in cui gli studenti possono mettere alla prova le proprie abilità di sicurezza informatica e risolvere sfide in un ambiente controllato e sicuro.

[15] https://code.org/

11.6 Cosa abbiamo capito

- I videogiochi sono divertenti, se usati correttamente allenano la mente e supportano nell'acquisizione di soft skill.
- Vincere le sfide proposte nei videogiochi spinge a continuare i percorsi e le missioni intraprese per arrivare a un obiettivo, permettendo di sfruttare diverse abilità.
- Il gaming è una realtà che sarà sempre più presente nel nostro futuro, va esplorata e conosciuta.
- Il gaming online ha dei rischi, è importante conoscerli per proteggersi.
- L'industria del gaming online è un'opportunità per coloro che desiderano perseguire una carriera nel settore.

11.7 Scheda didattica - *scuola secondaria di primo grado*

Titolo attività	**Regole della community di gioco**
Obiettivo	Promuovere un ambiente positivo, sicuro e inclusivo per tutti i membri del gruppo di gioco
Descrizione attività	L'attività è strutturata come un progetto di gruppo, coinvolgendo gli studenti in diverse fasi: **Discussione e Brainstorming:** gli studenti si riuniscono per discutere l'importanza di una community di gioco online positiva e sicura. Vengono invitati a condividere le loro esperienze personali riguardanti comunità di gioco, sia positive che negative, e ad esprimere le loro idee su come rendere il loro ambiente di gioco online migliore. **Definizione degli obiettivi:** insieme, i ragazzi stabiliscono gli obiettivi principali delle regole della community. **Creazione di Regole:** divisi in gruppi più piccoli o individualmente, gli studenti iniziano a scrivere, o ad individuare tra quelle proposte, le regole per la community di gioco online. Ogni regola dovrebbe essere chiara, concisa e formulata in modo positivo. **Revisione e Discussione:** le regole create dai gruppi vengono condivise con l'intera classe e vengono esaminate collettivamente per produrre un unico regolamento, accettato e condiviso da tutti gli studenti. Attività aggiuntive, opzionali, per mantenere alta l'attenzione sul tema: **Monitoraggio e Applicazione delle Regole:** gli studenti monitorano costantemente che le regole definite siano applicate quando giocano online tra loro o con altri, segnalando qualsiasi comportamento inappropriato incoraggiando una discussione aperta sulle eventuali preoccupazioni. **Valutazione e Riflessione:** alla fine dell'attività, gli studenti riflettono sull'esperienza di creare e gestire la community di gioco online. Discutono degli effetti positivi delle regole e dei cambiamenti che hanno notato nel comportamento degli utenti.
Documentazione fornita	Esempi di regole di community di giochi online
Strumentazione necessaria (HW/SW)	- PC, Smartphone o Tablet - Collegamento a internet
Impegno (durata stimata)	1 ora
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 7

continua da scheda didattiica 11.7

Contenuti propedeutici in ingresso	- Buona padronanza delle tecnologie digitali e delle piattaforme di gioco online, come navigare in Internet, utilizzare app e comunicare tramite chat o messaggistica. - Rischi e opportunità del gaming online.
Conoscenze / Competenze / abilità in uscita	- Valutare i comportamenti online e le dinamiche della community in modo critico, riflettendo su come le regole possono influenzare il comportamento e la cultura della comunità di gioco. - Apprendere l'importanza dell'etica digitale e della responsabilità nell'utilizzo di piattaforme online, comprendendo le implicazioni delle proprie azioni e decisioni nella comunità virtuale. Attività aggiuntive, opzionali: - Sviluppare abilità di mediazione e risoluzione dei conflitti, affrontando situazioni di potenziale violazione delle regole e cercando di risolverle in modo pacifico.
Documentazione di supporto aggiuntiva (URL o allegati)	- https://pegi.info/it - https://tuttosuivideogiochi.it/

11.8 Scheda didattica - *scuola secondaria di primo e secondo grado*

Titolo attività	**Game Jam**
Obiettivo	Promuovere la creatività e la collaborazione tra gli appassionati di giochi, sviluppatori, artisti e giocatori.
Descrizione attività	L'attività prevede la definizione di un tema o una parola chiave su cui i giochi dovranno basarsi e un limite di tempo per lo sviluppo del gioco. Al termine del periodo di sviluppo, i partecipanti condivideranno i loro giochi, le regole di gioco e della community con i loro compagni tramite sessione di gioco in cui i partecipanti possono mostrare i loro giochi e ricevere feedback dagli altri partecipanti e dagli spettatori. I giochi potranno essere, a seconda dell'indirizzo scolastico, creati sviluppando codice, graficamente tramite presentazione di storytelling, etc.
Documentazione fornita	- Strumenti di sviluppo come motori grafici o motori di gioco, risorse artistiche, suoni e musica, tutorial e documentazione tecnica. oppure - piattaforme online per la creazione di videogame quali: - https://rooms.xyz/ - https://make.gamefroot.com/ - https://www.easygamemaker.com/
Strumentazione necessaria (HW/SW)	- PC o Tablet - Collegamento a internet - Strumenti di sviluppo
Impegno (durata stimata)	1 mese
Tipologia	Attività individuale: sì Attività di gruppo: sì - Min partecipanti: 2 - Max partecipanti: 4
Contenuti propedeutici in ingresso	- Buona padronanza delle tecnologie digitali e delle piattaforme di gioco online, come navigare in Internet, utilizzare app e comunicare tramite chat o messaggistica. - Buona padronanza di piattaforme di sviluppo del codice, grafica, etc. - Rischi e opportunità del gaming online.

continua da scheda didattica 11.8

Conoscenze / Competenze / abilità in uscita	- Sensibilizzare i partecipanti sull'importanza della cittadinanza digitale responsabile, incoraggiando il rispetto degli altri, l'etica digitale e la consapevolezza delle implicazioni delle azioni online. - Pensare in modo fuori dagli schemi e a trovare soluzioni originali per i problemi di design dei giochi. - Competenze pratiche nello sviluppo di giochi, comprese le basi della programmazione, la progettazione dei livelli, l'implementazione delle meccaniche di gioco e l'ottimizzazione delle risorse. - Competenze di comunicazione digitale, inclusa la capacità di utilizzare strumenti di collaborazione online e interagire con altri sviluppatori attraverso piattaforme digitali.
Documentazione di supporto aggiuntiva (URL o allegati)	- https://pegi.info/it - https://tuttosuivideogiochi.it/

12 Conclusioni

Nella guida abbiamo toccato i principali argomenti che riguardano le basi della cybersecurity, e abbiamo scelto di fare un focus sul gaming perché è una delle attività online più diffusa tra i ragazzi, con lo scopo di fornire gli strumenti minimi per affrontare questi temi in classe o in famiglia. È impossibile scendere nel dettaglio di ogni argomento, ne verrebbe fuori un trattato, ma nel testo ci sono vari riferimenti e spunti di approfondimento.

La cybersecurity è un argomento in continua e rapida evoluzione: questo implica la necessità di aggiornarsi di continuo. La Rete stessa cambia e si trasforma rapidamente, non tanto nei protocolli e nella sua struttura (per quanto, anche in questo settore ci sono notevoli innovazioni, si pensi al 5G) quanto nei suoi aspetti "social": nel giro di meno di trent'anni abbiamo visto succedersi browser (Netscape, Explorer, Cyberdog per arrivare ai giorni nostri con Firefox, Chrome, Safari), motori di ricerca (qualcuno si ricorda ancora di Altavista, di Yahoo, di MSN? Eravamo già a metà degli anni '90 e ci sembra preistoria), social network (Myspace nacque nel 2003 ma dal 2010 in poi fu soppiantato da Facebook e oggi di Myspace si ricordano solo pochi appassionati di storia della Rete) e soprattutto i social frequentati dai ragazzi e dagli adolescenti: inutile dire che Facebook è ignorato dai ragazzi, che sono in uscita anche da Instagram, i cui utenti sono mediamente più vicini ai 30 anni che all'adolescenza; moltissimi sono su TikTok, ma anche su Twitch, Discord, Reddit, su YouTube (ammesso di poterlo definire un social) e diversi altri.

È difficile tenere il conto, ma sono gli ambienti online dove maggiormente "vivono" i ragazzi e quindi dove più facilmente possono essere esposti a rischi. Non è possibile conoscere tutti i social e indicare per ciascuno la specifica realizzazione del rischio ed è per questo che è importante conoscere e indicare ai ragazzi i criteri generali per conoscere i rischi catalogati secondo categorie principali, consentendogli di riconoscerli nelle mille facce in cui si realizzano in Rete ed evitarli.

Nel ruolo di educatori, se vogliamo concretamente dare un supporto ai nostri ragazzi, mettendo a disposizione la nostra esperienza da adulti nell' accompagnarli, bisogna che ci teniamo al passo, che facciamo uno sforzo per imparare le novità e restare aggiornati. Una chiave (non l'unica), a nostro parere, è imparare dai ragazzi ciò che c'è di nuovo: realizzare un canale a doppio senso tra chi impara e chi spiega alternandosi nei ruoli e creando, per quanto possibile, una certa complicità. Spesso il risultato di questo approccio è guadagnare (e non perdere) il rispetto e la considerazione da parte dei ragazzi, potendo mantenere autorevolezza e credibilità anche su questi argomenti, che spesso consideriamo fuori dalla nostra portata.

La nostra esperienza di adulti è indispensabile per dare ai ragazzi la misura dei rischi che corrono e delle loro conseguenze.

Infine, vorremmo suggerire di spronare le ragazze a interessarsi di questi temi: dalle statistiche emerge che la presenza femminile nel settore della cybersecurity è molto bassa. Dall'indagine svolta nel 2022 dalle Women for Security emerge che le donne che lavorano nel campo della Cybersecurity sono per il 55% laureate e il 44% è inserita in ruoli tecnici, mentre le altre sono inserite nel settore marketing o comunicazione, che pure richiedono competenze specifiche, ma solo il 5% ricopre funzioni dirigenziali. Le motivazioni per cui queste professioniste si sono avvicinate alla Cybersecurity all'inizio della loro carriera riguardano prevalentemente la curiosità per un mondo ancora poco esplorato, il caso o le offerte ricevute, ma anche le opportunità che il settore offre, opportunità, che le ragazze, con le capacità che dimostrano di aver quando si applicano a questo ambito, potrebbero sfruttare con grande successo.

13 Approfondimenti

Nel seguito sono elencati alcuni siti dove è possibile trovare contenuti, materiali e strumenti per approfondire, anche con gli studenti.

- Ludoteca Registro.it
- SIC Italia - KIT DIDATTICO (Generazioni Connesse- Safer Internet Centre)
- Arcipelago Educativo (Save the children)
- Parole Ostili
- Telefono azzurro

WOMEN
for Security

www.womenforsecurity.it

info@womenforsecurity.it