Sicurezza in rete

SCHEDA PER I GENITORI

Qual è il problema?

Proprio come nel mondo fisico, è importante che gli adolescenti imparino a capire di chi possono fidarsi su Internet. È frequente la richiesta di dati personali come nome, età ed indirizzo di casa in moduli o profili online ed i ragazzi devono sapere che rilasciando queste informazioni, vengono tracciati dalle aziende a scopo promozionale e - peggio ancora - possono cadere vittime di truffe su Internet, mettendo a rischio la loro identità. Ad esempio, potrebbero essere indotti a compilare un modulo per partecipare a un finto concorso a premi. Oppure ad aprire un allegato che installa uno spyware sul loro computer. O magari a cliccare su un annuncio ed inserire il loro indirizzo email che l'inserzionista può poi vendere ad altre aziende.

Con la sicurezza digitale si intende mantenere noi, i nostri dati ed i nostri dispositivi digitali al sicuro da minacce esterne. Questi problemi riguardano tutti: adolescenti, famiglie e persino intere comunità in rete. I problemi di sicurezza online possono essere suddivisi in tre categorie:

Truffe e furti di identità. I criminali possono ingannare gli adolescenti al fine di raccogliere dati personali. Possono poi usare questi dati per realizzare attività illecite a loro nome, compromettendo il loro futuro finanziario, ad esempio rendendo difficile fare acquisti e ottenere prestiti. I criminali prendono di mira i giovani perché hanno un profilo finanziario più pulito degli adulti.
Ecco alcune possibili fonti di rischio.

- *Phishing*: email, messaggi istantanei o link a siti web falsi che i truffatori usano per indurre le loro vittime a fornire dati personali e finanziari.
- *Clickjacking*: i truffatori ingannano gli utenti - di solito su un sito di social network - per indurli a cliccare su una pagina web apparentemente innocua, nel tentativo di rubare dati o propagare la truffa verso altri.

Virus e spyware. Molti adolescenti scaricano e condividono musica, film e giochi. Tuttavia, dovrebbero rivolgersi solo a siti sicuri ed evitare di cliccare su link e allegati che possono metterli in pericolo. Ci si può proteggere da virus e spyware mediante appositi software antivirus. Ecco alcune possibili fonti di rischio.

- *Virus informatico*: un programma che può replicarsi e diffondersi da un dispositivo digitale all'altro attraverso Internet, connessione diretta tra dispositivi, CD, DVD o memorie USB. Un virus si attacca ad un programma in modo che ogni volta che quest'ultimo viene eseguito, anche il virus si attivi causando problemi al dispositivo che lo ospita.
- *Spyware*: un programma che raccoglie dati di un utente di un dispositivo digitale a sua insaputa.

Le aziende tracciano gli utenti. Una delle strategie aziendali in maggior crescita è il monitoraggio dei dati, della posizione e del comportamento degli utenti su Internet. Lo scopo delle aziende è di personalizzare l'esperienza degli utenti e vendere i loro dati di navigazione agli inserzionisti. L'aspetto negativo è che la maggior parte degli adolescenti non sa che la loro attività online è tracciata. La legge impone alle aziende di dichiarare il modo in cui i comportamenti dei consumatori vengono tracciati (in Italia il 25 maggio 2018 è entrato in vigore il regolamento generale per la protezione dei dati personali, GDPR), ma spesso questi dettagli sono sepolti nelle sterminate informativa sulla privacy (che è umanamente impossibile leggere nel dettaglio). Il lato positivo è che può essere bello per i ragazzi visitare siti web con contenuti su misura per i loro interessi. Ecco alcuni possibili problemi.

- *Cookies*: piccoli file di dati memorizzati sul computer dell'utente quando visita un sito; le aziende li utilizzano per identificare i clienti abituali e personalizzare l'esperienza di navigazione.
- *Pubblicità mirata*: gli annunci su misura per gli utenti di Internet, basati sui dati che le aziende hanno precedentemente raccolto su di loro.

Sicurezza in rete

SCHEDA PER I GENITORI

Perché è importante?

Gli adolescenti devono essere consapevoli del fatto che quando sono connessi ad Internet, le aziende monitorano ciò che viene visitato per poi proporre delle pubblicità mirate. C'è poi il problema dei furti di identità e delle truffe online che possono produrre conseguenze rilevanti, sia dal punto economico che reputazionale. Conoscere i rischi legati alla sicurezza digitale è il primo passo per acquisire consapevolezza di come muoversi in rete in modo sicuro. Spetta ai ragazzi proteggersi per non essere dei facili bersagli.

Cosa possono fare le famiglie

Quali sono i vantaggi e gli svantaggi del fatto che le aziende tengono traccia dei vostri dati di navigazione, del vostro comportamento e della vostra posizione?

Quando scaricate qualcosa da Internet, come fate ad assicurarvi di essere su un sito sicuro?

Avete mai rischiato di cadere vittime di un tentativo di phishing?

La voce del buon senso

Create password robuste. Una password robusta fa miracoli nel proteggere gli account. Occorre spiegare agli adolescenti perché è necessario cambiare spesso le loro password e perché non condividerle mai, neanche con gli amici. Qui si possono trovare ottimi suggerimenti per creare password sicure: lastpass.com/it/password-generator. Il tema può essere ulteriormente approfondito in questo webinar di Programma il Futuro: *La password geniale*: video, presentazione.

Pensateci su prima di scaricare. I contenuti che gli adolescenti scaricano da fonti non sicure, possono infettare i dispositivi digitali con spyware e virus. Incoraggiate i ragazzi a scaricare solo da siti sicuri.

Fate attenzione a come condividete i vostri dati. Gli adolescenti dovrebbero fare attenzione quando condividono dati come il nome completo, l'indirizzo di casa, le coordinate bancarie o i dati di una carta di credito. Quando ricevono un messaggio in cui viene chiesto loro di condividere dati personali o finanziari, devono alzare la soglia di allerta. Se sospettano una truffa, non devono rispondere, né cliccare sui link presenti nel messaggio. Incoraggiateli a segnalare questi messaggi di phishing al provider di posta elettronica o al sito di social network tramite il quale lo hanno ricevuto.

Approfondite i temi della sicurezza. La conoscenza è un ottimo modo per evitare di essere ingannati. Il phishing ed altre problematiche di sicurezza vengono presentate in questo webinar di Programma il Futuro: *Pillole di sicurezza digitale: imparare dall'emergenza*: video, presentazione.

Installate sempre gli aggiornamenti di sicurezza. Utilizzando software aggiornato, i vostri dispositivi digitali sono più al sicuro da virus, spyware e altri problemi di sicurezza.

Considerate la possibilità di limitare la raccolta dei dati. Aiutate i ragazzi ad assumere il controllo dei propri dati:
1. disabilitando i "cookie" in modo che le aziende non possano tracciare il loro comportamento online,
2. evitando di cliccare sugli annunci pubblicitari
3. leggendo l'informativa sulla privacy di un sito web prima di rivelare qualsiasi dato personale o finanziario.

11 - 13 anni

Truffe online

*** LO SAPEVI CHE...**

"Malware" è l'abbreviazione di "software maligno": un programma progettato per danneggiare un dispositivo digitale.

Collega con una freccia le parole con la definizione corretta	
Phishing	un tipo di reato in cui i dati personali vengono rubati e sfruttati per attività criminali
Furto di identità	una licenza di diritto d'autore che permette agli altri di copiare, condividere e basarsi su un vostro contenuto creativo, a patto che vi indichino come autore dell'opera
Lavoro creativo	quando ricevi email, messaggi pop-up, messaggi sui social media o SMS, che contengono link a siti web fasulli, con la finalità di convincerti a fornire dati personali o finanziari
Creative Commons	qualsiasi idea o creazione artistica registrata in forma cartacea o digitale

*** COSA NE PENSI?**

È possibile che le persone vengano truffate su Internet? Come?

*** TI RICORDI?**

Che cos'è il furto d'identità e come ci si può proteggere?

1. Attività in famiglia

Insegna le basi della sicurezza su Internet ad un membro della tua famiglia, in modo che non rischi di cadere vittima di truffe. Condividi le tecniche imparate per individuare le email di phishing e cosa fare se si riceve un messaggio sospetto. Insieme, escogitate un modo concreto per migliorare la vostra sicurezza online (ad esempio, rendendo le password più sicure e facendo periodicamente i backup).

2. Sfrutta la tecnologia

Con il vostro familiare (o da soli), guardate queste regole di sicurezza:

https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-qualche-precauzione

Quello che avete imparato vi dà qualche idea in più per migliorare la vostra sicurezza online?

3. La voce del buon senso...

Ecco le caratteristiche di una email di phishing o di una truffa che occorre imparare a riconoscere per non essere ingannati: la richiesta di verificare le proprie credenziali, un senso di urgenza, errori di ortografia, la segnalazione di problemi con il tuo account, la richiesta di cliccare su link presenti nell'email o in un allegato, qualcosa che suona troppo bello per essere vero o un saluto generico. Se ricevi un'email dubbia, non aprirla: cancellala semplicemente. E, se la apri per sbaglio, non cliccare su alcun link e non scaricare alcun allegato: potrebbero contenere dei malware.