Furti d'identità e truffe online

Cittadinanza digitale consapevole
per la Scuola Secondaria di Primo Grado

Adattamento italiano a cura di I. Corradini, F. Lacchia, E. Nardelli

common sense education®

Programma il Futuro

Furti d'identità e truffe online
Cittadinanza digitale consapevole
per la Scuola Secondaria di Primo Grado

Contenuti originali di Common Sense Education (www.commonsense.org/education)

Versione italiana a cura di Programma il Futuro (www.programmailfuturo.it)

Direzione e coordinamento: Enrico Nardelli

Revisione e supervisione scientifica: Isabella Corradini

Traduzione e adattamento in italiano: Francesco Lacchia

Grafica di copertina: Paolo Alberti

Foto di copertina: Freepik.com

Ultimo aggiornamento: gennaio 2021

common sense education®

Programma il Futuro

Introduzione

Per diventare buoni cittadini digitali è necessario che gli studenti acquisiscano non solo i concetti base dell'informatica, ma anche le competenze per muoversi in modo responsabile in Internet. I cosiddetti nativi digitali, infatti, usano con sorprendente abilità gli strumenti tecnologici, ma spesso in modo non sicuro.

Questo materiale educativo è stato realizzato dall'organizzazione americana no profit Common Sense (www.commonsense.org/education) e adattato in italiano da Programma il Futuro (www.programmailfuturo.it), il progetto MI[1]-CINI[2] che ha l'obiettivo di fornire alle scuole una serie di strumenti semplici, divertenti e facilmente accessibili per formare gli studenti ai concetti di base dell'informatica.

Nel testo si è preferito non usare il termine *virtuale* per ciò che accade in rete e *reale* per ciò che avviene nel mondo fisico, perché potrebbe suggerire che ciò che accade in rete non sia tangibile. Invece, tutte le azioni che gli esseri umani compiono in Internet (ad esempio fare un post su un social media, inviare una mail) sono concrete. Inoltre, le esperienze che essi vivono in rete, nel bene e nel male, evocano delle emozioni e possono produrre conseguenze anche nefaste sulla vita degli altri (ad esempio nel cyberbullismo).

Per ogni lezione sono disponibili i seguenti documenti:

- il piano di lavoro della lezione,
- del materiale di approfondimento per l'insegnante,
- una o due esercitazioni,
- le versioni delle esercitazioni commentate per l'insegnante,
- la verifica,
- la versione della verifica commentata per l'insegnante.

È anche prevista una scheda di consigli utili per i genitori ed un'altra per svolgere delle attività insieme in famiglia.

I quaderni digitali di Programma il Futuro

Questa guida fa parte della seguente collana "Cittadinanza digitale consapevole":

- per la scuola primaria:
  - Segui le tracce digitali
  - Caccia via le cattiverie dallo schermo
  - Il mio quartiere digitale
  - Il potere delle parole
  - Super cittadino digitale
  - Dati personali e altri dati
- per la scuola secondaria di primo grado:
  - Comunicare in rete in modo sicuro
  - Le mie attività digitali
  - Furti d'identità e truffe online
- per tutti gli ordini di scuola (a partire dagli ultimi anni della primaria):
  - Come funzionano i computer

1 Ministero dell'Istruzione
2 Consorzio Interuniversitario Nazionale per l'Informatica

Sommario

- Piano di lavoro della lezione pag. 5
- Riconosci le truffe - Esercitazione pag. 10
- Riconosci le truffe - Versione insegnante pag. 12
- Verifica pag. 15
- Verifica - Versione insegnante pag. 16
- Sicurezza in rete - Scheda per i genitori pag. 17
- Scheda per attività in famiglia pag. 19

Furti d'identità e truffe online

Domanda chiave

Cos'è il furto di identità? Come puoi proteggerti?

Durata: 45 minuti - 1 ora

Parole Chiave –

truffa: il tentativo di ingannare qualcuno, di solito con l'intenzione di sottrargli denaro o dati personali

furto di identità: un tipo di reato in cui i dati personali vengono rubati e sfruttati per attività criminali

vulnerabile: chi si trova in una condizione che lo rende più esposto ad essere danneggiato o attaccato

phishing (pronuncia: *fiscing*): una tipologia di truffa basata sull'invio di messaggi falsi che imitano comunicazioni ufficiali: possono essere 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

Sommario

Gli studenti imparano come proteggersi dal furto di identità e dalle truffe online che hanno l'obiettivo di sottrarre e utilizzare i loro dati personali. Imparano cos'è il furto di identità, che tipo di dati cercano i ladri di identità e cosa si può fare con questi dati. Gli studenti analizzano poi delle email false ed imparano ad individuare le tecniche che i ladri di identità usano in rete. Infine, costruiscono una email di phishing basata su ciò che hanno appreso e verificano se i compagni di classe riescono ad identificare che si tratta di un tentativo di truffa.

Obiettivi

Gli studenti saranno in grado di...

- capire cos'è il furto d'identità e come proteggersi;
- riconoscere le tecniche che i truffatori online sfruttano per convincere gli utenti a comunicare i dati personali;
- difendersi dal phishing e dal furto d'identità.

Materiali e preparazione

- Carta e pennarelli o matite colorate (o computer con un pacchetto software da ufficio, nel caso si segua l'opzione tecnologica nella Parte 3)
- Stampa il documento **Riconosci le truffe – Esercitazione** (pag. 10), uno per ogni alunno.
- Leggi in anteprima la versione per l'insegnante del suddetto documento (pag. 12).

Risorse per la famiglia

- Puoi segnalare alle famiglie la seguente documentazione: **Sicurezza in rete – Scheda per i genitori** (pag. 17), puoi stampare i documenti oppure comunicare il seguente indirizzo: https://programmailfuturo.it/furti-d-identita-e-truffe-online#genitori

introduzione

Preparazione *(5 minuti)*

DEFINISCI la parola chiave **truffa**.

CHIEDI:

Conoscete qualcuno che è stato truffato? Com'è successo?	Gli studenti potrebbero raccontare storie in cui qualcuno è stato convinto ad inviare denaro a qualcun altro o ad acquistare un prodotto contraffatto.
Qual è lo scopo di una truffa? Quali inganni sono utilizzati per realizzare una truffa?	Gli studenti devono comprendere che lo scopo ultimo di una truffa è di convincere qualcuno a fornire al truffatore denaro o informazioni che possono aiutarlo a rubare denaro, come il numero della carta di credito, il PIN del bancomat o una password. Per raggiungere questo scopo, i truffatori mentono e spesso falsificano la loro identità.
È possibile essere truffati su Internet? In che modo?	Dai ai tuoi studenti l'opportunità di raccontare storie di amici o parenti che hanno subito truffe online. Poi incoraggiali ad analizzare ciò che sanno su queste truffe e su come i truffatori potrebbero trarne vantaggio. Esempi di risposte: • qualcuno può essere stato indotto con l'inganno a comprare online un prodotto contraffatto • qualcuno può essere stato indotto a comunicare dati che un truffatore può sfruttare per rubargli del denaro

SPIEGA ai tuoi studenti che gli verranno presentati diversi tipi di truffe online e verranno descritte le tipologie di dati che i truffatori cercano e come questi possono essere sfruttati a fini illegali. Grazie a queste conoscenze, gli studenti saranno in grado di proteggersi dalle truffe in rete.

parte 1

Cos'è il furto di identità? *(10 minuti)*

RICORDA agli studenti che i truffatori non cercano sempre di ottenere soldi direttamente. Spesso usano una varietà di strategie per indurre le persone a fornire dati personali, che poi possono essere utilizzati per accedere ai loro conti bancari, alle carte di credito o ad altri account personali. Possono anche "ricreare" l'identità di qualcuno e produrre documenti falsi, come carte di credito, carte di identità o patenti di guida a nome di qualcun altro.

DEFINISCI la parola chiave **furto d'identità**.

CHIEDI: *Che tipo di dati personali potrebbero cercare i ladri di identità?*

RIPASSA con gli studenti la lista sottostante. Sottolinea che i ladri di identità cercano qualsiasi dato che possa aiutarli a fingere di essere una delle loro vittime. Scrivi sulla lavagna la seguente lista o fai prendere appunti agli studenti.

- Nome e Cognome
- Data e luogo di nascita
- Attuale e precedenti indirizzi di casa e relativi numeri di telefono
- Numero di un documento di identità (come carta di identità, patente o passaporto)
- Credenziali di account associati a metodi di pagamento (PayPal, Amazon, ecc.)

DEFINISCI la parola chiave **vulnerabile**.

SPIEGA che siamo tutti vulnerabili a furti d'identità e truffe online. Anche se gli adolescenti spesso pensano di non essere esposti a questi rischi, ci sono alcune importanti ragioni per cui non bisogna assolutamente sottovalutarli. Soffermati sui seguenti punti.

- I ladri di identità cercano dati personali non ancora utilizzati per ottenere finanziamenti. Si rivolgono ad adolescenti e ragazzi, proprio perché non hanno ancora una storia di credito alle spalle. I ladri d'identità possono poi vendere questi dati, permettendo a qualcun altro di ottenere una carta di credito o un prestito e di accumulare debiti a vostro nome.
- Essere vittima di un furto di identità può rovinare il loro futuro finanziario e la possibilità di ottenere prestiti, ad esempio per l'acquisto di un'auto.
- Se gli adolescenti utilizzano online le carte di credito dei loro genitori, o compilano moduli con i loro dati, stanno condividendo informazioni di interesse per i malintenzionati.
- Possono essere necessari mesi, anche anni, per recuperare un'identità in caso di furto. Tornare alla normalità può essere molto costoso con notevole dispendio di tempo ed energia.

parte 2

Non abboccare! *(15 minuti)*

CHIEDI:

Come pensate che i ladri di identità agiscano per sottrarre i vostri dati?

Incoraggia gli studenti a condividere le loro opinioni, anche se non hanno mai avuto a che fare con un furto d'identità.

DEFINISCI la parola chiave **phishing** (pronuncia: *fiscing*).

SPIEGA agli studenti che il modo migliore per non abboccare ai tentativi di phishing è di essere sempre molto scettici su qualsiasi richiesta di dati personali online. È importante dubitare di messaggi online o dei post di amici che sembrano esprimersi in modo diverso dal solito: questo potrebbe anche indicare situazioni gravi, come la violazione del loro account. Nel seguito, analizzando uno dei principali metodi di phishing (email falsa), verranno descritti alcuni indizi che possono aiutare gli studenti ad individuare questo tipo di truffa.

DIVIDI gli studenti in coppie.

DISTRIBUISCI il documento **Riconosci le truffe – Esercitazione** (pag. 10), uno per ogni studente.

LEGGI ad alta voce le istruzioni che si trovano nella versione per l'insegnante del suddetto documento ed analizza con gli studenti la spiegazione completa di tutte le caratteristiche di un'email di phishing.

ISTRUISCI le coppie di studenti affinché completino correttamente l'esercitazione. Quando hanno terminato, fai in modo che le coppie si scambino e confrontino le risposte.

INVITA dei volontari a condividere le risposte con i compagni. Utilizza come guida la versione per gli insegnanti dell'esercitazione.
RICORDA agli studenti che i messaggi di phishing possono essere estremamente convincenti e che alcuni potrebbero non contenere gli indizi che hanno appena imparato a riconoscere. Quindi è fondamentale diffidare di qualsiasi messaggio che chieda loro di fornire dati personali.

parte 3

Proteggiti dalle truffe online *(10 minuti)*

RICORDA agli studenti che, quando in rete incontrano qualcosa che ritengono possa essere un messaggio di phishing, devono osservare le seguenti regole:

- Evitare di aprire il messaggio.
- Non cliccare sui link e non scaricare alcun allegato: potrebbero contenere virus o spyware.
- Non rispondere al messaggio.
- Se è un'email, contrassegnarla come "spam"; se è un post, segnalarlo al sito del social network.
- Se si verificano problemi con l'account di qualche servizio o si ha il timore delle ripercussioni da parte di qualche azienda (per esempio in caso di segnalazione di fatture non pagate), è bene contattare il loro servizio clienti (se possibile telefonicamente), verificando le informazioni di contatto dell'azienda al di fuori del messaggio ricevuto (per esempio digitando manualmente l'indirizzo del sito web).

SPIEGA agli studenti che ci si può proteggere dalle truffe su Internet anche immedesimandosi nei ladri di identità. Creeranno un messaggio di phishing o qualche altra forma di truffa online, sfruttando ciò che hanno imparato in questa lezione.

Facoltativo: prima che gli studenti creino i loro esempi, potresti mostrar loro alcuni esempi reali di messaggi di phishing.

CHIEDI agli studenti di utilizzare almeno quattro delle otto caratteristiche di un messaggio di phishing elencate nel documento **Riconosci le truffe – Esercitazione** (pag. 10). Chiedi loro di creare un messaggio di phishing che sfrutti le quattro caratteristiche che scelgono di evidenziare.

CHIEDI agli studenti di presentare alla classe gli esempi realizzati. I compagni devono segnalare gli indizi rilevatori del messaggio di phishing. In alternativa, possono lavorare a coppie, cercando di individuare la truffa a vicenda.

conclusione

Riepilogo *(5 minuti)*

Puoi usare queste domande per valutare il raggiungimento degli obiettivi della lezione da parte dei tuoi studenti. Potresti anche chiedere loro di approfondire per iscritto una delle domande.

CHIEDI:

Che tipo di dati cercano i ladri di identità? Perché?	Gli studenti dovrebbero rispondere con esempi di dati personali, come nome e cognome, indirizzo, data e luogo di nascita, numero di un documento di identità e credenziali di metodi di pagamento. I ladri di identità cercano di sfruttare questi dati per "ri-creare" l'identità di qualcuno per scopi illegali, principalmente per ottenere prestiti e acquistare oggetti o servizi.
In che modo i ladri di identità agiscono per sottrarre i tuoi dati?	I ladri usano il phishing per cercare di ottenere i dati personali degli utenti. Chiedi agli studenti di presentare alcune delle caratteristiche del phishing che hanno appena imparato.
Cosa puoi fare per evitare di cadere nelle truffe online?	Gli studenti devono ricordarsi di essere sospettosi nei confronti di qualsiasi comunicazione online che richieda l'invio di dati personali. Inoltre, è importante essere dubbiosi nei confronti dei messaggi di amici che sembrano esprimersi in modo diverso dal solito. Gli studenti dovrebbero apprendere che in questi casi occorre: non rispondere a tali messaggi, non cliccare su alcun link, non scaricare eventuali allegati e di segnalare il messaggio come spam o al sito del social network. Se hanno problemi con l'account di qualche servizio o temono delle ripercussioni da parte di qualche azienda, devono contattare il servizio clienti, verificando le informazioni di contatto dell'azienda al di fuori del messaggio ricevuto.

SCRIVI sulla lavagna il seguente URL:
https://www.commissariatodips.it/richiedi-informazioni
spiegando agli studenti che possono usarlo per chiedere aiuto se loro, o i loro genitori, scoprono che la loro identità è stata rubata.

Riconosci le truffe

Istruzioni

I seguenti messaggi di posta elettronica sono esempi di phishing. Leggi qui sotto le caratteristiche di un'email di phishing. Poi cerca queste caratteristiche in ciascuno dei tre messaggi. Elenca le caratteristiche trovate nella colonna a destra di ogni messaggio e traccia delle linee che colleghino ogni caratteristica con la parte dell'email a cui si riferisce.

Caratteristiche di un'email di phishing

- Richiesta di verificare le credenziali di un tuo account (spesso relativo ad un conto bancario)
- Senso di urgenza
- Errori di ortografia
- Segnalazioni di problemi relativi al tuo account
- Richiesta di cliccare su dei link nell'email o aprire degli allegati
- Troppo bello per essere vero
- Saluto generico

Messaggio email	Tipiche caratteristiche di phishing

Da: no_reply@emailinternet.chase.com
Oggetto: Situazione del conto

Alla cortese attenzione del cliente della banca NomedellaBanca,

a causa di un recente controllo di sicurezza sul tuo conto, ti chiediamo di confermare i tuoi dati. La mancata conferma entro 24 ore comporterà la sospensione del conto. Ci dispiace per l'inconvenente.

Clicca qui per confermare le credenziali del tuo conto.

Cordiali saluti,

Servizio clienti online della Banca NomedellaBanca

Questa e-mail è stata inviata dalla NomedellaBanca.

Riconosci le truffe

Messaggio email

Tipiche caratteristiche di phishing

Da: custservice@paypalonline.com
Oggetto: Il tuo conto è stato sospeso

Gentile utente PayPal,

di recente abbiamo notato uno o più tentativi di accesso al tuo account da un indirizzo IP estero. Per motivi di sicurezza, abbiamo sospeso l'operatività del tuo conto.

Se non sei stato tu ad accedere, visita urgentemetne il tuo account sul sito di PayPal ed esegui i passi necessari per confermare di essere il titolare del conto. L'esecuzione di questa procedura eliminerà la sospensione e ripristinerà l'operatività del tuo conto.

https://www.paypal.com/us/cvi-limit/webscr?-run

Cordiali saluti,

PayPal Servizio anti-frode

Da: Lotteria Internazionale Svizzera
Oggetto: Notifica di vincita

Caro [Nome e Cognome],

Congratulazioni! Puoi ricevere un assegno circolare per un massimo di 500.000.000 Euro in contanti! Una bella somma! Esentasse! La tua probabilità di vittoria è 1/6. Centinaia di cittadini italiani vincono ogni settimana usando il nostro sistema segreto! Puoi vincere quanto vuoi!

Se scegli di ricevere le tue vincite, contatta IMB INSURANCE & BROKERS. Utilizzeranno il loro servizio diplomatico di consegna per recapitarti l'assegno. Si prega di utilizzare i seguenti contatti:

Nome della società: IMB INSURANCE & BROKERS
Indirizzo: Ginevra, Svizzera
Contatto: Sig. Alexander Caspari
(Direttore del Dipartimento delle Rimesse Estere)
Telefono diretto: +44-802 655 4889
Fax: +44-802 655 4890
Email diretta: ACaspari@IMBInsurancebrokers.com

Ancora congratulazioni!

Marcus Gohl

NOME: _____

Riconosci le truffe

Istruzioni

I seguenti messaggi di posta elettronica sono esempi di phishing. Leggi qui sotto le caratteristiche di un'email di phishing. Poi cerca queste caratteristiche in ciascuno dei tre messaggi. Elenca le caratteristiche trovate nella colonna a destra di ogni messaggio e traccia delle linee che colleghino ogni caratteristica con la parte dell'email a cui si riferisce.

Caratteristiche di un'email di phishing

Richiesta di verificare le credenziali di un tuo account (spesso relativo ad un conto bancario) Le email false cercano di convincerti a fornire le credenziali del tuo account o a cliccare su un link malevolo dove ti verrà richiesto di inserire i dati che verranno quindi rubati dai ladri di identità. Riflettendoci, ciò che chiedono non ha senso, perché l'azienda che ti scrive dovrebbe già possedere quei dati!

Senso di urgenza - Quando nel messaggio c'è scritto che hai solo poco tempo per rispondere, spesso è un indizio di truffa.

Errori di ortografia - Le email di truffa spesso contengono errori ortografici e grammaticali. Un'azienda seria non invierebbe mai messaggi con errori di questo tipo.

Segnalazioni di problemi relativi al tuo account - I ladri di identità cercano di spaventarti dicendoti che ci sono dei problemi con il tuo conto, sperano così che tu reagisca impulsivamente rispondendo immediatamente all'email per risolvere il problema.

Richiesta di seguire dei link nell'email o negli allegati - Le email di phishing contengono spesso un link che sei invitato a cliccare (o un allegato da aprire). Questo link può condurti ad un sito fasullo (spesso perfettamente identico a quello originale) dove fornirai inconsapevolmente le tue credenziali direttamente ai criminali. Non devi mai rispondere a queste email o cliccare sui link che contengono. Collegati invece al sito web dell'azienda (digitando manualmente l'indirizzo) e solo da lì controlla il tuo conto.

Troppo bello per essere vero - Le email di truffa spesso propongono offerte troppo belle per essere vere, come la possibilità di vincere soldi o premi, senza fare nulla per meritarselo.

Saluto generico - Le email di truffa spesso iniziano con un saluto generico che non contiene il tuo nome, mentre le aziende rispettabili chiamano i loro clienti per nome. Ma attenzione, in alcuni casi i truffatori potrebbero conoscere il nome associato al tuo indirizzo email, quindi non abbassare la guardia anche se si rivolgono a te utilizzando il tuo nome.

Riconosci le truffe

Messaggio email

Da: no_reply@emailinternet.chase.com
Oggetto: Situazione del conto

Alla cortese attenzione del cliente della banca NomedellaBanca,

a causa di un recente controllo di sicurezza sul tuo conto, ti chiediamo di confermare i tuoi dati. La mancata conferma entro 24 ore comporterà la sospensione del conto. Ci dispiace per l'inconvenente.

Clicca qui per confermare le credenziali del tuo conto.

Cordiali saluti,

Servizio clienti online della Banca NomedellaBanca

Questa e-mail è stata inviata dalla NomedellaBanca.

Tipiche caratteristiche di phishing

- Saluto generico
- Richiesta di verificare le credenziali
- Senso di urgenza
- Errori di ortografia
- Link nell'email

Da: custservice@paypalonline.com
Oggetto: Il tuo conto è stato sospeso

Gentile utente PayPal,

di recente abbiamo notato uno o più tentativi di accesso al tuo account da un indirizzo IP estero. Per motivi di sicurezza, abbiamo sospeso l'operatività del tuo conto.

Se non sei stato tu ad accedere, visita urgentemetne il tuo account sul sito di PayPal ed esegui i passi necessari per confermare di essere il titolare del conto. L'esecuzione di questa procedura eliminerà la sospensione e ripristinerà l'operatività del tuo conto.

https://www.paypal.com/us/cvi-limit/webscr?-run

Cordiali saluti,

PayPal Servizio anti-frode

- Problemi al tuo account
- Errori di ortografia
- Richiesta di verificare le credenziali
- Senso di urgenza
- Link nell'email

Riconosci le truffe

Messaggio email

Da: Lotteria Internazionale Svizzera

Oggetto: Notifica di vincita

Caro [Nome e Cognome],

Congratulazioni! Puoi ricevere un assegno circolare per un massimo di 500.000.000 Euro in contanti! Una bella somma! Esentasse! La tua probabilità di vittoria è 1/6. Centinaia di cittadini italiani vincono ogni settimana usando il nostro sistema segreto! Puoi vincere quanto vuoi!

Se scegli di ricevere le tue vincite, contatta IMB INSURANCE & BROKERS. Utilizzeranno il loro servizio diplomatico di consegna per recapitarti l'assegno. Si prega di utilizzare i seguenti contatti:

Nome della società: IMB INSURANCE & BROKERS
Indirizzo: Ginevra, Svizzera
Contatto: Sig. Alexander Caspari
(Direttore del Dipartimento delle Rimesse Estere)
Telefono diretto: +44-802 655 4889
Fax: +44-802 655 4890
Email diretta: ACaspari@IMBInsurancebrokers.com

Ancora congratulazioni!

Marcus Gohl

Tipiche caratteristiche di phishing

Saluto generico

Troppo bello per essere vero

Link nell'email

Furti d'identità e truffe online

VERIFICA

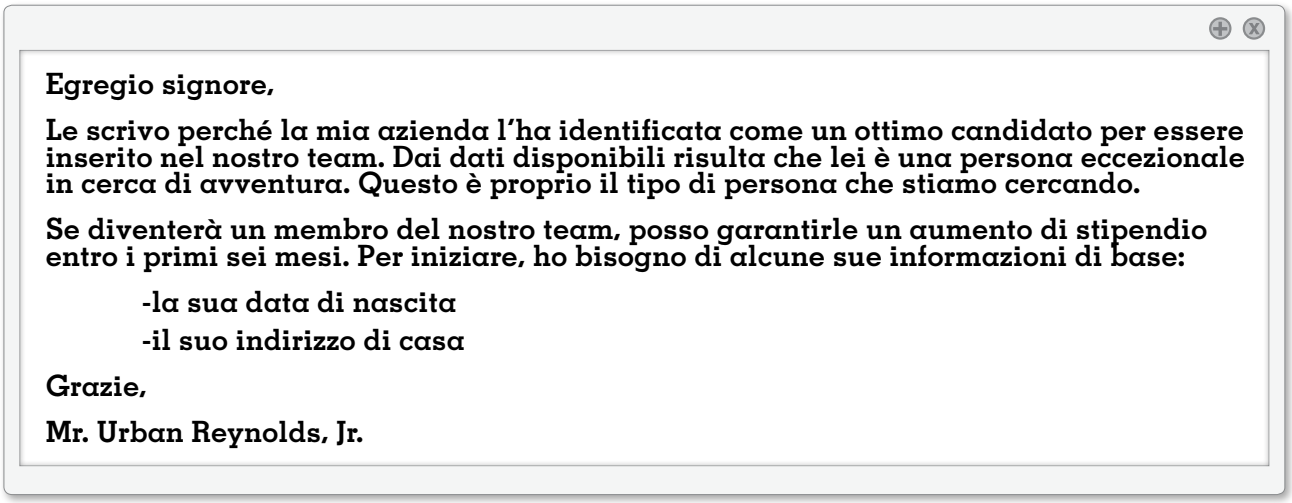
1. Un tipo di reato in cui i tuoi dati personali vengono rubati e sfruttati per attività criminali si chiama:

a) identificazione

b) furto d'identità

c) violazione di domicilio

2. Emilio riceve il seguente messaggio nella sua casella di posta elettronica:



Egregio signore,

Le scrivo perché la mia azienda l'ha identificata come un ottimo candidato per essere inserito nel nostro team. Dai dati disponibili risulta che lei è una persona eccezionale in cerca di avventura. Questo è proprio il tipo di persona che stiamo cercando.

Se diventerà un membro del nostro team, posso garantirle un aumento di stipendio entro i primi sei mesi. Per iniziare, ho bisogno di alcune sue informazioni di base:

-la sua data di nascita

-il suo indirizzo di casa

Grazie,

Mr. Urban Reynolds, Jr.

Quale dei seguenti NON è un segnale di avvertimento che indica che questo messaggio è una truffa:

a) l'offerta sembra troppo bella per essere vera

b) ad Emilio vengono richiesti alcuni dati personali

c) Emilio viene addirittura chiamato "Egregio signore"

3. Sara riceve sul suo telefono un messaggio che pensa possa essere una truffa. Dovrebbe:

a) inoltrare il messaggio ai suoi amici per vedere se anche loro pensano che sia una truffa

b) rispondere chiedendo al mittente di non inviarne altri

c) cancellare il messaggio

NOME: _____

Furti d'identità e truffe online

VERIFICA
VERSIONE INSEGNANTE

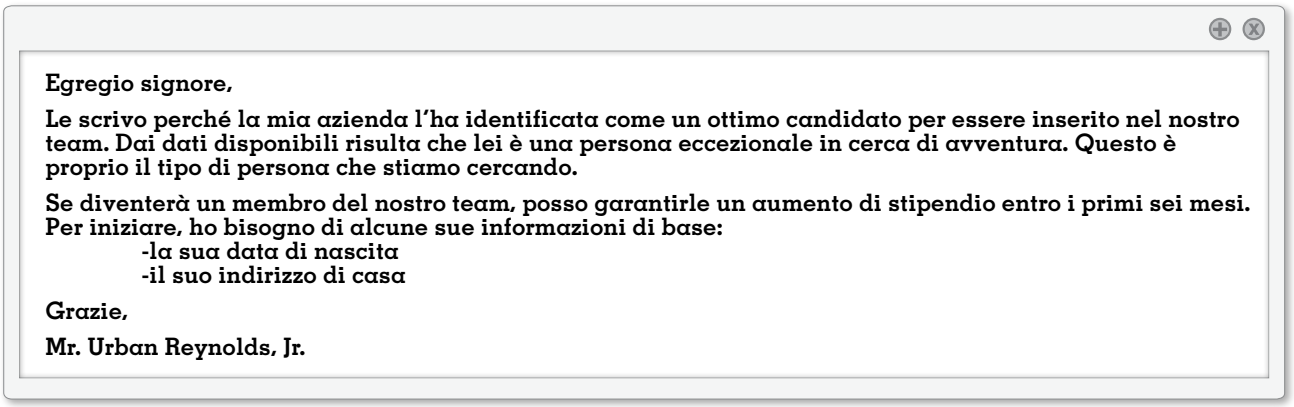
1. Un tipo di reato in cui i tuoi dati personali vengono rubati e sfruttati per attività criminali si chiama:

a) identificazione
b) furto d'identità
c) violazione di domicilio

Commento

La risposta corretta è **b**. Si può contribuire a proteggersi dal furto d'identità stando alla larga da tutte le offerte online progettate per carpire i dati personali.

2. Emilio riceve il seguente messaggio nella sua casella di posta elettronica:



Egregio signore,

Le scrivo perché la mia azienda l'ha identificata come un ottimo candidato per essere inserito nel nostro team. Dai dati disponibili risulta che lei è una persona eccezionale in cerca di avventura. Questo è proprio il tipo di persona che stiamo cercando.

Se diventerà un membro del nostro team, posso garantirle un aumento di stipendio entro i primi sei mesi. Per iniziare, ho bisogno di alcune sue informazioni di base:
-la sua data di nascita
-il suo indirizzo di casa

Grazie,

Mr. Urban Reynolds, Jr.

Quale dei seguenti NON è un segnale di avvertimento che indica che questo messaggio è una truffa:

a) l'offerta sembra troppo bella per essere vera
b) ad Emilio vengono richiesti alcuni dati personali
c) Emilio viene addirittura chiamato "Egregio signore"

Commento

La risposta corretta è **c**. È molto probabile che le offerte che sembrano troppo belle per essere vere o che richiedono dati personali possano essere truffe. I messaggi di questo tipi devono sempre essere segnalati come spam al proprio provider di posta elettronica e cancellati.

3. Sara riceve sul suo telefono un messaggio che pensa possa essere una truffa. Dovrebbe:

a) inoltrare il messaggio ai suoi amici per vedere se anche loro pensano che sia una truffa
b) rispondere chiedendo al mittente di non inviarne altri
c) cancellare il messaggio

Commento

La risposta corretta è **c**. Se Sara pensa che il messaggio possa essere una truffa, dovrebbe semplicemente cancellarlo.

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.