Allegato 2. Impara a distinguere il vero dal falso

1) Attività: “Non abboccare all’esca del phishing!”

Obiettivi:

- **Imparare** a riconoscere le modalità utilizzate da malintenzionati per ottenere informazioni personali, dati finanziari o codici di accesso durante una comunicazione digitale.
- **Analizzare** i sistemi a disposizione per prevenire i furti di identità.
- **Saper spiegare** a un adulto di fiducia le nozioni imparate, nel caso si creda di essere stato vittima
- **Riconoscere gli indizi** che identificano un tentativo di phishing.
- **Fare attenzione** a come e con chi condividere le proprie informazioni personali.

Spunti di discussione

Il phishing è quando qualcuno, fingendo di essere qualcuno di cui ti fidi, prova a rubarti informazioni come dati di accesso o altri dettagli di un tuo account via email, messaggio o tramite altre forme di comunicazione online. Le email di phishing (così come i siti su cui cercano di reindirizzarti e gli allegati che cercano di farti scaricare o aprire) possono infettare il tuo computer con virus che useranno l’elenco dei tuoi contatti per inviare email di phishing anche a loro.
Altri tipi di frode potrebbero tentare di farti scaricare malware o software indesiderati, facendoti credere che c’è qualcosa che non va sul tuo dispositivo. Ricorda: un sito o una pubblicità non possono sapere se c’è qualcosa che non va nel tuo dispositivo!

Alcuni attacchi di phishing sono facilmente riconoscibili.
Altri però possono essere sofisticati e convincenti. Per esempio, un truffatore potrebbe mandarti un messaggio che include alcune tue informazioni personali: questo tipo di attacco è chiamato spear phishing e spesso si rivela efficace.

È importante saper riconoscere prontamente messaggi e email inusuali o strani, prima di fare clic su link sospetti o inserire la propria password in siti web rischiosi

Ecco alcune domande che dovresti farti quando stai valutando la credibilità di un messaggio o di un sito:

- Sono presenti indicatori della sua affidabilità, come ad esempio dei badge?
- L'URL del sito combacia con il nome e con il titolo di ciò che stavi cercando?
- Si aprono dei pop-up? (Solitamente non sono un buon segno.)
- L'URL inizia con https:// preceduto da un lucchetto verde? (Questo significa che la connessione è crittografata e sicura.)
- Cosa c'è scritto a lettere piccole? (Solitamente le parti subdole vengono scritte a caratteri piccoli.)

Cosa faccio se riescono a truffarmi? Tanto per cominciare, non andare nel panico!

- Parlane subito con i tuoi genitori, i tuoi insegnanti o qualche altro adulto di cui ti fidi. Più aspetti, più la situazione potrebbe peggiorare.
- Cambia le password dei tuoi account online.
- Se si tratta di un tentativo di phishing o di frode, avvisa tutti i tuoi contatti che potrebbero essere il prossimo bersaglio.
- Usa le impostazioni per segnalare il messaggio come spam, quando possibile.

Attività nel dettaglio:

1. Analizziamo gli esempi in gruppo

Dividiamoci in gruppi, ogni gruppo analizzerà degli esempi di messaggi e di siti.

2. Scegliamo individualmente le risposte corrette

Indovina quali sono i tentativi di truffa e quali sono autentici, spiegando di seguito i motivi della tua scelta.

3. Discussione delle risposte in gruppo

Quali sono gli esempi che sembrano affidabili e quali quelli sospetti? C'era qualche risposta che non ti aspettavi?

4. Approfondimento

Ecco alcune altre domande che dovresti farti quando cerchi di capire se i messaggi o i siti che trovi online sono autentici:

- C'è qualcosa di strano in questo messaggio?
  Leggendolo qual è il tuo primo istinto?
  Noti qualcosa di sospetto?

- Nell'email ti viene offerto qualcosa gratuitamente?
  Normalmente le offerte gratuite non sono davvero tali.

- Ti vengono richieste informazioni personali?
  Alcuni siti ti chiedono informazioni personali per poterti mandare altri tentativi di frode. Per esempio, i "test della personalità" potrebbero raccogliere dati per riuscire a indovinare la tua password o sottrarti altre informazioni private. La maggior parte delle imprese reali, viceversa, non chiede informazioni personali via email.

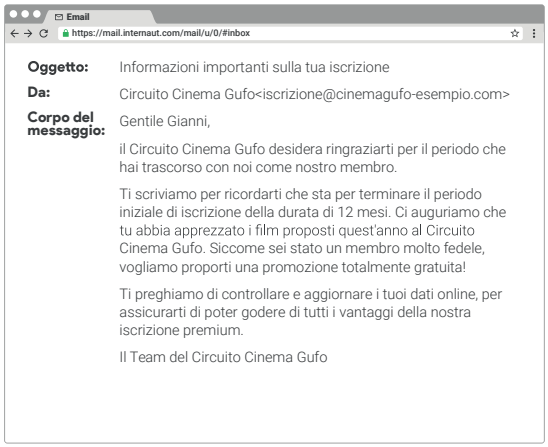
- Si tratta di una catena? Le email e i post in cui ti viene chiesto di far girare il messaggio a tutti i tuoi contatti possono mettere a rischio te e altre persone.
  Non farli girare a meno che tu non conosca la fonte e sappia con certezza che il messaggio è sicuro.

- Contiene parti scritte in piccolo? In fondo alla maggior parte dei documenti puoi trovare delle note scritte con caratteri più piccoli. Questa parte di testo spesso contiene informazioni importanti scritte in piccolo di modo che tu non le legga. Per esempio, potrebbe esserci un titolo in cui ti viene annunciato che hai vinto un telefono in omaggio, ma in piccolo c'è scritto che per averlo devi pagare 200 euro al mese.

Nota.

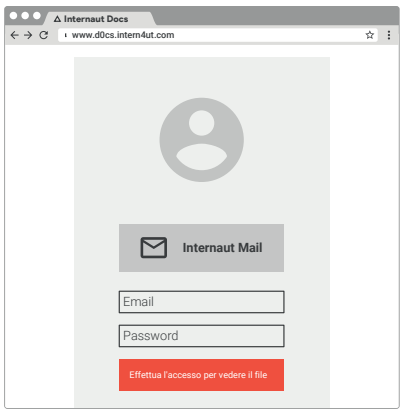
Ai fini di questo esercizio, immagina che Internaut Mail sia un servizio reale e affidabile

Esempi:



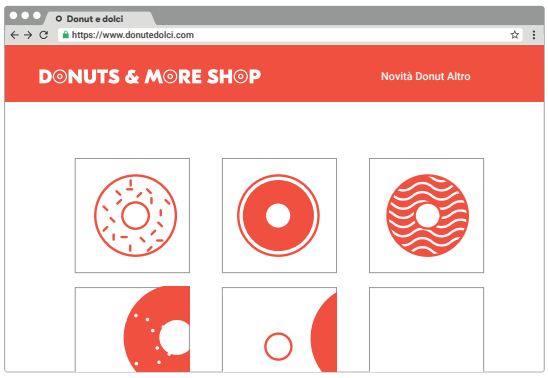
1. Truffa o verità?

Verità _____ Truffa _____



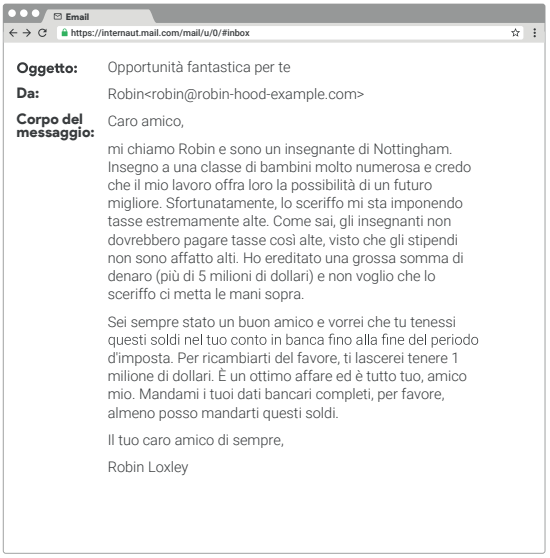
2. Truffa o verità?

Verità _____ Truffa _____



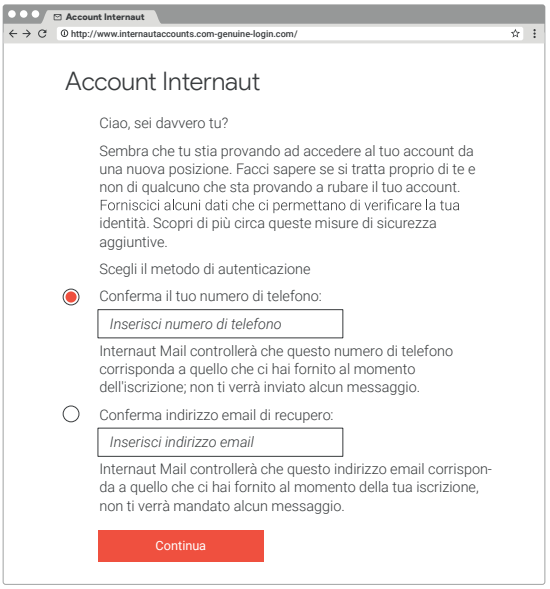
3. Truffa o verità?

Verità _____ Truffa _____



4. Truffa o verità?

Verità Truffa



5. Truffa o verità?

Verità Truffa