

Spam

Per ogni scenario, identificate se si tratta di un messaggio di spam e se dovrete condividere informazioni con tale persona. Scrivete le risposte a ciascuna domanda nello spazio fornito.

Scenario 1

Ricevete un'e-mail da un avvocato che vi informa che un parente lontano vi ha indicato come erede di una somma di denaro. Nell'e-mail vi scrive "Per ricevere il denaro, inviami il numero del tuo conto corrente e il codice di avviamento bancario, in modo da completare il bonifico".

Scenario 2

Un amico vi manda un messaggio, dicendovi che sta cercando di trovare una foto che gli avete mostrato in precedenza ma non ha l'autorizzazione necessaria per vederla. Non potete accedere al vostro computer in quel momento per inviargli la foto. Il vostro amico vi risponde "Posso accedere al tuo account un attimo per scaricare la foto? Qual è la tua password?"

Scenario 3

Ricevete un'e-mail indirizzata a voi dalla vostra scuola, che sostiene che molti account degli studenti sono stati violati. La scuola afferma "Di recente, abbiamo rilevato che molti account di studenti sono stati compromessi. Ci scusiamo e stiamo lavorando per risolvere il problema. Per reimpostare il tuo account, rispondi a questa e-mail fornendo il tuo nome utente e la tua password."

Scenario 4

Ricevete un'e-mail dalla banca con cui avete aperto un conto. L'e-mail afferma che i server della banca sono stati violati e che dovrete effettuare l'accesso per cambiare la password del vostro account il prima possibile e cambiare la password su qualsiasi account che condivida la stessa password.

Spam: copia per l'insegnante

Per ogni scenario, identificate se si tratta di un messaggio di spam e se dovrete condividere informazioni con tale persona. Scrivete le risposte a ciascuna domanda nello spazio fornito.

Scenario 1

Ricevete un'e-mail da un avvocato che vi informa che un parente lontano vi ha indicato come erede di una somma di denaro. Nell'e-mail vi scrive "Per ricevere il denaro, inviami il numero del tuo conto corrente e il codice di avviamento bancario, in modo da completare il bonifico".

Questa e-mail è molto probabilmente spam. Anche se usa correttamente il nome del vostro parente, il mittente potrebbe non essere davvero chi afferma di essere. Il mittente potrebbe aver ottenuto le informazioni sulla vostra parentela attraverso altri mezzi. Condividere le informazioni del vostro conto corrente è sempre rischioso e dovrebbe essere fatto con cautela. Non inviate mai le vostre informazioni a qualcuno a meno che non lo abbiate contattato voi per primi e, anche in questo caso, prestate molta attenzione. Ad esempio, probabilmente non è una buona idea inviare i vostri dati via e-mail, dato che le e-mail non sono crittografate. Ecco perché molti ospedali, avvocati e banche dispongono di siti web speciali per le comunicazioni con i clienti.

Scenario 2

Un amico vi manda un messaggio, dicendovi che sta cercando di trovare una foto che gli avete mostrato in precedenza ma non ha l'autorizzazione necessaria per vederla. Non potete accedere al vostro computer in quel momento per inviargli la foto. Il vostro amico vi risponde "Posso accedere al tuo account un attimo per scaricare la foto? Qual è la tua password?"

Sebbene non si tratti di spam, non dovrete condividere le vostre password con altre persone. Una volta ottenuta la password, possono bloccare il vostro accesso all'account o accedere ad altri account online con la stessa password. Inoltre, se una terza parte, un hacker o un passante vede il vostro messaggio, più persone potrebbero accedere al vostro account a vostra insaputa.

Scenario 3

Ricevete un'e-mail indirizzata a voi dalla vostra scuola, che comunica che molti account degli studenti sono stati violati. La scuola afferma "Di recente, abbiamo rilevato che molti account di studenti sono stati compromessi. Ci scusiamo e stiamo lavorando per risolvere il problema. Per reimpostare il tuo account, rispondi a questa e-mail fornendo il tuo nome utente e la tua password."

È prassi comune non chiedere agli utenti queste informazioni. Anche se il mittente

sembra legittimo, dovrete presumere che qualsiasi e-mail che richiede la vostra password sia spam.

Scenario 4

Ricevete un'e-mail dalla banca con cui avete aperto un conto. L'e-mail afferma che i server della banca sono stati violati e che dovrete effettuare l'accesso per cambiare la password del vostro account il prima possibile e cambiare la password su qualsiasi account che condivide la stessa password.

La procedura corretta è aprire una nuova finestra del browser e accedere al sito come fareste normalmente. Un avviso di questo tipo (ovvero che gli account sono stati violati) in genere sarà menzionato sul portale clienti dell'azienda o della banca. Le istruzioni sul portale dovrebbero essere facili da seguire in modo sicuro. Come nello scenario 3, nessun attore legittimo richiederà le credenziali dell'account via e-mail.