Sicurezza informatica per principianti

Consigli generali ed errori da evitare

1. Riconoscere la provenienza di email, SMS e telefonate fraudolente

La maggior parte delle truffe telematiche è veicolata da telefonate, email ed SMS che hanno tutta l'aria di provenire da enti conosciuti e fonti affidabili, spesso grandi aziende, banche e perfino enti pubblici. Quindi la prima cosa da fare è verificare la provenienza delle comunicazioni, in particolare di quelle che richiedono dati personali, credenziali, codici dispositivi o che invitano a cliccare su un link.

- Verifica l'indirizzo di provenienza delle email e i numeri di telefono da cui provengono telefonate e SMS.
- Controlla attentamente l'indirizzo del mittente delle email e il testo dei link che contengono: spesso i truffatori usano testi che differiscono di poco da quelli ufficiali delle aziende.
- Anche il testo di email e messaggi può darti indicazioni sulla loro natura fraudolenta, poiché spesso contengono errori di ortografia e di sintassi.
- Ricorda infine che talvolta le truffe si articolano in forma complessa, poiché i truffatori possono coordinarsi e agire su più canali (ad esempio effettuando una telefonata in seguito all'invio di SMS).

2. Non avere fretta

Molto spesso le truffe fanno leva sul senso di urgenza e sull'invito ad agire immediatamente. Ad esempio la comunicazione avverte di un servizio in scadenza, di un pagamento non andato a buon fine o della possibilità che un conto corrente venga bloccato e invita ad agire in fretta o addirittura immediatamente.

- In qualsiasi contesto regolare si ha sempre a disposizione del tempo per effettuare il rinnovo di un servizio o per intervenire su un'operazione di pagamento.
- Non agire d'impulso e prenditi il tempo necessario per verificare, ad esempio attraverso una telefonata all'azienda che ti fornisce il servizio o un controllo alla tua area riservata, la veridicità della comunicazione.

3. Fare attenzione alle proposte particolarmente vantaggiose o alle promesse di denaro o guadagni facili

Offerte a prezzi stracciati, prestiti stranamente vantaggiosi e proposte sospette relative al trading online potrebbero rivelarsi delle truffe.

- Verifica sempre la bontà dell'offerta paragonandola ad offerte simili e cercando informazioni sull'offerente.

4. Verificare le pagine web su cui si effettuano i propri acquisti

Nelle pagine web che propongono acquisti è sempre bene fare attenzione alla presenza di alcuni elementi di base, come ad esempio: l'indirizzo "https", la presenza del lucchetto nella barra di indirizzo (che indica che il sito è protetto da sistemi di sicurezza internazionali) e dei dati del venditore, come il numero di Partita IVA, la sede legale della società, i recapiti per il contatto, le condizioni generali di vendita, o un sistema di pagamento sicuro che riporti chiaramente i costi di spedizione.

- Ricorda inoltre che, sul sito dell'Agenzia delle Entrate, puoi verificare i dati fiscali riportati nella pagina web.

5. Usare la massima cautela nella gestione di dati, informazioni e documenti personali

Se ti viene richiesto di comunicare dati personali o sensibili o di inviare copia di documenti personali, devi porre la massima attenzione: invia copia dei tuoi documenti solo se necessario e in un contesto affidabile e accertati dell'identità dell'interlocutore.

6. Mantenere software e password sempre aggiornati

Oltre a modificare periodicamente le password, è necessario che i sistemi operativi e le applicazioni di PC e smartphone siano sempre aggiornati.

- In particolare, verifica che il browser che utilizzi sia aggiornato ed elimina periodicamente i cookie e i file temporanei utilizzando gli appositi strumenti del browser.

Sono caduto vittima di una truffa, cosa posso fare?

Essere vittima di una truffa è un'evenienza che può capitare a chiunque. Se, nonostante tutte le precauzioni messe in atto, sei caduto vittima di una truffa è sempre possibile attivarsi per denunciare quanto accaduto alle forze dell'ordine. Nel caso si tratti di una truffa avvenuta online, è opportuno fare riferimento alla Polizia Postale che ha competenza sui reati informatici.

- Raccogli tutto il materiale che può provare quanto accaduto.
- Inoltre, se temi di essere rimasto vittima di una truffa bancaria, contatta il tuo Istituto di credito per bloccare le carte di pagamento e per verificare che non vi siano state disposizioni di pagamento fraudolente.

Convinzioni sbagliate sulla sicurezza informatica

Mito: Cliccando sui link "annulla iscrizione" presenti nelle email di spam, queste verranno interrotte.

Fatto: Cliccando su tali link, il tuo indirizzo email potrebbe essere confermato dagli spammer, aumentando potenzialmente la quantità di spam.

- Ecco alcuni modi più sicuri per annullare l'iscrizione e gestire le e-mail di spam:
    - Imposta dei filtri nel tuo client di posta elettronica per spostare automaticamente le email di spam nella cartella posta indesiderata o spam.
    - Utilizza l'opzione "Segnala come spam" nel tuo client di posta elettronica per addestrare il filtro antispam a riconoscere e bloccare email simili.
    - Utilizza il link "annulla iscrizione" solo se riconosci il mittente e ti fidi dell'email. Per le altre email, è più sicuro eliminarle senza cliccare su alcun link.

Mito: Il ripristino delle impostazioni di fabbrica cancella completamente tutti i dati dal mio dispositivo.

Fatto: Dopo un ripristino delle impostazioni di fabbrica è comunque possibile recuperare i dati, a meno che non vengano sovrascritti correttamente con un software specializzato.

Mito: Il mio dispositivo è sicuro se non mi connetto mai a Internet.

Fatto: Anche i dispositivi offline possono essere vulnerabili al malware tramite unità USB o altre connessioni fisiche.

Mito: Chiudere il coperchio del portatile equivale a disconnettersi.

Fatto: La chiusura del coperchio sospende solo il sistema. Non ti disconnette, lasciando la tua sessione vulnerabile a accesso non autorizzato. Si consiglia di disconnettersi dal computer.

Mito: La modalità aereo è sufficiente per proteggere il tuo dispositivo durante il volo.

Fatto: Sebbene la modalità aereo disattivi i segnali wireless, non protegge da malware preinstallati o da accessi non autorizzati in caso di accesso fisico al dispositivo.

Proteggere la tua sicurezza e privacy sui social media

Consigli:

- **Usa password forti e uniche:** Crea password complesse e diverse per ogni account. Utilizza un gestore di password per memorizzarle in modo sicuro.
- **Abilita l'autenticazione a due fattori (2FA):** Aggiungi un ulteriore livello di sicurezza richiedendo un secondo fattore di verifica oltre alla password.
- **Controlla le impostazioni di privacy:** Rivedi e aggiorna regolarmente le impostazioni di privacy per limitare chi può vedere le tue informazioni e i tuoi post.
- **Fai attenzione ai link sospetti:** Non cliccare su link sospetti o provenienti da fonti non affidabili, poiché potrebbero essere tentativi di phishing.
- **Limita le informazioni personali condivise:** Evita di condividere dettagli sensibili come indirizzo, numero di telefono o informazioni finanziarie.
- **Usa reti Wi-Fi sicure:** Evita di connetterti a reti Wi-Fi pubbliche non protette per accedere ai tuoi account social.
- **Verifica le autorizzazioni delle app:** Controlla quali permessi concedi alle app sui social media e limita l'accesso ai dati non necessari.
- **Monitora le attività sospette:** Tieni d'occhio attività insolite sui tuoi account e segnala immediatamente eventuali problemi.
- **Educa te stesso e gli altri:** Informati sulle migliori pratiche di sicurezza e condividi queste informazioni con amici e familiari.

Errori da Evitare:

- **Usare la stessa password per più account:** Se un account viene compromesso, tutti gli altri con la stessa password sono a rischio.
- **Ignorare gli aggiornamenti di sicurezza:** Non aggiornare regolarmente le app e i dispositivi può lasciare vulnerabilità sfruttabili.
- **Accettare richieste di amiccizia da sconosciuti**: Potrebbero essere profili falsi creati per raccogliere informazioni personali.
- **Condividere la posizione in tempo reale:** Evita di condividere la tua posizione attuale, soprattutto in post pubblici.
- **Non fare il logout dai dispositivi condivisi:** Lasciare il tuo account aperto su dispositivi condivisi può permettere ad altri di accedere alle tue informazioni.
- **Non monitorare le attività sospette:** Ignorare segnali di attività insolite sui tuoi account può portare a problemi di sicurezza.
- **Condividere troppe informazioni personali:** Pubblicare dettagli sensibili può facilitare il furto di identità.
- **Non educarsi sulle pratiche di sicurezza:** La mancanza di conoscenza può renderti vulnerabile agli attacchi.

Quiz

1. Come si può verificare la provenienza di un'email sospetta?

a) Cliccando direttamente sui link presenti nell'email.

b) Verificando attentamente l'indirizzo del mittente e il testo dei link.

c) Rispondendo immediatamente all'email per chiedere conferma.

d) Inoltrando l'email a tutti i contatti per avvisarli.

2. Qual è un segnale di allarme nelle comunicazioni fraudolente?

a) La presenza di offerte particolarmente vantaggiose.

b) L'assenza di errori di ortografia e sintassi.

c) La richiesta di agire con calma e senza fretta.

d) La provenienza da un numero di telefono conosciuto.

3. Cosa fare di fronte a una proposta di trading online sospetta?

a) Investire immediatamente per non perdere l'opportunità.

b) Verificare la bontà dell'offerta confrontandola con altre simili.

c) Comunicare i propri dati finanziari per ricevere maggiori informazioni.

d) Condividere l'offerta sui social media per avere pareri.

4. Quali elementi indicano l'affidabilità di una pagina web di acquisti?

a) La presenza di offerte a prezzi stracciati.

b) L'indirizzo "https" e il lucchetto nella barra di indirizzo.

c) L'assenza di dati del venditore.

d) La richiesta di pagamento tramite bonifico bancario.

5. Come gestire la richiesta di comunicare dati personali o sensibili?

a) Inviare subito tutti i documenti richiesti.

b) Inviare i documenti solo se necessario e in un contesto affidabile.

c) Condividere i dati sui social media per maggiore sicurezza.

d) Ignorare la richiesta per evitare rischi.

6. Perché è importante mantenere software e password aggiornati?

a) Per ricevere notifiche pubblicitarie personalizzate.

b) Per proteggersi dalle vulnerabilità e dai rischi di sicurezza.

c) Per velocizzare la navigazione internet.

d) Per aumentare lo spazio di archiviazione del dispositivo.

7. Cosa fare in caso di truffa online?

a) Inviare un'email di protesta al truffatore.

b) Contattare la Polizia Postale e raccogliere tutto il materiale probatorio.

c) Cancellare tutti i propri account online.

d) Condividere l'accaduto sui social media per avvisare gli altri utenti.

8. Quale delle seguenti è una buona pratica per la sicurezza online?

a) Usare la stessa password per tutti gli account.

b) Cliccare su link sospetti per curiosità.

c) Abilitare l'autenticazione a due fattori (2FA).

d) Condividere la propria posizione in tempo reale sui social media.

9. Quale errore comune aumenta il rischio di essere vittima di truffe?

a) Aggiornare regolarmente le app e i dispositivi.

b) Verificare le autorizzazioni delle app.

c) Usare reti Wi-Fi pubbliche non protette.

d) Utilizzare password forti e uniche.

10. Cosa si intende per Phishing?

a) Una tecnica per migliorare la connessione internet.

b) Un tentativo di ottenere informazioni sensibili tramite link sospetti.

c) Un metodo per aggiornare automaticamente i software.

d) Un sistema di pagamento online sicuro.

Soluzioni:

1. b
2. a
3. b
4. b
5. b
6. b
7. b
8. c
9. c
10. b