

CYBER SECURITY

Truffe Online: Come Riconoscerle e Proteggersi

INTRODUZIONE



- Le truffe online sono sempre più sofisticate e diffuse.
- Il tempo che quotidianamente trascorriamo online è sempre di più, così come sono più numerose le azioni che svolgiamo tramite Internet. Senza dubbio oggi siamo utenti più esperti e più avvezzi alle tecnologie informatiche. Questo però non ha determinato un calo delle truffe online: al contrario dove ci sono più utenti, ci sono anche più occasioni di effettuare frodi online.
- È importante conoscere i vari tipi di truffe per proteggersi efficacemente.



RICORDA:

La difesa più efficace contro gli attacchi informatici è la tua consapevolezza.

Ricorda che i truffatori non possono far nulla senza il tuo aiuto.



Impara a smascherare i tentativi di frode

- Via e-mail, SMS, Whatsapp o telefonata potrebbero chiederti di cliccare su un link, aprire un allegato e inserire o comunicare i tuoi dati o codici. Non farlo.



Proteggi il tuo PC e il tuo smartphone

- Installa e tieni aggiornato sul tuo PC o sullo smartphone un programma antivirus.



Tieni alta la guardia

- Non memorizzare dati e codici nei browser utilizzati per navigare online.

RICORDA:



NON SARAI MAI CONTATTATO

- Per chiedere telefonicamente o via SMS i tuoi codici segreti per intero o i dati della carta di pagamento.
- Per chiedere di effettuare un trasferimento di denaro dal tuo conto corrente o dalle tue carte per bloccare un pagamento sospetto o per verifiche di sicurezza.
- Per contattare numeri di telefono differenti da quelli dell'istituto
- Per attivare sul tuo cellulare il trasferimento di chiamata o di concedere l'accesso remoto al tuo dispositivo.



LE TRUFFE ONLINE - 1



- **Il tipico messaggio è:**

"Gentile utente, durante i regolari controlli sugli account non siamo stati in grado di verificare le sue informazioni; in accordo con le nostre regole, abbiamo bisogno di confermarle le sue reali informazioni. È sufficiente che lei completi il modulo che le forniremo. Se ciò non dovesse avvenire, saremo costretti a sospendere il suo account."



LE TRUFFE ONLINE - 2



- Fai attenzione a non inviare dati personali ed in particolare codici PIN o numeri di carte di credito o di bancomat via mail o attraverso il telefono cellulare.
- Se ricevi e-mail dubbie, contatta i mittenti o la polizia postale, ma non utilizzare o contattare mai gli indirizzi o i canali forniti nell'e-mail.
- Non aprire e-mail provenienti da indirizzi sconosciuti, in particolare se con allegati.
- Non utilizzare password banali come data di nascita, nomi propri di familiari ecc. nè, possibilmente, parole presenti sul dizionario.

SPINTA AL PAGAMENTO FRAUDOLENTO



- I frodatori potrebbero contattarti fingendo di essere la banca, facendo apparire il numero di Banca Mediolanum come numero chiamante o inviarti un SMS, affermando che sei stato vittima di una frode e che devi trasferire i tuoi soldi su un conto bancario o fornire i dati della tua carta.



TRUFFA DELL'INVESTIMENTO



- Quando ti vengono proposte opportunità d'investimento insolitamente redditizie, generalmente sulle criptovalute o mercati esteri, presta attenzione, perchè potrebbe trattarsi di "Investment scam". Spesso si riceve una telefonata inaspettata dove la persona al telefono propone investimenti con rendimenti rapidi e particolarmente alti ponendosi in modo insistente



TRUFFA DELL'EMERGENZA FAMILIARE



- Il truffatore che attua una "Family emergency scam" si finge un membro della tua famiglia o un tuo amico e potrebbe contattarti per telefono, SMS, email o social media, fingendo di avere qualche tipo di problema e di aver bisogno di soldi immediatamente, fornendo un IBAN a cui bonificare una somma.



LA TRUFFA DEL PACCO BLOCCATO



1. **Modalità della truffa:** I truffatori inviano SMS o email fingendo di essere corrieri, informando che un pacco è bloccato e richiedendo un'azione per sbloccarlo. Questi messaggi spesso contengono link che portano a pagine fraudolente.
2. **Obiettivo:** Indurre le vittime a cliccare sui link e inserire dati personali e bancari, che vengono poi utilizzati per frodi finanziarie.
3. **Segnali di allarme:**
 - Messaggi che richiedono azioni urgenti.
 - Link che iniziano con “http” invece di “https”.
 - Richieste di pagamento per sbloccare il pacco.
4. **Come proteggersi:**
 - Non cliccare sui link ricevuti via SMS o email.
 - Verificare lo stato delle spedizioni direttamente sui siti ufficiali dei corrieri.
 - Segnalare e bloccare i numeri o gli indirizzi email sospetti.
5. **Cosa fare se si è caduti nella truffa:**
 - Formattare il dispositivo.
 - Informare i contatti di eliminare eventuali messaggi sospetti.
 - Cambiare le password e monitorare i movimenti bancari.

I TIPI DI PHISHING



- **Phishing di Reconnaissance:** raccogliere informazioni sulle potenziali vittime. I criminali informatici analizzano siti web, social media e utilizzano strumenti di raccolta di informazioni online per creare messaggi di phishing mirati.
- **Email Phishing:** il tipo più comune, questo metodo implica l'invio di email di massa in cui gli hacker impersonano un'identità o un'organizzazione legittima. Queste email spesso contengono un senso di urgenza per indurre la vittima a cliccare su un link dannoso.
- **Spear Phishing:** A differenza del phishing di massa, lo spear phishing si rivolge a individui specifici all'interno di un'organizzazione. Le email sono personalizzate per far credere alla vittima di avere una relazione con il mittente.

I TIPI DI PHISHING



- **Whaling:** Questo tipo di phishing prende di mira dirigenti di alto livello all'interno di un'organizzazione. Gli attacchi sono altamente personalizzati e mirano a ottenere informazioni sensibili o a indurre il dirigente a compiere azioni specifiche.
- **Smishing:** Questo metodo utilizza messaggi di testo (SMS) per indurre le vittime a cliccare su link dannosi o a fornire informazioni personali[.
- **Vishing:** Simile allo smishing, il vishing utilizza chiamate telefoniche per ingannare le vittime e ottenere informazioni sensibili.
- **Phishing di Spam (Pubblicità):** Questo tipo di phishing utilizza email fraudolente per rubare informazioni personali, spesso utilizzando tecniche di ingegneria sociale per convincere le vittime a cliccare su link o scaricare allegati dannosi.

I BARCODE & QR-CODE → QUISHING



Il quishing è una forma di phishing che utilizza codici QR per ingannare le vittime e ottenere informazioni personali o finanziarie¹.

Meccanismo:

- Gli utenti scansionano un codice QR contraffatto.
- Vengono reindirizzati a un sito web ingannevole che richiede l'inserimento di dati sensibili o scaricano malware².

Diffusione:

- Aumento dei casi in vari contesti come ristoranti, parcheggi e colonnine di ricarica per veicoli elettrici².
- Particolarmente diffuso in paesi come Belgio, Olanda, Francia, Germania e Italia.



I BARCODE & QR-CODE → QUIISHING



Segnali di Allarme:

- Codici QR in luoghi non ufficiali o sospetti.
- Richieste di informazioni personali o finanziarie dopo la scansione¹.

Misure di Prevenzione:

- Verificare l'autenticità del codice QR prima di scansionarlo.
- Utilizzare app che controllano la sicurezza del sito di destinazione.
- Educare se stessi e gli altri sui rischi del quishing e su come identificarli.



LE TRUFFE ONLINE – COME CONTRASTARLE



- Cambia le password con una certa regolarità ed evita di annotarle in luoghi facilmente accessibili.
- Mantieni costantemente aggiornato il sistema antivirus del tuo personal computer.
- Installa un sistema (firewall) che filtra i dati in entrata e in uscita dal tuo computer.
- Prima di effettuare acquisti on-line verifica che il sito sia certificato e sicuro e di avere tutte le informazioni sul venditore.
- Cerca di pagare gli acquisti fatti su internet con modalità sicure: in contrassegno, con bonifico bancario o con carte prepagate.

CONCLUSIONE



La consapevolezza è la prima linea di difesa contro le truffe online.



Seguire i consigli di sicurezza può aiutare a proteggere le proprie informazioni personali.



Rimanere sempre vigili e informati sulle nuove tecniche di truffa.



SITI & SERVIZI UTILI PER EVITARE LE TRUFFE



- <https://www.yourlifeupdated.net/news/siti-truffa-elenco-aggiornato-dei-siti-pericolosi/>
- <https://www.cybersecurity360.it/nuove-minacce/truffe-online-le-piu-diffuse-come-riconoscerle-e-i-consigli-per-difendersi/>
- <https://www.truffa.net/> ➔ <https://www.truffa.net/truffe-online/>