



### Cos'è il Pharming?

Nel Pharming, la vittima si ritrova ad utilizzare un dispositivo infettato da **un malware sviluppato per modificare gli URL** che vengono digitati. La vittima viene quindi reindirizzata verso **siti contraffatti che sono però in apparenza identici ai siti originali** e inserisce ignara i propri dati sensibili.

I siti bancari e le piattaforme di pagamento online sono tra i portali che vengono più spesso contraffatti.

In questo modo **i criminali possono acquisire informazioni sensibili** come le credenziali di accesso ai servizi di home banking o i dati delle carte di credito.

### Come riconoscere un attacco

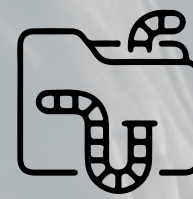
Potresti essere vittima di Pharming se scopri:

- addebiti imprevisti su carte di credito o Paypal;
- password e credenziali di accesso modificate;
- nuovi post non pubblicati personalmente sui social media;
- nuove applicazioni installate sul tuo dispositivo.

### Come proteggersi?

**Un attacco Pharming può colpire un singolo dispositivo o, molto peggio, un intero server**, reindirizzando ogni utente che cerca di visitare un sito legittimo verso quello fraudolento. Ecco alcune buone regole da seguire per proteggersi:

- evitare di cliccare su URL provenienti da fonti sconosciute;
- evitare i banner o i siti web sospetti;
- diffidare da offerte "esagerate" su siti di e-commerce;
- dotarsi di un software antivirus robusto e aggiornabile.



### Cos'è il Quishing?

**Il Quishing è una tecnica di attacco basata sulla possibilità che l'ignara vittima inquadri un QR code malevolo.** I QR code malevoli possono contenere informazioni false, indirizzamenti a siti compromessi o fasulli e non ultimo il download di malware o ransomware.

### Come non caderne vittima?

Prima di scansionare un codice QR, **assicurarsi che il codice non sia stato manomesso**, ad esempio con un adesivo posizionato sopra l'immagine originale.

Dopo aver scansionato il codice QR, **controllare sempre l'URL** per assicurarsi che si tratti del sito previsto e del contenuto autentico.

#### **Non scaricare app partendo da un codice QR.**

Per un download più sicuro è consigliabile utilizzare sempre gli store ufficiali.

#### **Attenzione ai pagamenti!**

**Usare il QR code solo su siti e negozi sicuri** e fare molta attenzione alla richiesta di dati sensibili.

Il reparto tecnico di Eli-net è a tua disposizione per effettuare **una completa analisi della tua infrastruttura informatica.**

Al termine di questa attività ti verrà fornito e un report nel quale saranno evidenziati i settori più deboli e le aree che richiedono miglioramenti, compresi i comportamenti pericolosi degli utenti nell'uso dei dispositivi in dotazione.

**Ti indicheremo quindi le soluzioni da apportare per mettere in sicurezza i sistemi informatici, i tuoi dati e la continuità operativa della tua azienda.**