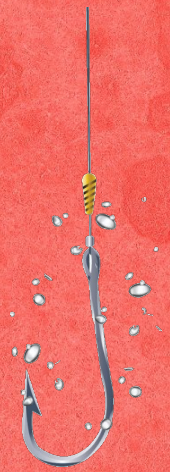
UN ATTACCO PHISHING È GENERALMENTE CARATTERIZZATO DA:

- ➔ **ESCA**
- ➔ **AMO**
- ➔ **CATTURA**



L'ESCA

L'esca è un "richiamo" consegnato tramite e-mail che incoraggia il destinatario a seguire un collegamento ipertestuale (URL) contraffatto.

L'AMO

L'amo è rappresentato dal link malevolo contenuto nell'esca e offuscato in maniera tale che sia molto simile a quello che la vittima ritiene legittimo. Il link conduce a un sito web sotto il controllo dell'aggressore, tramite il quale si chiede di divulgare informazioni relative alla privacy della vittima, come username e password.

LA CATTURA

La cattura avviene quando "il phisher" (auto re dell'attacco di phishing) utilizza le informazioni raccolte dall'amo per mascherarsi con l'identità della vittima e condurre transazioni finanziarie illegali.

IL PHISHING NELLE AZIENDE

Oggi più che mai, gli attacchi di phishing si stanno concentrando su precisi obiettivi per compromettere la sicurezza aziendale. Per questo motivo, è importante capire come identificare un'e-mail di phishing e quali misure intraprendere per prevenire il "furto di identità".

Ricorda di...

FERMARTI e PENSARE, prima di CLICCARE !

UN CLIC potrebbe compromettere...

- ✔ Le tue informazioni personali
- ✔ Le informazioni della tua agenzia
- ✔ Il sistema del tuo computer
- ✔ Le informazioni del tuo computer

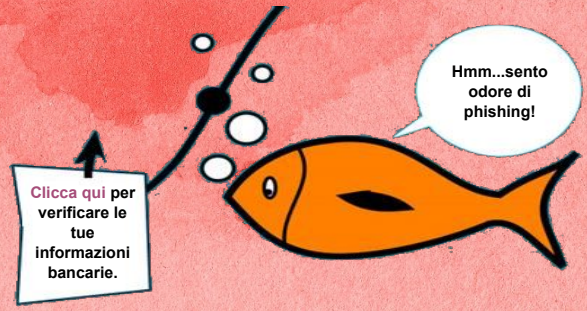
RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/phishing/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

PHISHING E FURTI DI IDENTITÀ

Scopri cos'è il phishing e proteggiti dai "pescatori" di dati personali.



1. Il phishing

Il **phishing** è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso, numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

2. Come avviene la truffa

La truffa avviene di solito via **e-mail**, ma possono essere utilizzati anche sms, chat e social media. Il **"ladro di identità"** si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc. .

3. Come riconoscere una e-mail di phishing

In genere, i messaggi di phishing **invitano a fornire direttamente i propri dati personali**, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

4. Il buon senso prima di tutto

Dati, codici di accesso e password personali non dovrebbero **mai essere comunicati a sconosciuti**. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali.
Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere malware capaci di prendere il controllo di pc e smartphone.

5. Occhio agli indizi

I messaggi di phishing sono **progettati per ingannare** e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.
È utile anche prestare attenzione al **mittente** (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).
Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

6. Proteggersi meglio

È utile installare e tenere aggiornato sul pc o sullo smartphone un **programma anti-malware** che protegga anche dal phishing. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare **password alfanumeriche complesse**, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato.

7. Acquisti online in sicurezza

Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.

8. La prudenza non è mai troppa

Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare **sistemi di alert automatico** che avvisano l'utente di ogni operazione effettuata.