Guida per difendersi dalle truffe online

Ivan Campari

Ritorniamo su alcune delle truffe online più comuni con i nostri consigli concreti per difendersi.

Tre tipologie di truffe fra le più comuni

Phishing

Il *phishing* è un attacco il cui scopo è carpire dati personali alla vittima. Il *phisher* contatta la vittima facendo credere di essere qualcun altro, generalmente un'azienda con la quale la vittima ha un qualche tipo di rapporto (per esempio la sua banca). Per riuscire nell'inganno, il truffatore può per esempio inviare un'e-mail che simula l'aspetto delle e-mail inviate dall'azienda in questione. Tale comunicazione invita la vittima a fornire dei dati sensibili, come username o password. Spesso i tentativi di *phishing* contengono link che portano a siti fasulli, che appaiono identici agli originali. Molti attacchi di *phishing* hanno lo scopo di raccogliere più informazioni possibili su una persona o su un'azienda, in modo da poterla attaccare più efficacemente in un secondo momento. Questa tipologia di *phishing* atta a testare il terreno per affondare il colpo in un secondo momento è definita *spear phishing*. Il *phishing* può anche essere telefonico.

Spoofing

Lo *spoofing* è una truffa informatica che riguarda la falsificazione dell'identità. In alcuni casi lo scopo può essere identico al *phishing* (impersonare qualcun'altro per carpire dei dati personali), ma può anche avere obiettivi differenti. Per esempio, assumere l'identità di qualcuno potrebbe servire per diffondere informazioni false, per superare determinati controlli di sicurezza o per avere accesso a dati sensibili. Lo *spoofing* può anche riferirsi alla falsificazione di alcune informazioni personali: per esempio, le informazioni geografiche (dare l'impressione di trovarsi in un luogo geografico diverso rispetto a quello dove realmente ci si trova). Si parla di *spoofing* anche quando gli autori fanno in modo di falsificare il mittente di un messaggio e-mail, per dare l'idea che provenga da una persona o un'entità affidabile. In questo caso, basta verificare l'indirizzo e-mail anziché fidarsi dell'intestazione. Operazione semplice che però la maggioranza delle persone non fa.

Pharming

Il *pharming*, termine nato dall'unione di *phishing* e *farming* (letteralmente "coltivare") è la pratica di ridirigere il traffico da un sito internet ad un altro. Per raggiungere questo scopo, l'autore potrebbe in un primo momento istallare un virus sul computer della vittima. Per farlo, può essere sufficiente un'e-mail contente un link sul quale la vittima clicca inavvertitamente, scaricando in questo modo il programma malevolo sul suo computer. Il virus farà poi in modo che quando la vittima si recherà su un determinato sito internet, anche se digita l'indirizzo corretto, verrà ridirezionata su un altro sito. Questo sito clone, preparato ad hoc dal truffatore, è una trappola per raccogliere i dati personali dei visitatori (quasi come una *coltivazione* di dati personali... da lì, *farming*). In alcuni casi il *pharming* può essere utilizzato per colpire un'intera rete di computer, magari una rete aziendale, facendo sì che tutti coloro che si trovano in quella rete verranno ridirezionati al sito fasullo.

Indizi che dovrebbero portare ad avere una maggiore diffidenza

- Denaro che piove dal cielo: vincite a lotterie, prezzi stracciati, eredità di parenti sconosciuti...
- Improvvise proposte romantiche da parte di persone molto attraenti
- Proposte di lavoro estremamente interessanti
- Prese di contatto o richieste di pagamento tramite canali inusuali (per esempio, prenotazione che avviene su un sito ma arriva poi la richiesta di chattare altrove, oppure e-mail non corrispondenti, pagamenti attraverso canali esterni...)
- Richieste in lingue straniere, o in italiano da traduttore automatico

Come difendersi se si viene presi di mira

- Verificare l'identità del proprio interlocutore (provenienza e-mail, telefonate, sms). Attenzione, il numero di telefono è falsificabile
- Controllare attentamente su quale sito internet ci si trova e se compaiono avvisi di sicurezza che segnalano per esempio una connessione non sicura
- Attenzione ai messaggi o alle richieste di amicizia sui social media: i truffatori possono clonare i profili di persone conosciute ed utilizzare il profilo clone per prendere contatto
- Non cliccare su link provenienti da fonti non accertate (inclusi quelli ricevuti via sms!)
- Fare una verifica aggiuntiva tramite un canale differente in caso di dubbio sull'identità di un interlocutore (l'ideale sarebbe vedersi di persona, altrimenti al telefono)
- Non avere fretta. La fretta è una componente essenziale delle truffe, perché quando si agisce di fretta si diventa più irrazionali e disattenti
- Prestare attenzione ogniqualvolta vengono richiesti dati personali
- Far bloccare immediatamente la carta di credito in caso di smarrimento o di incongruenze nelle fatture
- Cambiare i propri dati di accesso se si smarrisce un apparecchio o in caso di furto (smartphone, computer...)

Buone norme per prevenire i problemi e dormire sonni più tranquilli

- Mantenere sempre aggiornate le applicazioni e i sistemi operativi
- Usare password complesse e diverse. Non occorre ricordarle tutte, ci si può far aiutare da un *password manager*
- Attivare sempre la doppia autenticazione per i propri accessi
- Lasciare meno informazioni possibili su di sè online
- Non utilizzare wi-fi pubblici per accedere a siti o applicazioni sensibili
- Non dare accesso a terzi alla propria rete internet fissa o mobile senza password
- Ridurre al minimo la condivisione di informazioni sui social media anche tramite i settaggi della privacy
- Non recarsi su siti "poco raccomandabili" per guardare contenuti piratati. Spesso questi siti contengono virus o link fraudolenti

Conclusione

L'informatica è una materia indubbiamente complessa. Tuttavia, la realtà è che la netta maggioranza delle truffe e delle fregature si basa su banali errori umani. Delle norme abbastanza basilari permettono quindi di difendersi in maniera efficace. È possibile evitare la maggior parte dei problemi semplicemente astenendosi dall'aprire messaggi o cliccare su link provenienti da fonti sconosciute. Se si è in dubbio sulla reale identità del proprio interlocutore, meglio fermare tutto e prendersi il tempo di verificare con calma con chi ci si sta realmente relazionando. Infine, un po' di sana diffidenza dovrebbe permettere di distinguere ciò che è verosimile da ciò che "puzza" da un miglio di distanza. Anche qui, se qualcosa "sembra strano", prendersi il tempo di riflettere prima di cliccare non può certo recare danni.