Truffe nel mondo digitale

di Silvano Marioni


Foto: TeruleanSon da Pixabay

È semplice comprendere i rischi che ci circondano nella nostra vita quotidiana ma è più difficile avere la consapevolezza di quelli presenti nel mondo digitale, un ambiente spesso sconosciuto e caratterizzato da una maggiore complessità.
Di questo ne approfittano truffatori che, sfruttando la poca dimestichezza delle persone con la tecnologia, creano nuovi inganni che sono spesso difficili da immaginare.
Ad esempio non è evidente come dobbiamo reagire di fronte a messaggi di posta elettronica o di WhatsApp che ci chiedono di rispondere rapidamente in situazioni poco chiare o come comportarci con sconosciuti che ci contattano pretendendo di darci supporto tecnico per presunti problemi del nostro computer.
È difficile elencare tutte le possibili truffe escogitate dalla creatività dei malfattori, ma sono ben conosciuti i meccanismi comuni che le caratterizzano. Per ingannare le persone vengono utilizzate diverse tecniche che fanno spesso leva su precise emozioni e stati d'animo come l'avidità, la curiosità, la paura e l'urgenza di reagire a una minaccia (conti bloccati, multe, spese strane, accessi non autorizzati). Questi tranelli sono così ben congegnati che ci spingono a fare cose che non faremmo mai nella vita reale, come consegnare dei soldi a uno sconosciuto. Se non stiamo attenti il rischio è di mettere a repentaglio i nostri dati, le nostre informazioni, i nostri averi e, con quelli, a volte anche la qualità della nostra vita.

Vincita milionaria - Tra le truffe più conosciute per rubare soldi c'è la vincita milionaria a una lotteria inesistente che può essere incassata solo dopo aver mandato un importo necessario per il disbrigo delle pratiche. Naturalmente la vincita è fasulla ma l'importo inviato è reale.

Proposta sentimentale - Un altro tipo di truffa è quella sentimentale in cui il truffatore aggancia una persona fragile e sola con l'intento di costruire un'illusoria relazione a distanza, grazie alla quale, con varie scuse, riesce poi a farsi versare dei soldi.

Oggetti inesistenti - Attenzione anche alle vendite di oggetti inesistenti che vengono presentati con delle tecniche architettate in modo tale che, senza consegnare nulla, il malvivente riesce a prendere i soldi e a sparire senza tracce.

Furto di password - Non meno pericolose sono le truffe che cercano di rubare le password o i codici di accesso ai conti finanziari. Una tecnica molto usata è quella del "phishing", termine che deriva dalla storpiatura della parola inglese fishing, pescare. Si cerca infatti di pescare le informazioni di una persona tramite l'invio di messaggi, naturalmente falsi, che sembrano inviati da un ente affidabile. Questi messaggi sollecitano, ad esempio, l'accesso al sito di una banca per una verifica dei dati oppure per controllare un addebito o una fattura. Naturalmente cliccando sul link indicato si è dirottati su un sito fasullo, che si presenta esattamente come quello vero, con la richiesta del nome utente e della password. Se si prosegue inserendo quanto chiesto, i malfattori avranno i dati necessari per accedere al conto del malcapitato. Questi messaggi non riguardano solo la posta elettronica ma possono arrivare anche sullo smartphone tramite SMS o WhatsApp. È fondamentale ricordarsi che nessuno sconosciuto ci chiederà mai la password o il numero di carta di credito con un messaggio su internet o per telefono, e se dovesse avvenire siamo sicuramente di fronte a un truffatore. Altri tipi di truffa fanno leva sull'avidità. Come l'offerta di prodotti a prezzi inspiegabilmente vantaggiosi da parte di malfattori che attirano le persone solo per carpire i dati della carta di credito senza poi spedire nulla.

Consigli utili - Una buona regola a riguardo dei messaggi ricevuti da persone ignote è quella di non cliccare mai sui link o aprire gli allegati presenti nel messaggio, soprattutto se siamo indotti a farlo con un certo senso di urgenza. Il rischio è quello di installare sul nostro computer, o sul nostro smartphone, il software malefico che può rubare o danneggiare i nostri dati. Nel caso di messaggi sospetti provenienti da aziende o da persone che si conoscono, è meglio contattarle per verificarne l'autenticità. Uno stratagemma utile, che funziona molto bene per controllare la veridicità di un messaggio, è quello di cercare su Google il testo del messaggio ricevuto per vedere se ci sono altre persone che lo indicano come falso e pericoloso.
In un settore in continua evoluzione come l'informatica, l'atteggiamento corretto è quello di essere coscienti che esistono dei rischi e che cambiano continuamente. Conoscere questi rischi e avere dei comportamenti prudenti e attenti ai possibili inganni è fondamentale per garantire la nostra sicurezza, non solo nel mondo digitale, ma anche nella nostra vita reale.