

27.07.2026

Truffe informatiche: le tendenze da conoscere

L'intelligenza artificiale, i nuovi canali di attacco e il furto mirato di identità stanno cambiando radicalmente il panorama delle minacce nello spazio digitale. Ecco gli sviluppi che bisogna conoscere.

Ciò che un tempo era facilmente smascherabile come truffa, spesso oggi sembra autentico. E quindi è molto più pericoloso. Vi presentiamo qui alcune tendenze particolarmente importanti che riguardano direttamente i consumatori finali.

Quando la truffa raggiunge livelli di autenticità davvero ingannevoli

I criminali informatici usano sempre più l'intelligenza artificiale per rendere gli attacchi più perfetti e credibili. Un esempio particolarmente subdolo è quello che riguarda le cosiddette truffe deepfake, con le quali le vittime ricevono una telefonata da quella che sembra una persona che conoscono, come un familiare o la loro banca, quando in realtà si tratta di una voce creata al computer.

Allo stesso tempo, anche le classiche e-mail di phishing hanno cambiato forma radicalmente. Grazie all'IA, oggi non ci sono errori di grammatica, la formulazione è personalizzata e spesso talmente adattata alla singola persona da rendere quasi irriconoscibile il fatto che i messaggi siano fraudolenti.

Per i consumatori finali, ciò significa che ci si può affidare sempre meno all'istinto come in passato. La fiducia da sola non basta più: anche i contatti apparentemente reali andrebbero passati al setaccio dell'occhio critico.

Attacchi multicanale

Gli attacchi informatici non si limitano più alle e-mail. Piuttosto, i criminali utilizzano intere catene di attacchi su diverse piattaforme, dai messaggi brevi (SMS ecc.) ai social media e ai siti Internet falsi. Una tendenza recente sono le cosiddette truffe multicanale, con attacchi che ad esempio cominciano con un SMS, usano un link che dirige su un sito contraffatto e terminano con una chat o una richiesta di pagamento. Sono in chiaro aumento anche il phishing con codice QR e i messaggi di tutti i giorni dall'aspetto ingannevolmente autentico, che riguardano p. es. abbonamenti, consegne o fatture.

I truffatori, quindi, sfruttano con precisione sempre maggiore le situazioni quotidiane. Ogni canale – dalla cassetta delle lettere all'app di messaggistica – può diventare il punto di ingresso per un attacco.

Furto dell'identità: viso e voce nel mirino

Oltre alle password, i criminali informatici ora ambiscono anche a dati biometrici come il viso, la voce o il comportamento. Una nuova tendenza è infatti rappresentata dalle offerte di lavoro false o dai presunti colloqui di lavoro via video, nei quali le vittime trasmettono senza rendersene conto dati riguardanti il proprio viso e la voce. Si tratta di informazioni che poi possono essere utilizzate per eludere i meccanismi di sicurezza, ad esempio nelle banche o nei conti online. Il problema è che a differenza delle password, i dati biometrici rubati non si possono modificare e quindi, praticamente, sono persi per sempre.

Parallelamente, aumenta l'uso delle cosiddette identità sintetiche, cioè profili personali creati artificialmente e utilizzati per compiere truffe.

Gli attacchi informatici diventano più sofisticati – non più evidenti

Se c'è una cosa che le ultime tendenze insegnano, è che la prudenza nel mondo digitale deve diventare un'abitudine. Informatevi sempre e sensibilizzate anche familiari e amici, perché gli attacchi informatici moderni non colpiscono più solo i sistemi, ma soprattutto le persone.

Consigli pratici per proteggersi:

- Verificate sempre attraverso i canali ufficiali i messaggi o le chiamate provenienti da numeri sconosciuti
- Non aprite link, file allegati o codici QR da messaggi che non aspettavate
- Comunicate i vostri dati personali con grande cautela
- Procedete con i piedi di piombo se qualcuno vi trasmette un senso di urgenza o sfrutta le vostre emozioni
- Utilizzate sistematicamente le funzioni di sicurezza come l'autenticazione a 2 fattori o le passkey