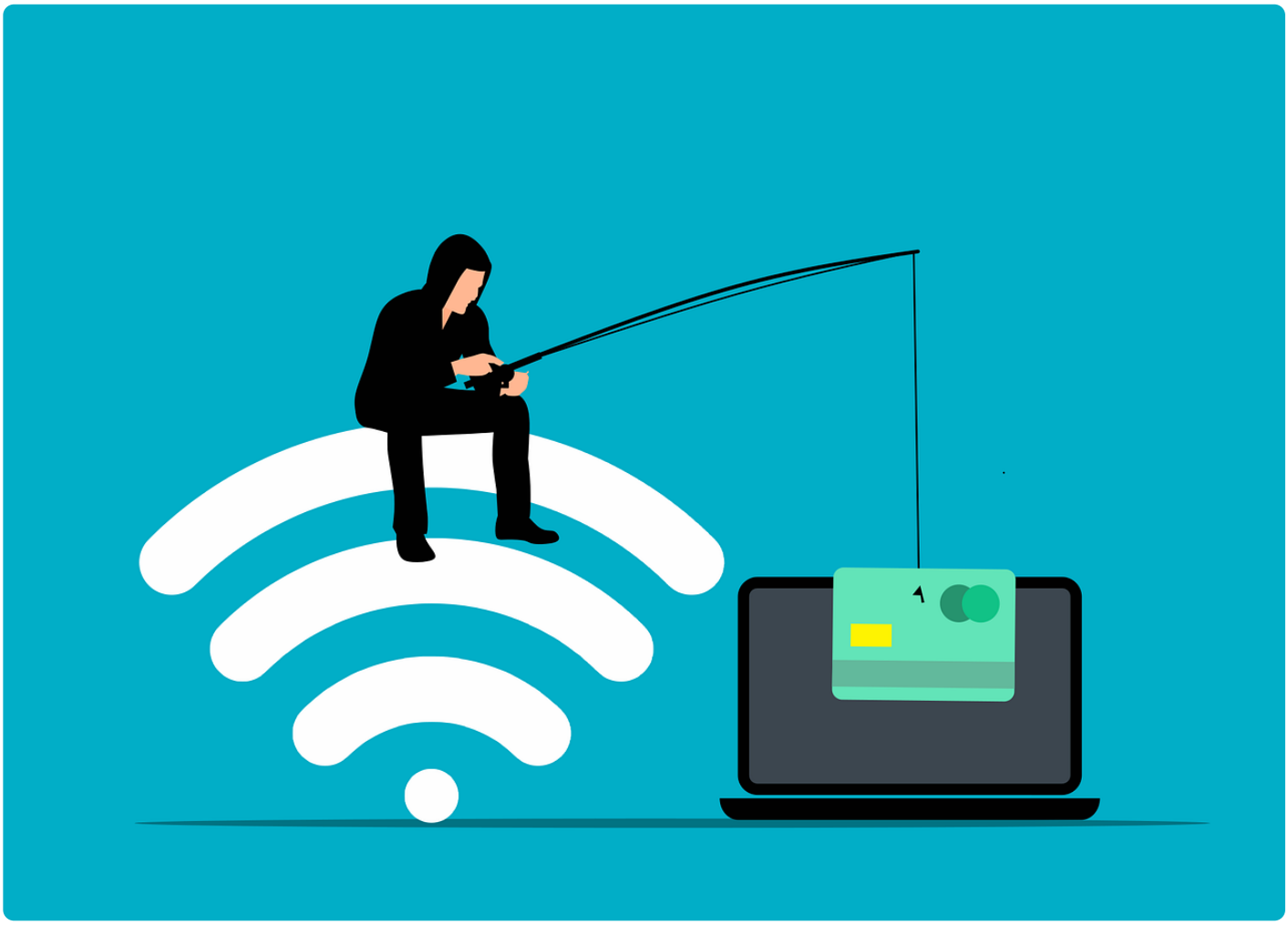

Il phishing continua a essere una delle minacce piÃ¹ serie anche per il pubblico italiano. Secondo questi dati, 3 italiani su 4 avrebbero subito almeno un attacco di phishing.

Con la travolgente ascesa dell'intelligenza artificiale (IA), queste truffe sono diventate ancora piÃ¹ difficili da rilevare. In questo articolo vedremo come sono cambiate le e-mail di phishing grazie all'IA, come riconoscerle e quali misure adottare per proteggersi.

L'evoluzione delle e-mail di phishing

Tradizionalmente, le e-mail di phishing erano facili da riconoscere grazie alla presenza di errori grammaticali e ortografici, nonchÃ© a contenuti generici e poco credibili. Tuttavia, l'introduzione di strumenti basati sullâ??IA come ChatGPT ha cambiato radicalmente lo scenario.

Ora, gli scammer possono scrivere e-mail personalizzate e molto convincenti, complicando la vita agli utenti che cercano di distinguere le comunicazioni affidabili da quelle a rischio.

Lâ??IA al â??servizioâ?• dei truffatori

L'IA consente ai truffatori di analizzare grandi quantitÃ di dati sui potenziali obiettivi, creando e-

Massimo De Vellis
2024/06/28

mail che sembrano autentiche, grazie allâ??attenzione al dettaglio. Questo livello di personalizzazione aumenta notevolmente le probabilitÃ che le vittime cadano nella trappola. Ad esempio, l'IA puÃ² analizzare i profili sui social media, il comportamento online e altre informazioni pubbliche per creare messaggi su misura che attirino l'attenzione del destinatarioâ??â??.

Inoltre, l'IA automatizza la procedura di creazione e invio di queste e-mail, permettendo ai truffatori di raggiungere un pubblico molto piÃ¹ ampio a fronte di uno sforzo minimo. Strumenti come Worm GPT e Fraud GPT, disponibili nella dark web, facilitano la creazione di e-mail di phishing convincenti e possono generare codici per clonare siti web, aumentando ulteriormente il tasso di efficacia dei tentativi di truffaâ??.

Come riconoscere le e-mail di phishing generate dall'IA

Per individuare le e-mail di phishing create dall'IA bisogna osservare bene i dettagli. Ecco alcuni segnali a cui prestare attenzione:

- Richieste insolite: le organizzazioni serie raramente chiedono informazioni sensibili tramite e-mail. Diffidate delle e-mail che richiedono dati personali, credenziali di accesso o informazioni finanziarie.
- Urgenza e tattiche per generare paura: le e-mail di phishing spesso creano un senso di urgenza o paura per indurre una reazione rapida e irrazionale da parte dellâ??utente. Verificate sempre la serietÃ di queste richieste attraverso canali ufficiali prima di rispondere.
- Incongruenze negli indirizzi e-mail e nei link: controllate l'indirizzo e-mail del mittente e passate il mouse sui link per vedere la destinazione effettiva. Qualsiasi discrepanza fra questi due elementi va vista come un segnale di allarme.
- Allegati inaspettati: massima cautela con gli allegati inaspettati, soprattutto se richiedono di abilitare macro o altre funzionalitÃ potenzialmente pericoloseâ??â??.

Prevenire il phishing

Per proteggersi dalle truffe come il phishing, specialmente nei casi in cui ci sia lo zampino dell'IA, Ã¨ fondamentale adottare misure di sicurezza avanzate:

- Soluzioni di sicurezza basate sull'IA: le stesse tecnologie utilizzate dai truffatori possono essere impiegate in fase difensiva. Questi strumenti possono analizzare il contenuto delle e-mail, rilevare pattern sospetti e segnalare le comunicazioni che potrebbero essere anche solo potenzialmente phishing.
- Formazione del personale: programmi di formazione regolare e simulazioni possono aiutare i dipendenti a riconoscere i tentativi di phishing e combattere la tentazione di cliccare su link o aprire allegati sospetti.
- Autenticazione a due fattori (2FA): implementare la 2FA se possibile. Anche nel caso in cui un'e-mail di phishing riesca a ottenere le credenziali di accesso, la 2FA puÃ² impedire accessi non autorizzati richiedendo un ulteriore passaggioâ??.
- Aggiornamenti regolari del software: assicurarsi che tutti gli elementi software, compresi i programmi antivirus e i client di posta elettronica, siano aggiornati per proteggersi dalle minacce piÃ¹ recentiâ??â??.
- Rete privata virtuale: una VPN (Virtual Private Network) nasconde il traffico Internet e lo

instrada attraverso server sicuri, cosÃ¬ per i truffatori diventa molto complicato intercettare dati sensibili. In particolare, le VPN per Mac possono anche nascondere l’indirizzo IP dell’utente, aumentando ulteriormente il livello di sicurezza.