

La sicurezza informatica è sempre più importante

Ivan Campari

Mentre gli attacchi informatici aumentano e le truffe diventano sempre più efficaci e sofisticate grazie all'intelligenza artificiale, è fondamentale non sottovalutare la cybersicurezza. Come consumatrici e consumatori che utilizziamo numerosi dispositivi connessi ad internet, dobbiamo usare la tecnologia in modo corretto e consapevole. **Alessandro Trivilini**, esperto di tecnologie digitali, ci aiuta con qualche suggerimento.

“L’intelligenza artificiale non ha inventato le truffe informatiche, ma sta rendendo più facile, veloce ed efficace il lavoro dei criminali informatici” ci ha spiegato **Alessandro Trivilini**.

“Pensiamo al phishing, una delle tecniche più diffuse per ingannare le persone e sottrarre informazioni personali, password o denaro. Fino a qualche anno fa, molti messaggi fraudolenti erano riconoscibili per gli errori grammaticali, le traduzioni approssimative o le richieste poco credibili. Oggi, grazie all’intelligenza artificiale, è possibile creare in pochi secondi messaggi perfettamente scritti, personalizzati e apparentemente provenienti da banche, aziende o persone conosciute. Con i cosiddetti deepfake è inoltre possibile imitare voci e volti, rendendo ancora più difficile distinguere una comunicazione autentica da una fraudolenta. Ma c’è un aspetto ancora più importante: la capacità manipolatoria dell’intelligenza artificiale. Gli algoritmi di IA possono essere utilizzati non soltanto per creare contenuti convincenti, ma anche per adattare i messaggi alle risposte, alle emozioni e alle convinzioni delle persone, cercando di orientarne le decisioni.”

E come consumatrici e consumatori, cosa cambia? “Soprattutto una cosa: non possiamo più considerare una voce familiare, un’immagine convincente o un messaggio scritto correttamente come garanzie di autenticità. Il consiglio è semplice: quando riceviamo una richiesta inattesa di denaro, informazioni personali o credenziali, soprattutto se accompagnata da urgenza, **dobbiamo fermarci e verificarne l’autenticità attraverso un canale indipendente**”.

Aumentano i dispositivi connessi

La sicurezza informatica non riguarda più soltanto i computer e gli smartphone. Oggi siamo circondati da dispositivi connessi a Internet che utilizziamo quotidianamente, spesso senza renderci conto della quantità di informazioni personali che possono raccogliere e condividere.

Pensiamo agli smartwatch, che possono monitorare la nostra salute, i movimenti e le abitudini quotidiane, oppure agli occhiali smart di Meta, dotati di fotocamere, microfoni e funzionalità di intelligenza artificiale, capaci di osservare e interpretare ciò che ci circonda.

Ma i rischi possono nascondersi anche dietro strumenti apparentemente innocui, come i codici QR, molto diffusi anche per effettuare pagamenti. I criminali informatici possono sostituire un codice QR legittimo con uno fraudolento, indirizzandoci verso siti falsi per sottrarre informazioni personali, credenziali bancarie o indurci a effettuare pagamenti non autorizzati.

Per difendersi non serve essere degli esperti

Proponiamo di seguito dieci suggerimenti tratti dalla guida pratica di Alessandro Trivilini **Cosa devi sapere prima di**.

“La sicurezza informatica non dipende soltanto dalla tecnologia, ma anche dalle nostre decisioni quotidiane”, sottolinea Trivilini.

Ed effettivamente, leggendo i dieci consigli, ci rendiamo conto che sono cose che ognuno è in grado di fare.

Dieci consigli di cybersicurezza

1. **Attivare l’autenticazione a due fattori.** Una password potrebbe non bastare. Un secondo sistema di verifica rende più difficile l’accesso ai nostri account da parte di persone non autorizzate.
2. **Utilizzare password diverse e facili da ricordare.** Un metodo utile è creare una frase lunga, legata a un ricordo personale importante, ma difficile da indovinare per gli altri. Ogni servizio deve avere una password diversa.
3. **Aggiornare dispositivi e applicazioni.** Gli aggiornamenti correggono anche problemi di sicurezza. Quando possibile, attivare quelli automatici per non dimenticarsi di effettuali.
4. **Diffidare dei messaggi urgenti.** SMS, email e messaggi WhatsApp che chiedono di agire immediatamente possono nascondere tentativi di truffa. Verificare sempre attraverso i canali ufficiali, ad esempio telefonando ai numeri ufficiali conosciuti.
5. **Controllare i codici QR prima di pagare.** Un codice QR può indirizzarci verso un sito fraudolento. Prima di inserire dati o confermare un pagamento, verificare il sito e il destinatario.
6. **Non fidarsi soltanto di una voce o di un’immagine.** L’intelligenza artificiale può imitare persone conosciute. Prima di inviare denaro o informazioni riservate, verificare la richiesta attraverso un altro canale ufficiale conosciuto.
7. **Eliminare le applicazioni che non utilizziamo più.** Spesso dimentichiamo di avere installato applicazioni alle quali abbiamo autorizzato l’accesso alla fotocamera, al microfono, alla posizione o ai contatti.
8. **Effettuare regolarmente copie di sicurezza.** Fotografie, documenti e dati importanti devono poter essere recuperati anche in caso di furto, guasto o attacco informatico. Verificare periodicamente che le copie funzionino.
9. **Proteggere le informazioni condivise con l’IA, come ad esempio chatGPT.** Evitare di inserire password, dati bancari, documenti riservati o informazioni personali senza sapere come verranno utilizzati e conservati.
10. **Fermarsi prima di agire.** La fretta, la paura e la curiosità sono spesso sfruttate dai criminali informatici. Quando qualcosa non convince o mette fretta, paura o eccessivo entusiasmo, meglio fermarsi e verificare prima di fare click.