

LegnanoNews

Le news di Legnano e dell'Alto Milanese

Truffe online sempre più sofisticate con l'intelligenza artificiale: attenzione ai siti clone e alle false comunicazioni

Gea Somazzi · Thursday, October 22nd, 2026

Voci di familiari riprodotte artificialmente, video falsi con volti di personaggi famosi e siti internet praticamente identici a quelli ufficiali. L'intelligenza artificiale viene utilizzata sempre più spesso anche per realizzare truffe online, rendendo più difficile per gli utenti riconoscere i tentativi di frode. A segnalarlo è la Polizia Postale che in questi giorni ha diffuso alcuni consigli. Tra le tecniche utilizzate ci sono gli audio che imitano la voce di persone conosciute, i video deepfake e i messaggi di phishing sempre più credibili, scritti senza errori grammaticali e talvolta personalizzati in base al profilo della vittima. Strumenti che possono indurre gli utenti a fidarsi di comunicazioni apparentemente autentiche e a fornire informazioni riservate.

Attenzione ai siti clone

Uno dei rischi riguarda la diffusione dei cosiddetti siti clone, pagine web false che riproducono fedelmente l'aspetto di quelle originali. Grazie all'intelligenza artificiale è possibile realizzare siti che utilizzano loghi, immagini e testi di aziende, istituti bancari, enti pubblici e servizi online, rendendo difficile distinguere una pagina autentica da una contraffatta. L'obiettivo dei truffatori è convincere le vittime a inserire credenziali di accesso, dati personali, informazioni bancarie o altri dati sensibili, che possono poi essere utilizzati per ulteriori attività fraudolente. Questi siti possono essere raggiunti attraverso link inviati tramite e-mail, SMS, social network o applicazioni di messaggistica. In alcuni casi possono comparire anche tra i risultati dei motori di ricerca, aumentando il rischio di essere scambiati per pagine ufficiali.

Come difendersi dalle truffe online

La prima precauzione è controllare sempre con attenzione l'indirizzo internet (URL) prima di inserire qualsiasi dato personale. Anche una piccola modifica nel nome del sito, una lettera diversa o un carattere aggiunto possono essere segnali di una pagina contraffatta. È importante inoltre non fidarsi soltanto dell'aspetto grafico: un logo conosciuto, immagini curate e contenuti apparentemente autentici non garantiscono che il sito sia sicuro. In caso di dubbio, il consiglio è di non cliccare sui link ricevuti e non inserire informazioni personali, ma raggiungere il servizio desiderato digitando direttamente l'indirizzo ufficiale nel browser oppure utilizzando l'applicazione ufficiale. Una verifica in più può evitare di consegnare inconsapevolmente password, credenziali bancarie e altri dati sensibili ai truffatori. In caso di dubbio, il consiglio è di non cliccare sui link ricevuti e non inserire informazioni personali, ma raggiungere il servizio desiderato digitando direttamente l'indirizzo ufficiale nel browser oppure utilizzando

l'applicazione ufficiale. Una verifica in più può evitare di consegnare inconsapevolmente password, credenziali bancarie e altri dati sensibili ai truffatori.

[Clicca qui per tutte le info](#)

This entry was posted on Thursday, October 22nd, 2026 at 1:05 pm and is filed under [Altre news](#). You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can skip to the end and leave a response. Pinging is currently not allowed.