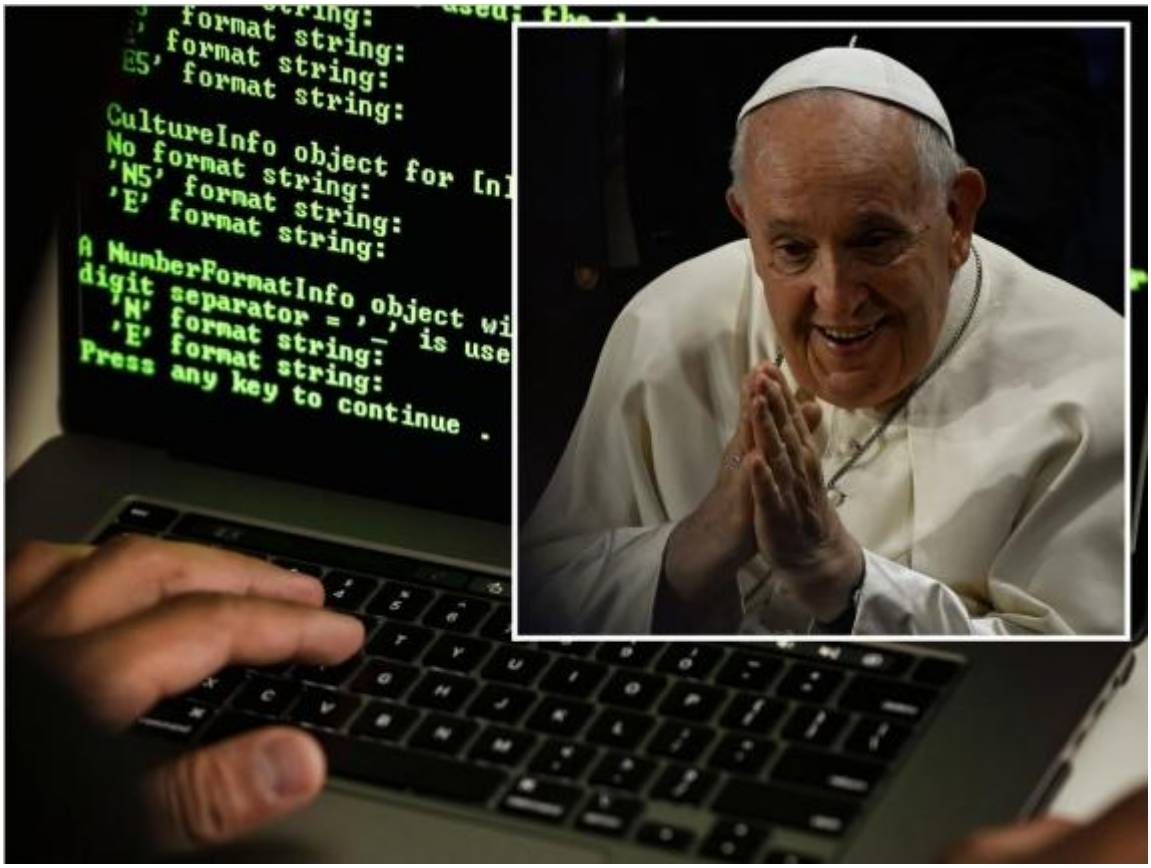
Truffe online, ora si moltiplicano quelle legate alla morte di Papa Francesco: come riconoscerle e come difendersi

Allarme degli esperti di Check Point Software, due le principali tipologie di minacce da cui tenersi alla larga. Tutti i consigli per non finire in trappola

(Fonte: https://www.corriere.it/tecnologia/ 25 aprile 2025)

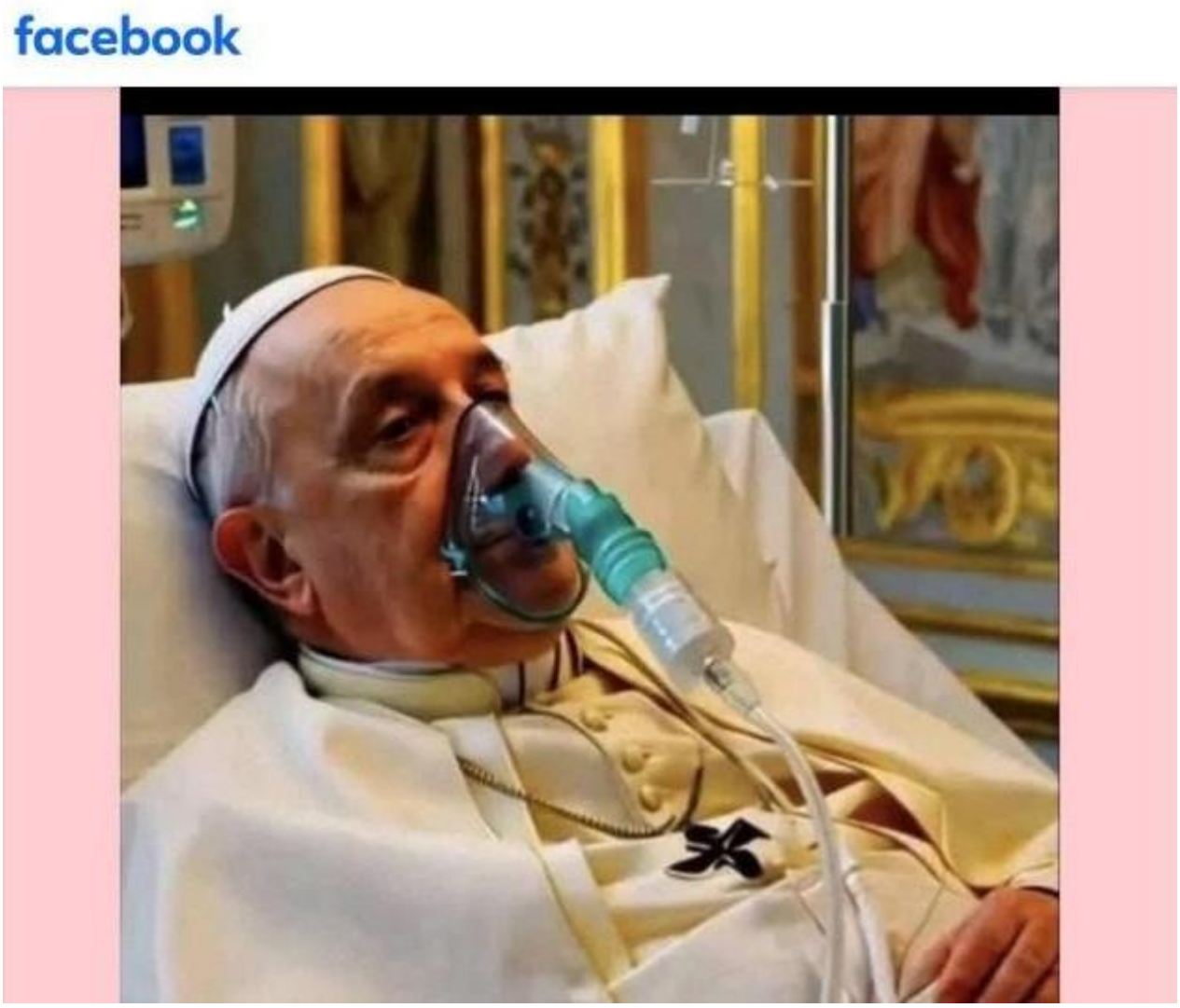


Tecnicamente sono **criminali informatici**, ma non sarebbe comunque scorretto definirli sciacalli o avvoltoi. Non si fanno infatti scrupoli a trarre cinico beneficio da situazioni di lutto o di crisi. Accade puntualmente quando si verificano disastri naturali – si pensi alle finte raccolte fondi –, è successo anche durante l'emergenza Covid e ora il copione si ripete a seguito della **morte di Papa Francesco**. Il motivo è presto detto: «La curiosità del pubblico e le reazioni emotive rendono per gli aggressori questi momenti **occasioni privilegiate per colpire**». Lo affermano in una nota trasmessa alla stampa gli esperti di Check Point Software Technologies, fornitore internazionale di piattaforme di cybersecurity basate sull'intelligenza artificiale per aziende e governi.

La disinformazione sui social

Più nel dettaglio, le principali tipologie di minacce rilevate in questi giorni dagli specialisti sono due: la prima fa leva su **campagne di disinformazione lanciate sui social tramite la condivisione di immagini false** generate proprio con l'AI. «Queste campagne – si legge – sono progettate per catturare l'attenzione degli utenti, spingendoli a cercare ulteriori informazioni tramite i motori di ricerca o a cliccare sui link incorporati nelle immagini o nei post. Una volta cliccati, gli utenti possono essere **reindirizzati a siti web fraudolenti che hanno diversi scopi malevoli, dal furto di**

dati alle truffe finanziarie». A rendere questi portali particolarmente insidiosi il fatto che, come spesso capita, vengano progettati per somigliare il più possibile ad ambienti digitali viceversa tanto conosciuti quanto affidabili (in linea con il tipico meccanismo del phishing). In uno dei casi osservati, per esempio, i malcapitati venivano spinti ad accedere a una **finta pagina di Google che promuoveva una truffa con carte regalo**, «tattica comunemente usata per ingannare le persone e indurle a consegnare informazioni sensibili o a effettuare pagamenti».



Un'immagine fasulla realizzata con l'Intelligenza Artificiale e postata sui social network (fonte: Check Point Software Technologies Ltd.)

L'avvelenamento Seo

L'altro schema fraudolento più utilizzato consiste invece nel cosiddetto **avvelenamento Seo** (dall'inglese *Search Engine Optimization poisoning*). «In questo caso – illustrano gli esperti –, i criminali informatici **pagano per posizionare i propri siti dannosi tra i risultati di ricerca legittimi**, ingannando gli utenti e facendo credere loro di accedere a informazioni affidabili. Questo metodo consente di distribuire malware, rubare credenziali o dirottare i cookie di sessione, finendo per monetizzare il traffico generato da questi siti». Nel concreto, quindi, chiunque in queste ore dovesse cercare notizie o aggiornamenti su Papa Francesco potrebbe finire per **cliccare inconsapevolmente su un link dannoso posizionato in alto nei risultati** di Google o di altri motori

di ricerca online. Un problema – viene specificato – «aggravato dal fatto che molti di questi domini non compaiono negli strumenti di intelligence sulla reputazione. I domini potrebbero essere stati registrati di recente o essere rimasti inattivi per mesi senza mostrare alcun comportamento dannoso, consentendo loro di **eludere il rilevamento da parte della maggior parte dei sistemi di sicurezza informatica**».

Sei consigli pronti all'uso

«**I criminali informatici prosperano grazie al caos e alla curiosità** – afferma Rafa Lopez, Security Engineer, Email Security di Check Point Software Technologies –. Ogni volta che si verifica un evento di cronaca importante, assistiamo a un **forte aumento delle truffe progettate per sfruttare l'interesse del pubblico**. La migliore difesa è una combinazione di consapevolezza dell'utente e di protezione stratificata della sicurezza». Sei, sotto questo profilo, **i consigli** forniti dall'azienda per «ridurre significativamente il rischio di cadere vittime di campagne di disinformazione o di attacchi informatici che sfruttano eventi globali». Eccoli in chiusura.

1. **Mantenere il browser e il sistema operativo aggiornati** alle ultime versioni. Le patch di sicurezza spesso risolvono le vulnerabilità sfruttate dagli aggressori.

2. **Utilizzare strumenti di protezione della navigazione** che verificano i siti web in tempo reale, bloccando i link dannosi prima che vengano caricati.

3. **Essere cauti con i titoli sensazionali o i contenuti virali**, soprattutto sui social media. Se la notizia sembra scioccante, è meglio fare un controllo incrociato con i media affidabili.

4. **Non cliccare su link provenienti da fonti sconosciute**, soprattutto nelle email o nei post sui social relativi a notizie dell'ultima ora. Digitare invece gli URL dei siti ufficiali di notizie direttamente nel browser.

5. **Utilizzare i servizi di intelligence sulle minacce** per verificare i domini o i file sospetti prima di accedere ad essi.

6. **Considerare di adottare un software di sicurezza avanzato** che includa la protezione dal phishing, il rilevamento delle minacce informatiche e gli aggiornamenti delle informazioni sulle minacce per mantenere sicuri i propri dispositivi.

Truffe online, notizie e approfondimenti

[Ecommerce, nel 2024 truffati 2,8 milioni di italiani: casi in aumento (ma metà delle vittime non denuncia)]

«Abbiamo ricevuto il tuo curriculum»: come funziona la nuova (e diffusissima) truffa telefonica in Italia

In Svizzera allarme quishing, la «truffa del postino» tramite Qr Code (segnalata anche in Italia): cos'è e come difendersi

Truffe online, in Italia dilaga il phishing: tripla allerta della polizia, i consigli per difendersi

«È stata avviata un'azione legale contro di te», nuovo allarme della Polizia contro le false convocazioni giudiziarie