AVVISO CONTRO LE FRODI INFORMATICHE

Le frodi informatiche ai danni degli operatori finanziari e/o della loro clientela rappresentano una minaccia in costante crescita nell'era digitale. Gli attacchi, sempre più sofisticati, mirano a sottrarre dati sensibili, denaro, identità.

I principali schemi adottati, come identificati dal Gruppo di Azione Finanziaria Internazionale – GAFI (si veda: https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html) sono qui di seguito riassunti:

- **frode BEC (Business E-mail Compromise):** è una forma di frode informatica nella quale i criminali utilizzano le e-mail per indurre le vittime ad inviare denaro o a divulgare informazioni riservate. Questo tipo di attacco è particolarmente efficace perché spesso coinvolge la falsificazione dell'identità di un dirigente o di un fornitore affidabile, creando un senso di urgenza e fiducia nelle vittime.
  Esempio: una mail apparentemente proveniente da un dirigente aziendale sottolinea all'addetto ai pagamenti che non ha ancora saldato un fornitore e gli dispone quindi di provvedervi immediatamente fornendogli fattura, importo e coordinate bancarie. In realtà, il mittente non è il dirigente aziendale al quale i criminali si sono sostituiti nell'identità, ma i truffatori stessi.
  Come funziona:
  - falsificazione dell'identità: di prassi i truffatori si fingono un dirigente aziendale, un fornitore fidato o un soggetto di rilievo ben conosciuto in azienda per guadagnare la fiducia della vittima. A tal fine, scansionano le e-mail aziendali ed il relativo archivio per poter acquisire il linguaggio e lo stile di comunicazione del soggetto a cui si sostituiscono nell'identità;
  - manipolazione psicologica: i criminali, utilizzando tecniche di manipolazione psicologica, creando un senso di urgenza e di pressione per indurre la vittima a non chiedere ulteriori informazioni o a non effettuare una verifica;
  - richiesta di pagamento o di informazioni: le e-mail BEC richiedono alle vittime di inviare denaro ad un conto fraudolento, di modificare le coordinate bancarie di un fornitore, di condividere documenti sensibili o di rivelare informazioni riservate;
  - effetti negativi: l'attacco BEC può causare perdite finanziarie significative, compromissione di dati sensibili e danni alla reputazione aziendale.

  Come difendersi:
  - formazione e consapevolezza: i dipendenti devono essere formati sulla sicurezza delle e-mail e sulle tecniche di phishing per riconoscere i segni di un attacco BEC;
  - controllo delle e-mail: verificare sempre l'identità dell'emittente, utilizzare strumenti di verifica delle e-mail e richiedere sempre ulteriori informazioni per qualsiasi richiesta di pagamento o di informazioni sensibili;
  - separazione dei compiti: implementare procedure aziendali che richiedano la verifica di richieste di pagamento o di informazioni da parte di più persone;
  - protezione anti-phishing: utilizzare soluzioni anti-phishing per bloccare le e-mail sospette e proteggere i sistemi informatici;
  - sicurezza delle password: utilizzare password complesse e aggiornare regolarmente le credenziali di accesso;
  - etichettatura delle e-mail esterne: etichettare le e-mail esterne per distinguerle dalle e-mail interne ed avvisare i dipendenti.
- **frode di phishing**: è una truffa online che sfrutta la manipolazione psicologica per indurre gli utenti a rivelare informazioni sensibili, come password o dati bancari. Solitamente si usano e-mail, SMS o messaggi falsi, che si spacciano per comunicazioni ufficiali di banche, siti web o altre istituzioni.

Esempio: una comunicazione che sembra provenire dalla propria banca, richiede di cliccare su un link per aggiornare i propri dati di accesso. Procedendo, si viene reindirizzati ad un sito web falso, che sembra identico a quello della banca, ma che in realtà è progettato per rubare i dati.

Come funziona:

- manipolazione psicologica: gli attacchi di phishing utilizzano tecniche di manipolazione per convincere gli utenti a cliccare su link o allegati dannosi, a compilare moduli falsi o a rivelare informazioni in modo ingannevole;
- e-mail, SMS e messaggi falsi: le e-mail, gli SMS ed i messaggi di phishing possono sembrare legittimi, ma spesso presentano errori di ortografia, grammaticali, saluti generici, richieste di informazioni che le istituzioni non chiederebbero, link sospetti o indirizzi e-mail del mittente non corrispondenti;
- link ed allegati dannosi: i link in queste e-mail, SMS e messaggi spesso rimandano a siti web falsi che imitano il sito legittimo, o gli allegati contengono malware che possono infettare i dispositivi;
- scopi: l'obiettivo principale è ottenere i dati di accesso a conti online, informazioni personali, dati di pagamento o l'accesso a sistemi informatici.

Come difendersi:

- non cliccare su link sospetti: non cliccare su link o allegati in e-mail, SMS o messaggi che non sembrano legittimi o che richiedono informazioni sensibili;
- non fornire informazioni online: non fornire informazioni personali, come password, numeri di carte di credito o codici di sicurezza, in siti web che non sembrano affidabili;
- verificare l'indirizzo e-mail del mittente: controllare che l'indirizzo e-mail del mittente corrisponda all'organizzazione che dichiara di rappresentare;
- riconoscere i segni di phishing: essere consapevoli dei segni di phishing, come errori di ortografia, saluti generici, richieste di informazioni insolite o toni urgenti e minacciosi;
- installare software antivirus e antispyware: utilizzare un software aggiornato per proteggere il proprio dispositivo dai malware;
- segnalare gli attacchi: segnalare eventuali e-mail, SMS o messaggi di phishing alle Autorità Competenti, per contribuire a diffonder la notizia ed a prevenire attacchi simili.

- **frode di impersonificazione sui social media e nelle telecomunicazioni**: nota come "spoofing", è una tecnica fraudolenta nella quale i truffatori fingono di essere qualcuno di cui le vittime dovrebbero fidarsi, per ottenere informazioni o manipolarli. Questo avviene attraverso varie forme, inclusi messaggi di testo, chiamate telefoniche, e-mail o messaggi sui social media che sembrano provenire da fonti legittime.

  Esempio: un messaggio ricevuto apparentemente da un amico che chiede dati personali, ma che in realtà proviene dai truffatori. O una telefonata della propria banca che richiede di fornire le proprie credenziali perché le stesse sono state violate, o la carta di credito clonata. In tal modo si consegna il controllo del proprio conto corrente bancario ai criminali, che lo possono svuotare oppure, se poco capiente, possono utilizzarlo temporaneamente per farvi affluire proventi da crimini, da bonificare poi a terzi conti, spesso esteri.

  Come funziona:

  - spoofing via social media: i truffatori creano profili falsi che imitando quelli di aziende o persone di fiducia. Questo può includere la creazione di account che utilizzano le foto e i dati personali di altri, o la creazione di account che imitano in modo preciso i profili ufficiali di aziende;
  - spoofing nelle telecomunicazioni (vishing): i truffatori utilizzano chiamate telefoniche per ingannare le vittime ed ottenere informazioni personali, spesso facendo credere di essere rappresentanti di banche o altre istituzioni;
  - smishing: un'altra forma di phishing, detta smishing, sfrutta i messaggi di testo (SMS) per ingannare le vittime ed indurle a fornire informazioni personali o a cliccare su link malevoli;

- pretexting: questa tecnica prevede l'uso di scenari falsi e ingannevoli per manipolare la vittima a rivelare informazioni sensibili od a compiere azioni specifiche.

Come proteggersi:

- verificare le richieste: prima di fornire qualsiasi informazione personale, controllare se la richiesta proviene effettivamente da una fonte affidabile e non da un account falso o da una chiamata fraudolenta.;
- porre attenzione con i link: prima di cliccare su link ricevuti tramite messaggi di testo o e-mail, verificare la loro legittimità. Se si ha il minimo sospetto che possano esser fraudolenti, non cliccare;
- seguire le linee guida di sicurezza: seguire le linee guida di sicurezza dei social media e delle telecomunicazioni per proteggere i propri account e dati personali;
- non condividere informazioni personali online: evitare di condividere informazioni personali come indirizzi, numeri di telefono o dettagli bancari sui social media;
- denunciare le truffe: se si riceve un messaggio o una chiamata fraudolenta, denunciare la situazione alle autorità competenti ed al provider di servizi.

- **frode del trading online/piattaforma di trading**: anche definita "fake trading", è un raggiro consistente nella sottrazione di denaro ad investitori a cui è stato fatto creder di poter ottenere guadagni facili, rapidi e consistenti. I truffatori creano piattaforme di trading online fittizie, spesso tentando le vittime con promesse allettanti e spingendole ad investire somme sempre maggiori.

  Esempio: navigando in rete appaiono pubblicità di piattaforme che consentono di negoziare titoli esteri o titoli otc o certificati o asset virtuali, tipologie di investimento spesso alternative rispetto a quelle proposte dalle banche tradizionali, e spesso superficialmente conosciute dal pubblico per elevati guadagni (ad esempio bitcoin). Cliccando su tali pubblicità si viene rimandati ad una piattaforma di trading online, apparentemente semplice ed intuitiva da utilizzare. Dopo essersi iscritti, viene richiesto di bonificare una piccola somma di denaro (spesso su conti esteri) che, apparentemente, poi sembrerà fruttare bene. Nei giorni successivi, vengono richiesti versamenti di importi sempre più ingenti, con la prospettiva di un guadagno facile assicurato. Una volta investiti i soldi, però, cessano le comunicazioni dal falso operatore, e ci si rende conto che non c'è alcun modo per poter accedere a quanto (apparentemente) investito ed ai relativi (falsi) guadagni.

  Come funziona:

  - contatto e proposta: i truffatori contattano le potenziali vittime, spesso tramite telefonate, e-mail o con pubblicità su Internet, proponendo investimenti con prospettive di grandi guadagni facili;
  - iscrizione alla piattaforma: le vittime vengono convinte a iscriversi ad una piattaforma di trading online apparentemente affidabile, spesso gestita da broker fittizi;
  - investimento iniziale: viene chiesto un investimento iniziale, spesso di importo contenuto, che sembra produrre rapidi risultati positivi;
  - somme crescenti e promesse inesistenti: nel tempo, i truffatori sollecitano alle vittime ulteriori versamenti, sempre maggiori, sull'onda di apparenti lauti guadagni;
  - disattivazione e perdita: quando le vittime decidono di prelevare i loro guadagni, la piattaforma si blocca o si chiude, ed i soldi versati si volatizzano, senza possibilità di recupero.

  Come difendersi:

  - diffidare da promesse di rendimenti eccessivi: se i guadagni fossero certi, sicuri, ingenti, non ci sarebbe bisogno di proporre tali investimenti a terzi;
  - verificare l'affidabilità: prima di investire, controllare se la piattaforma di trading è autorizzata dall'Autorità di Vigilanza nazionale ed è offerta da operatori finanziari vigilati. Ricercare online più informazioni e recensioni possibili. Visitare il sito ufficiale dell'operatore

finanziario, accedendovi non tramite i link forniti ma da un motore di ricerca, e chieder informazioni direttamente a tale operatore, contattando la relativa assistenza.
  - non cedere a pressioni ed all'ingordigia: diffidare da richieste di investimenti urgenti e non temere di perder l'occasione per realizzare rendimenti assurdi;
  - non trasferire denaro a conti stranieri: evitare di trasferire denaro verso IBAN stranieri, a meno che non si abbia la certezza che il beneficiario sia un operatore autorizzato;
  - segnalare alle Autorità competenti: in caso di sospetto di truffa, rivolgersi alle Autorità competenti.

L'Intelligenza Artificiale a supporto delle frodi informatiche

L'Intelligenza Artificiale (IA) sta rapidamente trasformando il panorama delle truffe online, offrendo ai criminali strumenti sofisticati per ingannare le vittime potenziali. L'IA può essere utilizzata per raccogliere e analizzare grandi quantità di dati personali, rendendo più facile per i truffatori rubare l'identità delle vittime, estorcere denaro, sottrare dati sensibili, manipolare e disinformare, inducendo a credere a false informazioni. L'IA può creare e-mail e messaggi di testo di phishing altamente personalizzati e convincenti: analizzando i dati delle potenziali vittime, crea messaggi che sembrano provenire da aziende o organizzazioni legittime, inducendo i truffati a cliccare su link dannosi o a condividere informazioni sensibili.

L'uso fraudolente dell'Intelligenza Artificiale è favorito dai chatbot malevoli. I chatbot (da chatterbot, in italiano "robot di conversazione") sono software progettati per interagire con un essere umano, utilizzando sistemi di elaborazione del linguaggio naturale per fornire risposte automatiche. Il chatbot più famoso è probabilmente ChapGPT (Chat Generative Pre-trained Transformer), basato sull'Intelligenza Artificiale e sull'apprendimento automatico, sviluppato da OpenAI. Ma ne esistono altri, anche più semplici, utilizzati per una larga varietà di scopi, come per esempio assistenza clienti, guida in linea, risposte alle FAQ. A fianco dei chatbot benevoli, per facilitare il lavoro dei cybercriminali, sono stati creati i chatbot malevoli (ad esempio WormGPT e FraudGPT, "gemelli malvagi" di ChatGPT) che sfruttano l'Intelligenza Artificiale generativa per aumentare l'efficacia di attacchi informatici su larga scala, mettendo a rischio numerosi utenti e organizzazioni. I chatbot malevoli sono già in grado di scrivere e-mail di phishing più convincenti rispetto agli umani.

Ecco alcune delle principali truffe elaborate con l'IA:

- **deepfake e manipolazione multimediale:**
  - i deepfake sono video falsi incredibilmente realistici che possono mostrare persone che dicono o fanno cose che non hanno mai detto o fatto. I truffatori possono utilizzare i deepfake per impersonare celebrità, politici o persino familiari ed amici, inducendo le vittime a fidarsi di loro ed a condividere informazioni personali o denaro;
  - la manipolazione audio basata sull'IA può clonare la voce di una persona, rendendo possibile creare messaggi vocali falsi, che tuttavia sembrano provenire da fonti attendibili.
- **sorveglianza e raccolta illecita di dati:** la sorveglianza, la raccolta e l'utilizzo di dati senza il consenso dell'interessato sono azioni che violano la privacy e possono essere perseguite penalmente. La sorveglianza, in questo contesto, si riferisce all'osservazione, attraverso strumenti tecnologici, di una persona senza il suo consenso. La raccolta illecita, invece, è la raccolta di dati personali senza il rispetto delle regole stabilite dalla legge sulla privacy. L'utilizzo dell'Intelligenza Artificiale permette di raccogliere ed analizzare informazioni sensibili e di sorvegliare in modo estremamente efficace ed efficiente;
- **automazione di attacchi informatici:** grazie all'uso dell'IA, attacchi informatici quali brute force, scansione vulnerabilità, exploit di software incrementano la loro potenzialità offensiva, in termini sia di quantità che di qualità, raggiungendo un grado di efficienza superiore a quelli prodotti esclusivamente dall'azione umana;
- **disinformazione:** l'utilizzo dell'Intelligenza Artificiale generativa consente l'efficace diffusione di false informazioni, in particolare tramite i social media, nei quali l'IA può creare profili falsi, che sembrano appartenere a persone reali;

- **frodi:**
  - truffe finanziarie: sistemi IA che apprendono come ingannare piattaforme finanziarie, simulare comportamenti umani ed aggirare controlli. Possono creare documenti falsi e facilitare l'acquisizione fraudolenta delle credenziali per l'accesso a conti online;
  - frodi sui social media: come già detto sopra, l'IA può creare profili falsi, che sembrano appartenere a persone reali. I truffatori possono utilizzare questi profili per entrare in contatto con le vittime e costruire relazioni, per poi manipolarle ed indurle ad inviare denaro o a condividere informazioni personali;
  - manipolazione dei prezzi e delle recensioni: l'IA può essere utilizzata per manipolare i prezzi dei prodotti o dei servizi online, creando l'illusione di un affare. I truffatori possono anche utilizzare l'IA per generare recensioni false, influenzando le decisioni di acquisto dei consumatori;
  - truffe romantiche: grazie all'Intelligenza Artificiale, è possibile creare falsi profili su siti o su app di incontri, profili che sembrano appartenere a persone interessate ad una relazione. I truffatori possono utilizzare l'IA per analizzare i dati delle vittime e creare profili che corrispondano ai loro interessi e desideri, per poi manipolarle, sottrargli dati sensibili ed indurle ad inviare denaro.

Come mitigare i rischi

L'IA è uno strumento potente che può essere utilizzato sia per scopi benefici che dannosi. È importante essere consapevoli dei rischi e adottare misure preventive per proteggersi dalle truffe.
La costruzione di un modello generativo pre-addestrato richiede poche centinaia di righe di codice. Quindi, la minaccia derivante dall'uso di chatbot malevoli rappresenta un serio motivo di preoccupazione. E' urgente e necessario che tutti assumano la consapevolezza dei rischi dell'ingegneria sociale e del phishing, tenendo sempre presente che gli attaccanti stanno sfruttando nuove tecnologie per intensificare le loro attività criminali online.
Deve esser adottato e diffuso un modello mentale orientato allo scetticismo:

- mai fornire i propri dati personali e/o finanziari;
- verificare sempre l'identità, anche nel caso di telefonate, e-mail, messaggi apparentemente provenienti da soggetti conosciuti. Come detto, l'IA può generare video, audio, testi falsi, seppur assolutamente realistici e verosimiglianti;
- non cliccare su link in e-mail o messaggi, se non c'è l'assoluta certezza che si sta agendo in sicurezza;
- utilizzare password sicure, aggiornate frequentemente, diversificate per ogni account online;
- mantenere aggiornato il software delle device utilizzate, in particolare l'antivirus e l'antispyware;
- prevedere un sistema di blocco anche per l'accesso fisico alle proprie device, evitando così che terzi soggetti possano entrare se le device fossero lasciate incustodite anche per breve tempo.