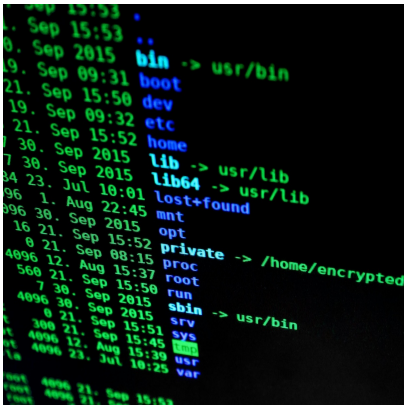

S.O.S. truffe informatiche

Descrizione

Ottobre Ã¨ il mese dedicato alla **sicurezza informatica europea** e, in occasione di ciÃ², il Museo del Risparmio di Torino, da sempre attento alle problematiche attuali connesse allâ€™educazione finanziaria, ha organizzato un incontro sul tema. Con il termine anglosassone di *cyber security* comunemente si intende lâ€™insieme di tecniche e processi di protezione informatica per prevenirne gli attacchi, mentre per **minaccia cibernetica** si intendono tutte le condotte controindicative che possono essere realizzate per il tramite del *cyber space*, in danno a questâ€™ultimo.

CiÃ² premesso, un dato di fatto Ã¨ che in Italia sono aumentati i *cyber crimes* â€“ del 9% nellâ€™ultimo semestre rispetto il semestre dello scorso anno -, complici anche le tecniche sempre piÃ¹ evolute, compreso lâ€™uso malevole dellâ€™intelligenza artificiale. Prezioso lâ€™intervento di **Alessandra Belardini**, dirigente della polizia postale del Lazio, centro operativo di sicurezza cibernetica, che ha permesso di puntualizzare alcuni aspetti problematici. Primo aspetto, la peculiaritÃ dei reati informatici rispetto a quelli ordinari, laddove i truffatori in rete sono molto facilitati dalla probabilitÃ che, attraverso i grandi numeri, qualche â€œpesce che abboccaâ€• o che cade nella rete della â€œpesca a strascicoâ€• vi Ã¨ quasi sempre.

Infatti, in questa tipologia di reati il fattore umano, forse di piÃ¹ di quello tecnologico, incide molto, in quanto la vittima spesso â€œcollaboraâ€• con il truffatore. Rilevante diventa il profilo psicologico della vittima, la cui vita viene osservata e studiata (il c.d. social engineering) a fini malevoli. Il **trading on line** , i video, le foto e simili vengono mistificati e si gioca per lo piÃ¹ sul fattore emozionale, dai problemi di utenza di urgente soluzione agli affetti familiari (il figlio/a che ha smarrito il telefono e chiama la mamma per un aiuto da un nuovo numero di cellulare, alle chiamate dalla quale compare un numero che effettivamente corrisponde ad un ufficio/persona, per carpire le nostre informazioni piÃ¹ riservate).

Quali sono i consigli degli esperti della **polizia postale**? Abbastanza intuitivi: monitorare sempre i propri conti (spesso le truffe iniziano con piccole somme non controllate), mai dare informazioni riservate personali, tutelare la nostra privacy evitando il piÃ¹ possibile di mettere in rete la propria immagine (e la propria voce), preferire i pagamenti contrassegno e gli acquisti in Italia, verificare ogni fonte e, infine, sempre informarsi (vi Ã¨ un apposito sito del commissariato di P.S), segnalare e denunciare i fatti alle autoritÃ competenti, anche ai fini della prevenzione. In sintesi, acquisire una

sempre maggiore **consapevolezza informatica** e, soprattutto, trasmetterla alle nuove generazioni di nativi informatici.

Anche i consigli nati dallâ€™esperienza dei preposti alla sicurezza cibernetica delle banche sono importanti e preziosi, in quanto la cultura della consapevolezza digitale (in stretta connessione con lâ€™educazione finanziaria) Ã¨ sempre piÃ¹ necessaria per la **sicurezza informatica**: si ritiene che lâ€™82% degli incidenti informatici, sia riconducibile alla non corretta applicazione delle procedure o alle scorrette informazioni.

Come premessa Ã¨ necessario distinguere tra **frode** e **truffa informatica**, essendo la prima posta in essere attraverso una identitÃ digitale fasulla (il cosiddetto *spoofing)* mentre la seconda presuppone che la vittima abbia lâ€™intestazione dellâ€™utenza. Fatta questa precisazione, non si puÃ² non osservare che, anche se le tecniche truffaldine usate si sono raffinate negli anni, Ã¨ sopravvissuta nel tempo la cosiddetta â€œtruffa sentimentaleâ€•, caratterizzata dal rapporto sentimentale che si viene a creare on line tra la vittima e il truffatore.

La tecnica Ã¨ il classico â€œinnamoramentoâ€• delle parti (veritiero da parte della vittima nei cui confronti sono stati spiati i lati particolarmente deboli e quindi piÃ¹ facilmente aggredibili della sua personalitÃ) che sfocia, dopo un certo lasso di tempo, con la richiesta di un incontro di persona, preceduto per lo piÃ¹ da una cauta richiesta di denaro, per svariati motivi, da parte del **truffatore**.

Ottenuto il denaro, lâ€™incontro fisico viene rimandato nel tempo con varie scuse, sino alla scomparsa totale di ogni contatto del truffatore sentimentale. Simile a questa tipologia, la richiesta di aiuto che perviene da un finto amico o da un finto familiare, generalmente figlio/a, che con svariati motivi (perdita del telefono, incidente stradale o simili) chiede un aiuto immediato di denaro o comunque lâ€™instaurazione di un contatto. Elemento costante e comune di quasi tutte le frodi e truffe informatiche e lâ€™urgenza, in quanto si gioca sul fattore psicologico della paura di un imminente evento negativo e si abbassano pertanto le reazioni di difesa.

Attenzione anche ai **falsi investimenti**, proposti attraverso i social. Il guadagno facile attrae da sempre (soprattutto i giovani) e talvolta i truffatori permettono anche un guadagno iniziale di modiche somme (quale impiego di precedenti illeciti profitti) per invogliare la vittima ad investire somme sempre piÃ¹ significative. A quel punto, dopo la breve fase iniziale positiva, iniziano le perdite, ovvero la piattaforma sparisce del tutto dalla rete! Ora, con **lâ€™intelligenza artificiale**, i truffatori informatici hanno unâ€™arma ancora piÃ¹ efficace (*deep fake)*, potendo mistificare, anche lâ€™immagine e la voce di una persona a loro piacimento (si pensi alle truffe perpetrate attraverso le false emergenze familiari, alle quali si puÃ² anche aggiungere lâ€™audio).

Lâ€™intelligenza artificiale generativa, attraverso le piÃ¹ recenti applicazioni ormai quasi di comune utilizzo (come la **chatGTP**), se utilizzata per fini malevoli, costituisce un ulteriore notevole pericolo informatico. Molte pericolose le richieste di aggiornamento delle applicazioni, cliccando su links sconosciuti: in questo caso si installa unâ€™applicazione malevole che dÃ al truffatore il controllo totale su tutte le applicazioni della vittima! Pertanto, mai scaricare applicazioni se non dai siti ufficiali e, possibilmente, non installare troppe applicazioni non necessarie (piÃ¹ si aumenta il numero di applicazioni piÃ¹ si aumenta il rischio di frodi) e per quanto possibile, non accettare troppi cookies, i quali da esigenze di marketing potrebbero diventare informazioni utili a fini malevoli.

Molta attenzione anche alla provenienza delle emails, soprattutto se si chiede di cliccare su links dalle

stesse indicate per attivitÃ necessarie ed urgenti (ad esempio per lâ€™ultima conferma della prenotazione di un hotel o di un bed and breakfast, nellâ€™imminenza del viaggio). Eâ€™ sempre necessario verificare la legittima provenienza della richiesta.

In sintesi quale Ã¨ il messaggio che si puÃ² trarre da tutto ciÃ²? La parola chiave del messaggio consiste – ovviamente insieme allâ€™informazione e allâ€™attenzione per la tutela della propria privacy – nel verbo dubitare, sempre, di tutto Ã¨ di tutti. Non sarÃ molto simpatico ricordarlo, ma in punto **frodi e truffe informatiche**, nessuno Ã¨ innocente sino a prova contraria. Purtroppo.

Liliana Perrone

CATEGORY

1. AttualitÃ

Categoria

1. AttualitÃ

Data di creazione
04/11/2024
Autore
perrone