



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€cesce che abboccaâ€ o che cade nella rete della â€pesca 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€collaboraâ€ 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 dall'esperienza dei preposti alla sicurezza cibernetica delle banche sono importanti e preziosi, in quanto la cultura della consapevolezza digitale (in stretta connessione con l'educazione finanziaria) è sempre più necessaria per la **sicurezza informatica**: si ritiene che l'82% degli incidenti informatici, sia riconducibile alla non corretta applicazione delle procedure o alle scorrette informazioni.

Come premessa è necessario distinguere tra **frode** e **truffa informatica**, essendo la prima posta in essere attraverso una identità digitale fasulla (il cosiddetto *spoofing*) mentre la seconda presuppone che la vittima abbia l'instaurazione dell'utenza. Fatta questa precisazione, non si può non osservare che, anche se le tecniche truffaldine usate si sono raffinate negli anni, è sopravvissuta nel tempo la cosiddetta "truffa sentimentale", caratterizzata dal rapporto sentimentale che si viene a creare on line tra la vittima e il truffatore.

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

Ottenuto il denaro, l'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 l'instaurazione di un contatto. Elemento costante e comune di quasi tutte le frodi e truffe informatiche è l'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 più significative. A quel punto, dopo la breve fase iniziale positiva, iniziano le perdite, ovvero la piattaforma sparisce del tutto dalla rete! Ora, con **l'intelligenza artificiale**, i truffatori informatici hanno un'arma ancora più efficace (*deep fake*), potendo mistificare, anche l'immagine e la voce di una persona a loro piacimento (si pensi alle truffe perpetrate attraverso le false emergenze familiari, alle quali si può anche aggiungere l'audio).

L'intelligenza artificiale generativa, attraverso le più 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 un'applicazione malevola che dà 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 (più si aumenta il numero di applicazioni più 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 attività necessarie ed urgenti (ad esempio per l'ultima conferma della prenotazione di un hotel o di un bed and breakfast, nell'imminenza del viaggio). È sempre necessario verificare la legittima provenienza della richiesta.

In sintesi quale il messaggio che si può trarre da tutto ciò? La parola chiave del messaggio consiste – ovviamente insieme all'informazione e all'attenzione per la tutela della propria privacy – nel verbo dubitare, sempre, di tutto di tutti. Non sarà molto simpatico ricordarlo, ma in punto **frodi e truffe informatiche**, nessuno è innocente sino a prova contraria. Purtroppo.

In occasione dello *European Cybersecurity Month*

SOS TRUFFE ONLINE

EVENTO IN PRESENZA E ONLINE
23 ottobre 2024 ore 18:00
Museo del Risparmio – Via San Francesco D'Assisi, 8/a Torino

Truffe online, attacchi informatici, frodi sui pagamenti: negli ultimi anni le minacce informatiche sono aumentate, grazie alle tecniche più evolute e all'utilizzo dell'intelligenza artificiale. Tuttavia, imparare a proteggere la propria identità digitale e i propri dati è possibile. In occasione del European Cybersecurity Month, il Museo del Risparmio presenta, grazie agli esperti della Divisione Cybersecurity di Intesa Sanpaolo, trucchi e segreti per scovare le trappole del web e far fronte alle minacce Cyber.

- Ore 18.00** **SALUTI DI BENVENUTO**
Giovanna Paladino | *Direttore e Curatore Museo del Risparmio*
- Ore 18.10** **CYBERCRIME IN ITALIA: A CHE PUNTO SIAMO**
Alessandra Belardini | *Dirigente del Centro Operativo per la Sicurezza Cibernetica del Lazio*
- Ore 18.30** **NUOVE TRUFFE E INTELLIGENZA ARTIFICIALE: COME PROTEGGERSI**
Mauro Marigliano | *Divisione Cybersecurity Intesa Sanpaolo*
- Ore 18.50** **Q&A**
- Ore 19.00** **CHIUSURA LAVORI E SALUTI**

MODALITÀ DI PARTECIPAZIONE
Evento gratuito con prenotazione obbligatoria compilando il form:
https://bit.ly/EventoSoStruffeonline_23ott

 **MdR**
MUSEO DEL RISPARMIO

Liliana Perrone

CATEGORY

1. Attualità

Categoria

1. AttualitÃ

Data di creazione

04/11/2024

Autore

perrone

default watermark