SERATA INFORMATIVA ORGANIZZATA DALL'ASSOCIAZIONE ARTIGIANI E COMMERCIANTI VALPOSCHIAVO

La truffa online è quotidianamente dietro a un click: a cosa bisogna prestare attenzione

di GIOVANNI RUATTI

Alessandro Zala ha reso attento il pubblico sulle truffe online

Venerdì 13 marzo la sala dell'Hotel La Romantica si è potuto assistere alla conferenza, organizzata dall'Associazione Artigiani e Commercianti Valposchiavo, sulle truffe online. Dal numeroso pubblico presente si comprende che il tema desti un certo interesse, anche perché chi naviga in Internet (ormai la grande maggioranza della popolazione) e ha una casella di posta elettronica, si ritrova costantemente con messaggi pubblicitari o avvisi, alcuni dei quali capaci di innescare delle truffe inaspettate e dannose.

Alla serata è stato invitato a parlare di truffe e di come ci si può proteggere, l'ingegnere informatico Alessandro Zala, originario di Brusio e collaboratore della società Compass Security, occupandosi di test di penetrazione, verifiche di sicurezza, attività di attacchi simulati (red team) e formazione in ambito della sicurezza informatica.

Dopo la presentazione della coordinatrice dell'Associazione Artigiani e Commercianti Valposchiavo, Manuela Kalt-Demonti, si è data la parola all'esperto Zala che esordisce con una frase: «Ci vuole un ladro per catturare un ladro», e poi chiarisce il concetto. Si definisce infatti simpaticamente un hacker buono che conosce i trucchi degli hacker cattivi e aiuta i clienti a chiudere le falle dei loro sistemi.

Truffe online fatte da gruppi ben organizzati

Al giorno d'oggi i cyber-attacchi si verificano quotidianamente bloccando aziende fino al momento del riscatto, oppure inducono le vittime a pagare dei soldi, se non a essere proprio derubate. A capo di queste iniziative criminali ci sono gruppi ben organizzati (poche volte lupi solitari come si vedono nei film); Zala fa l'esempio di un luogo in Myanmar denominato *Scam City*, ovvero città della truffa, dove i suoi lavoratori/gruppi si impegnano giorno e notte a creare iniziative truffaldine nella rete di tutto il mondo.

Per gli hacker cattivi è il loro lavoro: s'impegnano a "scannerizzare" Internet per trovare delle falle e poi ad attaccare i sistemi.

Phishing e Deepfake

Ci sono diversi modi per imbrogliare e attaccare. Molto comune è il "phishing", truffa online su larga scala che utilizza e-mail, SMS o messaggi falsi per ingannare le vittime fingendosi una persona o un ente affidabile. Lo scopo è quello di far rivelare informazioni sensibili, dare dati d'accesso come password, PIN o dati bancari, o far eseguire un programma. Si possono riconoscere questi messaggi fraudolenti, perché fanno leva su alcune emozioni o stati esistenziali come l'avidità, l'urgenza, la curiosità, la paura e la compassione. Questi messaggi si possono individuare per il tono, la firma e il saluto, il mittente sconosciuto, e le imperfezioni nell'ortografia e nella grammatica.

SERATA INFORMATIVA ORGANIZZATA
DALL'ASSOCIAZIONE ARTIGIANI E COMMERCIANTI VALPOSCHIAVO

La truffa online è quotidianamente dietro a un click: a cosa bisogna prestare attenzione

Continua dalla 1ª pagina

Grazie all'Intelligenza Artificiale i cybercriminali riescono a generare video clonando l'aspetto di personalità famose o camuffando l'aspetto della persona parlante. Oppure clonando la voce della persona famosa. Quest'inganno si chiama Deepfake.

Si stima che in Svizzera sono 200 milioni di franchi che vengono rubati o estorti da queste frodi.

Clickfix e Ransomware

Esiste poi un'altra frode chiamata Clickfix, ossia con un pretesto gli utenti vengono indotti a inserire un codice dannoso nella riga di comando del computer e questo permette ai malintenzionati di accedere nel sistema o nel computer attraverso lo stesso aiuto dell'utente che non è consapevole di ciò che sta accadendo. In questa maniera i cybercriminali possono rubare dati sensibili.

Si è parlato anche di Ransomware, che è un programma dannoso che infetta il dispositivo digitale bloccando l'accesso al sistema o ad alcuni dei suoi contenuti al fine di richiedere un riscatto.

Come ci si può proteggere

Raccomandazioni per i singoli:
- Utilizzare password univoca (e complessa) per ogni servizio online.
- Utilizzare un gestore di password.
- Proteggere i servizi online importanti con un secondo fattore di autentificazione.
- Aggiornare regolarmente i sistemi operativi e i programmi.
- Utilizzare un programma antivirus e mantenerlo aggiornato.
- Prestare attenzione ai campanelli d'allarme nelle e-mail, SMS, chiamate, ecc.

Misure di sicurezza per le aziende:
- Sensibilizzare i dipendenti sui pericoli e sulla sicurezza.
- Definire processi chiari e sicuri per pagamenti o accessi ai sistemi.
- Monitorare e verificare regolarmente la sicurezza della propria infrastruttura.
- Creare e applicare linee guida chiare per i social media e piattaforme con IA.
- Cifrare i dati sensibili.
- Aggiornare regolarmente tutti i sistemi (in particolare quelli di sicurezza)
- Obbligare l'uso di password complicate.
- Eseguire il backup (offline) di tutti i dati.

Anche in Valposchiavo succede

Numerosi sono i metodi per ingannare gli utenti del web e oggigiorno le truffe progrediscono. Molte sono le domande che sono seguite su diversi aspetti di truffa. Si è confermato che le carte di credito e quelle prepagate sono le più sicure e che è importante avere un secondo fattore di sicurezza per l'autentificazione.

Anche il direttore della Banca Cantonale Grigione, Fabio Pola, è intervenuto con alcune raccomandazioni. Prima di tutto, le truffe online si verificano anche in Valposchiavo e occorre continuare a sensibilizzare e informare la popolazione. Per quanto riguarda i dubbi su azioni bancarie online che sembrano poco chiare, è fortemente raccomandato di passare fisicamente in banca e rivolgersi al personale per gli accertamenti.