SUPLANTACIÓ DE TÈCNICS DE MICROSOFT: COM PROTEGIR-TE DE LES ESTAFES

Les ciberestafes es poden produir de diverses formes: **des de correu electrònic, SMS, WhatsApp o, inclòs, trucades telefòniques**.

Ës aquest precisament el mètode que estan utilitzant especialment els ciberdelinqüents per fer-se passar per l'empresa tecnològica **MICROSOFT** i robar informació als usuaris.

Recentment la mateixa companyia Microsoft ha alertat sobre un augment del nombre important de casos detectats.

Els delinqüents insten a les persones a les que truquen a instal·lar programes amb els quals aconsegueixen el control dels seus equips i poder accedir a la seva informació personal i financera.

Les ciberestafes en les quals els delinqüents fan servir la trucada telefònica com a mitjà a través del qual roben dades és conegut com a **<<vishing>>**. Es tracta d'una realitat que els cibercriminals coneixen a la perfecció. I per això, fan molt bé els seus deures, mitjançant una tècnica anomenada enginyeria social.

Amb aquesta metodologia de hacking aconsegueixen saber-ho tot sobre les seves víctimes abans de fer la trucada.

És a dir, els hackers cerquen tota la informació que hi ha sobre una persona a internet i les xarxes socials, per saber on treballen les seves víctimes, on viuen o al col·legi al que porten als seus fills. Un cop assolida tota aquesta informació, la utilitzen per generar confiança en les persones a les quals estan estafant. Aquesta afirmació és feta pel prestigiós Hervé Lambert, responsable d'operacions de Panda Scurity (un dels més potents antivirus del mercat).

En allò que es refereix als casos en els quals se suplanta a Microsoft, la companyia fa èmfasi que "**mai envia proactivament missatges de correu, ni fa trucades per tal d'oferir suport tècnic o demanar informació personal o financera de cap usuari**". Al seu torn, destaca que "el suport tècnic de Microsoft només es posa en contacte amb aquells usuaris que ho hagin sol·licitat prèviament, mitjançant els canals establerts per la companyia".

Cas que hagis estat víctima d'una estafa d'aquest tipus, des de la companyia Microsoft es destaca que, **si s'ha lliurat informació bancària, s'ha d'avisar l'entitat, revisar els comptes i canviar les claus**. Si han accedit al vostre ordinador o dispositiu, ha de contactar amb el servei tècnic del fabricant. A la vegada, ha de denunciar l'intent d'estafa a la policia. Per reportar aquest tipus d'incidències, Microsoft també ha habilitat una plana web (localitzable a www.microsoft.com).

CARDING

Darrerament associat a la suplantació de tècnics de Microsoft, s'ha detectat que els ciberdelinqüents utilitzen el mètode conegut com **<<carding>>**.

Què és el carding?

Es tracta de l'ús (o generació) de targetes de crèdit (o els seus números), pertanyents a altres persones amb la finalitat d'obtenir béns realitzant frau amb elles. Se relaciona molt amb les males pràctiques del hacking i el cracking, mitjançant els quals s'aconsegueixen els números de les targetes.

El seu objectiu és fer-se amb les dades numèriques de la targeta, inclòs el codi de verificació.

Pot realitzar-se a través de telèfon, això és, un operador et convenç per tal que li facilitis el teu número de targeta de crèdit, o a través d'internet rebent un correu electrònic fraudulent, en el qual ens demanen aquestes dades.

Els imports de les compren sempre seran petits i seqüencials, per tal d'evitar sospites i que sigui difícil donar-se compte que l'estafa està succeint.

Com evitar-ho ?

 S'ha d'evitar obrir correus en els quals ens demanen les nostres dades personals o financeres.

 En cap cas, donar o facilitar les nostres dades bancàries per telèfon.

 Per això, les empreses i entitats emissores de targetes de crèdit, fan molt èmfasi que mai ens enviaran un correu electrònic o missatges al telèfon mòbil demanant el número de targeta del client, la data de caducitat, etc.

IMPORTANT: Si sou víctima d'una estafa cal denunciar-ho a les Forces i Cossos de Seguretat (Policia Local i Policia de la Generalitat – Mossos d'Esquadra), essent important aportar la major informació possible: pàgina web, report de la transacció, nom de la persona de contacte (encara que sigui fictici), tarja de crèdit utilitzada pel pagament i entitat expenedora de la mateixa, eventual gravació de la trucada, missatges rebuts, etc. Si no heu estat víctima de l'estafa però en teniu coneixement, us recomanem posar-ho d'igual forma en coneixement de les forces policials, per tal de poder investigar l'origen de l'estafa i si s'escau detenció dels ciberdelinqüents.