PHISHING A WHATSAPP: L' APP PREFERIDA PER ESTAFAR-TE.

Cada cop els cibercriminals intenten estafar als usuaris de WhatsApp mitjançant el mètode conegut com a phishing.

S'estima que el phishing representa el 90 % de tots els intents de ciberatacs. Aquest terme fa referència a la pràctica mitjançant la qual un ciberdelinqüent intenta fer-se passar per una entitat o marca coneguda utilitzant un email o un lloc web fals per tal de robar als usuaris les seves contrasenyes, informació personal, dades bancaries, etc.

WhatsApp és l' app preferida dels hackers per tractar de que caiguem en aquest tipus d'estafa.

La majoria dels atacs de phishig a telèfons del país són perpetrats a través d'aplicacions populars com WhatsApp, Facebook o PayPal.

Els atacs a telèfons mòbils representen un 15 % del total. Si ens referim a phishing a través de planes web (61 % del total), Google i Amazon són les marques més imitades.

Per sectors, la tecnologia, la banca i les xarxes socials són els principals objectius dels cibercriminals. Es comença a detectar un augment dels atacs phishing per correu electrònic, que ja representa un 24 % del total.

Per evitar caure a la trampa, es recomana desconfiar de les ofertes especials que podem rebre a través de correu electrònic. És important revisar de forma detallada dominis similars, els errors d'ortografia als mails o llocs web i el remitents de correus electrònics desconeguts.

Principals riscos de seguretat i recomanacions per evitar-los

Riscos de seguretat més comuns associats a l'ús de les aplicacions de missatgeria instantània:

- **Infecció del dispositiu:** quan un ciberdelinqüent accedeix remotament al vostre dispositiu i aconsegueix monitoritzar les vostres accions. Això pot perjudicar el funcionament de l'aparell o robar-ne informació.
- **Fuita o robatori d'informació:** perdreu la confidencialitat de la vostra informació, la qual anirà a parar a mans alienes.
- **Suplantació d'identitat:** amb les dades personals que obtinguin els delinqüents es faran passar per vosaltres per cometre algun tipus de delicte.
- **Sessions sense tancar:** si no tanqueu la vostra sessió algú altre pot accedir a les vostres dades.
- **Infecció del dispositiu amb codi maliciós:** es tracta d'un programari o arxiu que s'instal·la sense coneixement de l'usuari i intenta accedir a les vostres dades personals, com ara les credencials d'accés als serveis bancaris en línia.
- **Ubicació dels dispositius:** si teniu les opcions activades, altres persones podran saber on sou i us podran localitzar encara que vosaltres no ho vulgueu.

Recomanacions per evitar els riscos:

Informeu-vos sobre tots els riscos de seguretat i les principals amenaces més comuns en les aplicacions de missatgeria instantània.

Conegueu les característiques i les funcionalitats de seguretat dels vostres dispositius.

Configureu els programes de forma adequada:

Activeu les opcions de privacitat,

No emmagatzemeu contrasenyes,

Activeu la protecció antivirus per a missatgeria.

Mantingueu els programes i els antivirus actualitzats amb la finalitat de tancar possibles forats de seguretat.

Desconfieu de fitxers i enllaços, especialment d'aquells que no heu sol·licitat o dels que heu rebut de desconeguts.

Tanqueu les sessions obertes a webs, aplicacions i serveis web.

El segrest de WhatsApp

En els darrers mesos s'ha detectat un increment dels intents de robatori de comptes de WhatsApp per part de ciberdelinqüents mitjançant un atac de suplantació d'identitat.

Hi ha diversos sistemes, com les aplicacions que usen l'IDCAT SMS, la banca electrònica o les aplicacions de xarxes socials, que utilitzen com a mesura de seguretat avançada l'enviament per missatges de text de codis de seguretat al mòbil.

Els codis de seguretat rebuts per missatges de text no s'han de compartir amb ningú, com les contrasenyes, podríeu estar donant, de forma involuntària, el control total del programa a terceres persones.

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.