Societat | NacióDigital | Actualitzat el 11/03/2021 a les 11:56

Creus que has caigut en l'estafa de l'SMS? Així ho pots detectar i solucionar

Aquesta pràctica és coneguda com a "SMSing"

L'estafa arriba a les víctimes via SMS | Europa Press

Una estafa massiva a través de missatges SMS ha estat el malson de les autoritats policials durant les últimes setmanes. La policia espanyola ja va advertir d'aquesta pràctica fraudulenta fa uns dies, coneguda com a *SMSing*. Els estafadors envien missatges on es fan passar per diferents empreses d'enviament de paqueteria com FedEx, Correus o DHL i, amb l'excusa d'un paquet pendent de ser entregat, suplanten la identitat de la companyia i pretenen dirigir a les víctimes a webs o aplicacions malicioses.

La intenció dels estafadors és que la víctima faci clic a l'enllaç que adjuntem en el fals SMS. Al fer-ho, i de forma automàtica, una aplicació mòbil prèviament registrada pels delinqüents es descarregarà al terminal mòbil facilitant així l'accés a les dades d'usuari.

L'aplicació maliciosa pot instal·lar un troià bancari que permetrà que els delinqüents accedeixin a les dades dels comptes més sensibles, ha informat la policia espanyola en un comunicat. A més, els estafadors donen instruccions per trencar els elements de seguretat instal·lats en els mòbils i que eviten que es descarreguin aplicacions perjudicials.

Com pots detectar si has caigut en l'estafa o has rebut l'SMS fraudulent? El virus utilitza les

agendes dels mòbils per reenviar l'enllaç que farà clicar els usuaris i caure de quatre grapes en l'estafa. Per detectar un enllaç fraudulent cal veure amb quin nom s'ha enviat aquell SMS, si ho fa amb el nom de pila, el nom complet o una referència poc comuna. Des del portal especialitzat Xataka (https://www.xatakandroid.com/tutoriales/mi-android-tiene-virus-consejos-para-evitar-apps-maliciosas-y-como-eliminarlas) expliquen que hi ha diversos elements fàcils de detectar gràcies a l'SMS per no clicar-hi. Cal, però, parar atenció:

1) **El nom de qui t'envia l'SMS.** El virus utilitza l'agenda de contactes dels mòbils. Per exemple, si es rep un missatge amb "Joan feina" i no en tenim cap així registrat, és fraudulent. És tan fàcil com comprovar la mateixa agenda.

2) **Comprovar l'enllaç.** Aquest virus fraudulent envia un link a una web de missatgeria. Si l'enllaç és de FedEx, cal recordar que no opera a Espanya. El problema arriba si és de Correus o DHL, on cal seguir el tercer pas.

3) **Les empreses d'enviament utilitzen enllaços curts.** L'estafador fa servir un enllaç molt llarg i complicat, que no té res a veure amb els links originals que fan servir aquestes companyies.

[noticiadiari]2/217150[/noticiadiari]
Per assegurar-te que tot està sota control, es comprova a dins de la configuració del mòbil, a l'apartat "Instal·lar aplicacions desconegudes". Dins d'aquest apartat es veu una llista d'aplicacions amb un text a sota que hauria de ser *No permès*. Si en alguna apareix *Permès*, s'ha de prémer sobre ella i canviar la configuració.

Com ho pots solucionar? Si per desgràcia hem arribat a descarregar l'aplicació i hem instal·lat el virus, desfer-se'n d'ell no és impossible però tampoc fàcil.

1) La més radical és **formatar completament el telèfon mòbil.** Fent això s'esborrarà tot el que hi hagi al dispositiu, així que caldria guardar de manera segura imatges o contactes que es puguin perdre.

2) **Descarregar-se una aplicació (ho pots fer aquí) (https://github.com/linuxct/malninstall/releases/tag/202103064) que combat el virus** i s'ha creat específicament per destruir-lo. No es pot descarregar des de la Play Store i s'ha d'instal·lar de manera manual. **Aquí pots seguir les passes per fer-ho. (https://www.xatakandroid.com/analisis/estafa-sms-uno-troyanos-peligrosos-sofisticados-historia-android-como-funciona-como-eliminarlo)**

3) **Iniciar el Mode Segur d'Android.** Cada dispositiu és diferent i cal buscar com fer-ho a internet, però això permetrà tornar a començar al mòbil només amb les aplicacions que venien de fàbrica.

En què consisteix l'*SMSing*? Per evitar aquest tipus d'estafes, la policia recomana prestar atenció quan es rep una comunicació electrònica i no actuar impulsivament fent clic als enllaços. En aquest tipus de missatges sol haver-hi algunes pistes que conviden a sospitar de la veracitat de la mateixa: enllaços poc habituals, que s'han escurçat o que tenen un domini diferent de la companyia.

A més, és fonamental que només s'accedeixi a les webs oficials de les companyies de missatgeria per saber en quina situació es troben els enviaments. Davant la més mínima sospita, s'aconsella denunciar davant les autoritats els SMS potencialment fraudulents rebuts i, sobretot, mai accedir als enllaços que els acompanyen.

Així mateix, mai s'ha d'instal·lar aplicacions de tercers, ja que cap companyia de paqueteria exigirà als usuaris la instal·lació d'aplicacions mòbils per a facilitar els seguiments dels paquets. Tampoc s'han d'obrir enllaços que exigeixin donar dades personals a través d'internet, ni descarregar cap

arxiu de què es tingui el més mínim dubte de la seva procedència.

Altres notícies que et poden interessar
[noticiadiari]2/217065[/noticiadiari]
[noticiadiari]2/217086[/noticiadiari]