ACTUALITAT | Redacció | Actualitzat el 15/03/2021 a les 16:59

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

[inicicentrareport]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.

Com pots detectar si has caigut en l'estafa o has rebut l'SMS fraudulent?
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.

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) 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.**

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.
[ficentrareport]