EL POU de la gallina
Revista manresana d'informació i opinió

Opinió | | Actualitzat el 13/11/2023 a les 11:55

Com evitar estafes en els correus electrònics i codis QR

Les estafes amb els codis QR s'anomenen *QRishing* i es produeixen bàsicament en restaurants, bars i locals nocturns. S'ha d'anar amb compte en els llocs que tenen il·luminació deficient i en establiments molt concorreguts. Abans d'escanejar el codi QR s'ha de vigilar que no es tracti d'un adhesiu enganxat sobre el QR original. Si es tenen dubtes, cal consultar l'amo del bar, restaurant o establiment per si realment correspon amb el seu codi, amb la qual cosa el propietari del local es posarà en alerta en el cas que s'hagi produït aquesta manipulació. A part d'això, si nosaltres escanegem el codi QR i no hem tingut la precaució que hem indicat abans, sabrem que es fals quan els enllaços no ens envien a la pàgina web del restaurant, bar o local de què es tracti o no ens mostren directament la carta dels seus establiments.

Les estafes amb el correu electrònic s'anomenen *phishing*, una tècnica d'enginyeria social que fa servir correus electrònics falsos per suplantar la identitat d'entitats de confiança i obtenir informació confidencial dels seus usuaris. Els ciberdelinqüents usen el phising per robar dades personals, bancàries o d'accés a diferents serveis. Aquests correus solen fer servir un to urgent i sol·licitar una acció immediata, com ara obrir un enllaç, descarregar un arxiu o enviar informació.

Com es poden evitar?

Verificant la font del correu: mireu si el remitent és conegut i si la direcció del correu és legítima. Cal desconfiar si l'encapçalament dels correus és un genèric, com per exemple: "benvolgut amic", "notificació a usuari" o quelcom semblant.
Comprovant la direcció URL. Passeu el ratolí per sobre de qualsevol enllaç o link que tingui el correu. Normalment apareixerà en una petita finestra la direcció URL real a la qual es dirigeix aquest link. Si no coincideix amb el que apareix en el correu electrònic o creieu que no es correspon amb la del lloc que representa, probablement ens trobem amb un cas de phising.
Desconfiant dels missatges sospitosos. Sovint són missatges amenaçadors: bloqueig de comptes, notificació de deutes, etc.
No s'han d'obrir arxius adjunts. Especialment si estan en format Word, Excel, Power Point o PDF.
Cal mantenir el software actualitzat.

Què cal fer si som víctimes de *phising*?

Posar una denúncia virtual o presencial davant els Mossos d'Esquadra.
Trucar al 017 (Institut Nacional de Ciberseguretat).
Presentar una reclamació davant l'Agència Espanyola de Protecció de Dades.
Canviar totes les contrasenyes immediatament i notificar-ho al banc.
Informar de seguida al banc si ens han buidat els comptes.
Accedir al nostre compte de correu electrònic per expulsar el hacker, canviar la contrasenya i comprovar si l'atacant ha canviat qualsevol de les configuracions del nostre compte.