bankinter

Com protegir-se dels ciberdelinqüents?

Conèixer les estafes virtuals més comunes és el primer pas.

Els hi expliquem

Els ciberdelinqüents intentaran contactar amb vostè **mitjançant qualsevol canal** de **comunicació**, normalment suplantant una entitat que li resulti coneguda, com el seu propi banc.

Copiaran els logotips i l'estil de comunicació perquè cregui que és real, i li demanaran realitzar alguna acció en concret, en la majoria dels casos de forma urgent perquè no tingui temps de verificar la informació.

Aquests són alguns dels **canals més freqüents:**

Phishing

Consisteix en l'**enviament d'un correu electrònic a una persona simulant ser una empresa pública o privada** perquè comparteixi la seva informació personal, professional o financera.

Copien els logotips, l'estil dels missatges reals i li demanen que realitzin alguna acció, normalment de forma urgent.

Com actuar?

- **Desconfiï si li demanen** contrasenyes o dades bancàries.
- **Presti atenció al remitent de** l'email, i si veu alguna cosa rara, no l'obri.
- Si nota alguna cosa sospitosa, **no respongui al correu**.
- **No faci clic** en cap enllaç ni descarregui arxius adjunts si li demanen una acció que no ha demanat.

Smishing

És l'intent de **frau a través d'un missatge de text al telèfon mòbil (SMS)**,
per obtenir informació personal, professional o financera. Normalment, **li demanaran fer clic en algun enllaç web o trucar a un telèfon** per "verificar", "actualitzar" o "reactivar" algun servei.

Com actuar?

- No s'afanyi, **no faci clic** en enllaços, arxius adjunts o imatges sense verificar el remitent i l'adreça web.
- **No respongui a un SMS** que sol·liciti el seu PIN, la contrasenya del seu banc o altres credencials de seguretat.
- **Bankinter mai li demanarà** les seves credencials a través d'un SMS.

QRishing

El ciberatac es produeix quan **escaneja un codi QR** des del seu telèfon mòbil **que li dirigeix a un lloc web fals**, allà li demanaran les credencials o informació confidencial.

Com actuar?

- **Desactivi** al seu mòbil l'opció d'obrir automàticament els enllaços en escanejar un codi QR.
- **Utilitzi aplicacions d'escaneig** que permetin veure a quin URL dirigeix aquest codi abans d'obrir-lo.
- **Presti atenció** per si el codi QR hagués estat manipulat.

Vishing

Els atacants **truquen per telèfon** per aconseguir els seus diners o el de la seva empresa, informació sensible o accés al seu ordinador. Per convèncer-lo, **faran servir informació bàsica sobre vostè que hauran trobat a Internet** perquè cregui que és una entitat legítima.

Com actuar?

- **Sospiti** si algú li truca creant una sensació d'urgència o pressió.
- **No faciliti cap mena d'informació** sensible per telèfon.
- Si la persona que truca li demana descarregar un programari, fer clic en algun enllaç o obrir algun arxiu, **no ho faci.**
- Bankinter **mai contactarà amb vostè per sol·licitar-li informació confidencial.**

Baiting

És un ciberatac en què s'utilitza un **dispositiu extraïble, per exemple un USB, per infectar el seu ordinador** amb un programa maliciós que els permeti obtenir la seva informació confidencial.

Com actuar?

- **Desconfiï** dels dispositius extraïbles que no sàpiga d'on provenen.
- **Mantingui sempre actualitzat** l'antivirus del seu ordinador.
- **No connecti** dispositius externs que no li pertanyin.

bankinter

A través de xarxes WiFi públiques

Les xarxes WiFi públiques són **insegures**, ja que són més vulnerables davant d'atacs, tinguin o no contrasenya.

Els ciberdelinqüents solen posar noms a les WiFi públiques semblants a les reals en llocs transitats, com un aeroport.

Com actuar?

- No accedeixi a la seva banca en línia ni a la seva informació confidencial **des de WiFi públiques o sense contrasenya**.
- No entri en xarxes WiFi **obertes sense credencials** d'inici de sessió.
- Mantingui el navegador i el sistema operatiu **actualitzats a l'última versió** disponible. A més de comptar amb un antivirus correctament instal·lat.

En compres online

Les compres a Internet poden ser segures, però de vegades apareixen ofertes que no són reals i pot tractar-se d'un frau.

Com actuar?

- **Vigili que l'URL** comenci per "https".
- **Verifiqui si la botiga** en línia disposa de certificat digital. **Busqui informació i opinions** de l'empresa.
- **Observi que el disseny** de la pàgina no sigui estrany o tingui errors.

bankinter

A través de Bizum

Bizum es fa servir per enviar diners necessitant únicament el número de mòbil del destinatari. És una funció que està inclosa en la mateixa app del banc, però també pot donar lloc a frau.

Alguns ciberdelinqüents envien **sol·licituds de diners a través de Bizum** a clients del servei, i sense adonar-se'n, aquests accepten l'enviament de diners.

Com actuar?

- Recordin **verificar** el perfil de l'usuari amb el qual està interactuant.
- Quan utilitzi Bizum, asseguri's de **llegir** tot correctament abans de realitzar qualsevol gestió.
- Quan rebi un Bizum, l'import apareixerà instantàniament en el seu compte bancari i rebrà una **notificació** de la seva entitat per informar-lo.

Frau del CEO

Consisteix a **suplantar la identitat d'una persona amb autoritat** sobre d'altres que tenen accés a béns econòmics, amb l'objectiu de realitzar moviments de diners als comptes del ciberdelinqüent. Solen fer servir el correu electrònic o trucades.

Com actuar?

- **Sospiti** d'aquest tipus de peticions, sobretot si no són habituals, o involucren comptes a l'estranger.
- **Examini** amb deteniment el remitent del missatge i les errates gramaticals.
- En cas de dubte, comprovi que la persona que contacta amb vostè **és qui diu ser.**

Fake news

Es tracta de **notícies falses que es difonen** per escandalitzar l'opinió pública i poder manipular-la; l'objectiu sol ser polític, econòmic o social.

Com actuar?

- **Analitzi el mitjà** que ha publicat la notícia i contrasti-la.
- **Observi amb atenció** l'URL, per si la troba sospitosa.
- **Comprovi les dades** en què va ser publicada.
- **Verifiqui** que no existeixin errors ortogràfics o gramaticals.
- **Observi** si les imatges han estat manipulades.

A través de targetes

Els fraus amb targeta es produeixen quan algú accedeix a la seva targeta (o a les seves dades) i utilitza aquest servei de pagament per efectuar compres, retirada o extracció de diners en efectiu que no ha autoritzat.

Com actuar?

- **Mai faciliti les dades de la seva targeta**, llevat que estigui comprant en un lloc legítim.
- **Verifiqui** l'import de la compra abans de realitzar qualsevol transacció.
- **Utilitzi sempre el doble factor d'autenticació**, encara que les compres siguin imports menors.

I recordi:

- Bankinter mai li demanarà informació confidencial per correu electrònic.
- No sol·licitarà les seves credencials a través d'un SMS.
- I mai contactarà amb una altra persona per sol·licitar-li en el seu nom aquesta informació.

Si ja ha caigut en un frau, pot trucar al **Servei d'Atenció al Frau (900 81 00 62)**, o acostar-se a l'oficina més propera, per rebre ajuda.

El coneixement és la millor protecció.