Recomanacions

No donis dades confidencials per cap canal desconegut

Cometen errors ortogràfics, molta atenció a l'ortografia!

Limita la informació que comparteixes a xarxes socials

Evita connectar-te a xarxes Wi-Fi públiques

Què fer en cas de sospita per ciberatac?

Revisa si hi ha hagut algun moviment sospitós al compte

Contacta amb l'entitat

Bloqueja la targeta bancària

Canvia la clau de seguretat

Fes la reclamació a l'entitat

L'entitat té 15 dies per donar contestació

Vols saber-ne més?

Apunta't al curs en línia d'ADICAE
El comerç electrònic i les persones consumidores
i compra segur per la web

https://formacion.adicae.net

CONTACTA amb AICEC-ADICAE:

www.adicae.net

/aicecadicae

/AICEC

@AicecAdicae

aicec@adicae.net

Barcelona: 933 425 044
Tarragona: 877 440 370
Girona: 872 591 050
Lleida: 973 940 350

c/Creu dels Molers , 13
Barcelona

Amb la col·laboració de:

Ajuntament de Barcelona

CIBERATACS ALS MITJANS DE PAGAMENT

AICEC-ADICAE
Associació d'Usuaris de Bancs, Caixes i Assegurances de Catalunya

PRINCIPALS TIPUS DE CIBERATACS VINCULATS ALS MITJANS DE PAGAMENT

COMERÇ ONLINE

PHARMING

Manipulen el trànsit d'una web per a redirigir a pàgines web falses o introduint un malware en el dispositiu

FORMAJACKING

Injecten un programari als pagaments d'alguns comerços i còpia les dades personals per a utilitzar-les posteriorment

TRASHING

Agafen informació a través d'un virus a l'ordinador (Trashing)

- **Als arxius eliminats**
- **A l'historial de navegació**
- **Per les cookies (Dades de les cerques que has fet a l'ordinador)**

RECOMANACIONS

-**Verificar l'URL**. Sempre comencen amb 'https', la '**S**' indica que és un lloc segur

-**Revisar les condicions** de postvenda per evitar altres pagaments

-**Destruir** la informació confidencial

-Tenir instal·lat **antivirus**

ATENCIÓ! Activa les notificacions, el banc t'avisarà quan facis compres o transferències

BANCA EN LÍNIA

Estafen l'usuari fent creure que està en un lloc de confiança per robar dades, i realitzar càrrecs econòmics.
Hi ha tres canals per robar dades:

PHISHING

Per correu electrònic

SMISHING

Per missatgeria instantània: SMS o WhatsApp

VISHING

Per trucades telefòniques

OBJECTIUS DEL PHISHER

- **Fer-se amb les contrasenyes**
- **Informació bancaria**
- **Treure diners**
- **Suplantar l'identitat**

RECOMANACIONS

-Verificar les fonts
-Fer servir només la web oficial
-No accedir a través del e-mail
-Revisar els comptes
-Revisa les faltes d'ortografia
-Davant el dubte, **ignorar el missatge**

IMPORTANT! El banc hauria de donar un avís si es fa un pagament des d'una IP no habitual

TARGETES

CARDING

Copien dades de la targeta bancària per a accedir als teus comptes

Amb ajuda de sistemes que creen combinacions de números fins a obtenir els de la tarjeta, inclòs el de seguretat

SKIMMING

Clonen la targeta de crèdit en el moment de la transacció amb dispositius que injecten al caixer

OBJECTIUS DELS DELINQÜENTS

- **Targetes de crèdit**
- **PIN** (****)
- **Fer compres**
- **Virus**

RECOMANACIONS

-Quan fas operacions al caixer la **targeta sempre a la vista**

-Sempre que sigui possible fer ús del **contactless** per evitar la clonació

-Revisar els **moviments bancaris**

-Quan una targeta caduca, **trencar la banda magnètica**