Generalitat de Catalunya

mossos d'esquadra

Prevenció

Frau i riscos Internet

Mesures de prevenció generals

- **Tenir contrasenyes segures/robustes, que no es puguin deduir. Tot seguit es detalla les característiques d'una contrasenya segura.**
  Una contrasenya segura ha de tenir al menys tres d'aquestes quatre característiques:
  - Tenir números
  - Tenir lletres
  - Tenir majúscules i minúscules
  - Tenir símbols (!, $, %, &, #, etc.)

  També ha de complir els següents requisits:
  - Longitud no inferior a vuit caràcters
  - No ha de formar-se amb números i lletres consecutius al teclat
  - No ha de contenir informació fàcil d'endevinar, com ara la informació personal
  - No ha de contenir paraules existents en cap idioma

  I per últim, però igual d'important, s'ha de:
  - Tenir una contrasenya per a cada servei
  - S'ha de canviar amb certa freqüència
  - Guardar la contrasenya en un lloc segur i no donar-la a ningú

- **Utilitzar només connexions WIFI segures, evitar les gratuïtes, per exemple per fer operacions bancàries en xarxes gratuïtes tenen més probabilitats de ser objecte d'un frau que puguin aconseguir les claus d'accés (Phishing bancari). A més per poder fer ús de connexions gratuïtes ens poden demanar dades personals i contrasenyes de xarxes socials, amb aquesta informació es facilita l'entrada a la pàgina personal ja sigui d'una entitat bancària, xarxa social....**
- **Desconnectar el Bluetooth quan no es necessita. Hi ha programes que escolten les trucades (Ex. Car Whisperer), d'altres poden tenir accés al telèfon de l'usuari i utilitzar les seves funcions (Ex. Bluebugging).**
- **No identificar la WIFI o el Bluetooth amb el nom propi o altres dades personals que es podrien identificar fàcilment.**
- **Tenir actualitzat el sistema operatiu, les APP, l'antivirus i utilitzar talla focs (el qual s'encarrega de vigilar els accessos entre l'ordinador i la xarxa. A més, bloqueja totes les connexions que no estan permeses explícitament.)**
- **Xifrar/codificar els dispositius d'emmagatzematge extern. Es pot fer en qualsevol moment utilitzant un programari adequat.**
- **Prestar atenció a la instal·lació de programaris en els PC, tablets o telèfons mòbils. Especialment en el que es detalla en els permisos.**
- **No posar informació privada o que ens pugui comprometre en perfils oberts de xarxes socials.**

Mesures de prevenció per tipus de frau

Phishing bancari (o suplantació d'identitat)
En aquest tipus de frau es cerca aconseguir contrasenyes diverses (d'identificació d'usuari bancari, el n. de targetes de crèdit, el n. de compte) amb la finalitat de poder fer transaccions amb els diners de la víctima. *Exemples: correu electrònic que simula ser la nostra entitat bancària i que ens sol·licita canviar la contrasenya que disposem, ja que ha caducat.*

Prevenció

- **No obrir correus d'usuaris desconeguts o que no s'hagin sol·licitat. Fins i tot, eliminant-los directament sense obrir cap enllaç o arxiu adjunt.**
- **Si es tracta de la web d'un banc, sempre vindrà detallada en l'adreça del navegador/URL de manera xifrada/segura i inclourà "s" https://, a més de figurar la imatge d'un cadenat.**
- **És important no accedir a serveis de banca on line a través d'ordinadors públics o xarxes WIFI.**
- **Cal recordar que les entitats bancàries no demanen mai dades personals als seus clients per correu electrònic, ni tampoc targetes bancàries o de coordenades o dades d'usuari i contrasenya. Si es reben aquest tipus de sol·licituds per correu, no és el banc.**

SMS Premium
Són números, normalment de cinc xifres, que estan regulats i són legals. Cerquen un parany perquè la víctima (enviï un SMS) faciliti el seu telèfon mòbil. Sovint es cau en el parany perquè pensem que només són publicitat sense saber que aquests missatges tenen un cost elevat.

Exemples:

- *Subscripció voluntària o involuntària d'un usuari a una base de dades que li envia informació sobre certs temes (generalment jocs i concursos), però li cobran per cada SMS rebut.*
- *Per Facebook, t'etiqueten en un vídeo i si els vols veure et demanen el número de mòbil. Si el poses ja està subscrit a SMS Premium.*
- *Missatge Whatsapp on t'informen d'una aplicació gratuïta nova que pot ser del teu interès. Et demanen el número de mòbil i et subscriuen al SMS Premium.*

Prevenció / com identificar número de SMS Premium

- **Trucar a la nostra operadora i sol·licitar que doni de baixa i bloquegin tots els serveis SMS Premium i els números de tarificació addicional**
- **Es componen de 5 a 7 xifres i comencen per 25, 27, 28, 29, 35, 37, 39, 79 o 99.**

Ransomwares

És un tipus de malware (programes maliciosos) que restringeix l'accés a determinades parts o arxius del sistema infectat, i demana un rescat a canvi de treure aquesta restricció. Es transmet tant com un *troià* com un *cuc* infectant el sistema operatiu. En aquest punt el ransomware s'iniciarà i xifrarà els arxius amb una clau que només coneix el creador. Aquest tipus de frau es pot rebre a través del correu electrònic o la consulta de determinats enllaços maliciosos a través d'Internet. *Exemple: Es rep un correu on consta com a remitent/assumpte "correos" amb el que s'informa que el destinatari ha de recollir un paquet o una carta. Dins el correu hi ha un enllaç que suposadament és per gestionar la recollida, el qual enllaça amb una pàgina web que suplanta la identitat de Correos y Telégrafos, on es sol·licita la introducció d'un codi per a consultar l'estat detallat de l'enviament. Si s'omple el codi i es prem "consultar" s'inicia la descàrrega d'un codi maliciós ransomware.*

Prevenció

- **No obrir el correu d'usuaris desconeguts o que no hagin estat sol·licitats.**
- **Esborrar el correu sense obrir-lo i assegurar-nos també d'esborrar-lo definitivament de la carpeta dels elements suprimits o esborrats.**
- **Revisar el contingut dels missatges que es rebem, i també els que enviem per evitar enviar-los a destinataris equivocats**
- **Guardar la informació en mitjans d'emmagatzematge externs, per evitar perdre informació dels clients, facturació...**
- **Apagar l'ordinador al més aviat possible, fins i tot desendollant el cable corrent. El xifrat d'arxius és un procés llarg, si aconseguim aturar-lo aviat, és possible que la majoria dels nostres documents estiguin intactes.**
- **No intentar desinfectar la màquina immediatament, esborrant fitxers sospitosos o formatant la màquina. Es podrien perdre fitxers necessaris per trencar el xifrat dels nostres documents.**

Altres modalitats de frau

- ***Estafa en compres online***
  A través de pàgines web que venen productes que no existeixen i que, tot i pagar, no es rebran. Per exemple vehicles d'alta gama.
- ***Estafes de caritat***
  Es suplanta una organització de caritat sol·licitant donacions para catàstrofes naturals, malalties o per atendre a una mare o fill malalts. Poden arribar a utilitzar-se logotips d'organitzacions prestigioses.
- ***Oferta treball (des de casa/oportunitat de negoci)***
  Aquest tipus d'estafes té molta varietat, i inclou des d'intents per aconseguir accés a la informació personal i privada de la persona que cerca feina (com ara comptes bancaris, números d'identificació personal, …) fins a requeriments de pagar una taxa per a poder entrar dins la llista de candidats a aconseguir una possible feina.
- ***Scam*** *(també anomenat frau 419, scam 419, o engany nigerià)*
  La denominació 4-1-9 ve del número de l'article del codi nigerià que sanciona aquest tipus de frau. Aquest frau es presenta generalment sota la forma d'una persona (en alguns casos es presenta com a familiar llunyà) que afirma posseir una important suma de diners (diversos milions de dòlars d'una herència, suborns, comptes sense hereu, fons a col·locar a l'estranger per un canvi de context polític, etc.) i demana l'ús d'un compte per transferir ràpidament aquests diners.
- ***Virus policial***
  En aquest cas apareix un missatge dient que estava mirant pornografia o fent descàrregues il·legals per la qual cosa ha de pagar una sanció de 100€.