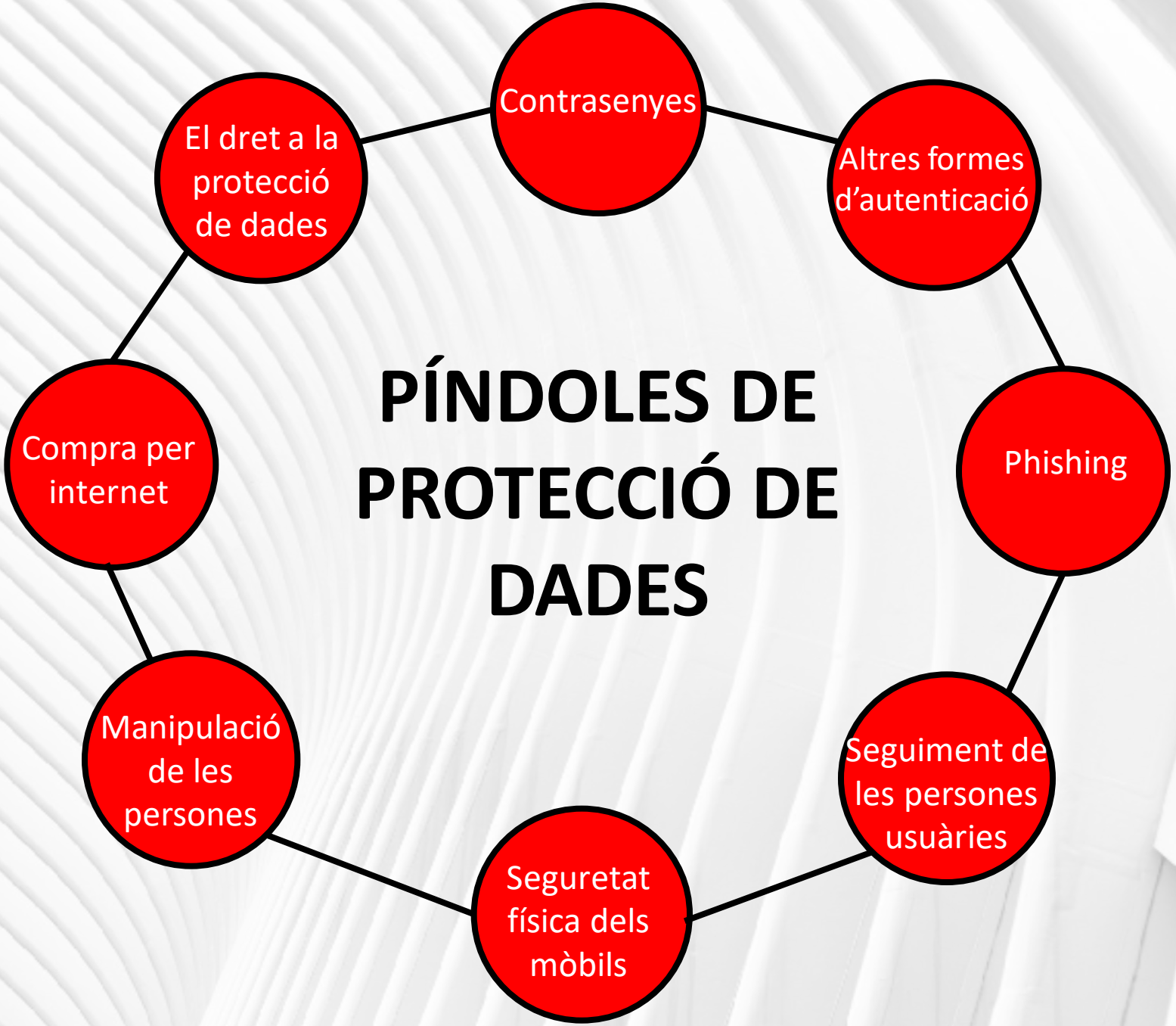
Píndoles de Protecció de Dades

apdcat

Autoritat Catalana de Protecció de Dades

ÍNDEX DE CONTINGUT

PÍNDOLES DE PROTECCIÓ DE DADES



El dret a la protecció de dades

El dret a la protecció de dades és el dret de tota persona a controlar les seves dades personals. Això permet que les persones puguin veure protegit aquest dret i, també, el conjunt de drets i llibertats que es poden veure afectats pel tractament de dades personals.

Tot i que l'individu és al centre de la protecció de dades, aquesta no és una qüestió únicament personal, sinó que dona forma a la societat on vivim. Per exemple, prohibint o requerint garanties addicionals per a tractaments concrets, com ara la vigilància sistemàtica d'àrees públiques, el tractament de categories especials de dades o les decisions automatitzades.

REGLAMENT EUROPEU

El Reglament general de protecció de dades (RGPD) és la principal normativa europea sobre aquesta matèria.

La normativa de protecció de dades regula l'ús de dades personals que fan les organitzacions.

DADES PERSONALS

Són dades personals qualsevol informació relacionada amb una persona identificada o identificable.

Aquesta identificació pot ser directa (a través d'un nom, d'un telèfon, d'un número d'identitat, etc.) o indirecta (amb la combinació de diferents factors físics, psicològics, econòmics, culturals, socials, etc.).

Cal remarcar que les dades personals no són només les que s'utilitzen per identificar una persona, sinó totes les dades sobre aquesta persona.

DRETS

La normativa de protecció de dades promou l'autodeterminació informativa. És a dir, vol donar a les persones el dret a decidir sobre el tractament de les seves dades.

Dret d'accés. Podem sol·licitar informació al responsable de tractament sobre si està tractant dades personals nostres i, en cas afirmatiu, rebre diversa informació.

Dret de rectificació. Podem demanar que es corregeixin les nostres dades, si són inexactes o incompletes.

Dret de supressió. En determinats casos, podem demanar que se suprimeixin les nostres dades.

Dret de portabilitat de les dades. Podem sol·licitar les nostres dades personals, si el tractament es fa per mitjans automatitzats i es basa en el consentiment o en el compliment d'un contracte.

Dret de limitació. En determinats casos, podem sol·licitar que s'aturi el tractament de les nostres dades.

Dret a no ser objecte de decisions individuals automatitzades. Tenim el dret a no ser objecte de decisions basades únicament en un tractament automatitzat, quan aquesta decisió té efectes significatius.

DOCUMENTS D'INTERÈS

- Reglament general de protecció de dades
- Llei orgànica de protecció de dades personals i garantia dels drets digitals
- Preguntes freqüents

Contrasenyes

Avui en dia fem ús de tot tipus de serveis en línia, que tenen accés a una gran quantitat d'informació: correu electrònic, botigues en línia, xarxes socials, aplicacions bancàries, etc.

Perdre el control d'aquests comptes pot tenir conseqüències greus: des de l'accés no autoritzat o la pèrdua de gran quantitat d'informació personal que emmagatzemem al núvol (correus, fotos, vídeos) fins a pèrdues econòmiques.

CONTRASENYES SEGURES

Les contrasenyes són l'eina més utilitzada per controlar l'accés als nostres comptes, però no serveix qualsevol contrasenya. De fet, la dificultat que suposa gestionar la gran quantitat de contrasenyes que tenim ens fa caure en pràctiques de risc:

- ✗ Ús de contrasenyes curtes que, fins i tot, poden ser paraules del diccionari. Aquestes ofereixen molt poca protecció. Un atac basat en el diccionari és suficient per trencar-les.
- ✗ Reutilització de contrasenyes. Cada vegada que reutilitzem una contrasenya, estem dient a un servei la contrasenya que fem servir en altres serveis. A banda, la reutilització de contrasenyes incrementa molt l'impacte en cas que una contrasenya es filtri. Pensa que hi ha serveis que utilitza una gran part de la població; si es filtra una contrasenya teva, es fàcil que un atacant provi amb aquests serveis.

Perquè una contrasenya sigui útil, ha de ser secreta i molt difícil d'endevinar:

- ✓ Una bona contrasenya ha de ser complexa. Hi ha diferents recomanacions: llargues amb majúscules, minúscules i caràcters especials; o fins i tot frases.
- ✓ No comparteixis ni reutilitzis les teves contrasenyes.
- ✓ Tingues precaució amb les preguntes de seguretat. Si n'hi ha, assegura't que només les coneixes tu. Tingues en compte que hi ha molta informació nostra a internet i, a banda, aquestes preguntes es presten a atacs d'enginyeria social.
- ✓ Si deses un recordatori de la contrasenya, fes-ho de manera segura.

GESTORS DE CONTRASENYES

Els gestors de contrasenyes són una solució per guardar de manera segura la multitud de contrasenyes que tenim. D'aquesta manera, n'hi ha prou de recordar la contrasenya que dona accés al gestor.

A banda, com que no cal recordar les contrasenyes, resulta més fàcil utilitzar contrasenyes prou complexes. Moltes vegades és el mateix gestor que ofereix la funcionalitat de generar contrasenyes segures.

Alguns d'aquests gestors tenen funcionalitats avançades, com alertar si descobreix que una contrasenya s'ha filtrat i, fins i tot, canviar les contrasenyes de diferents serveis des del mateix gestor.

ATACS

Les teves contrasenyes es poden filtrar encara que les gestionis correctament. La causa pot ser una violació de seguretat del proveïdor del servei o un atac adreçat contra un usuari, com ara:

- **Shoulder surfing** (o mirar per sobre de l'espatlla). Observar la contrasenya, quan la introdueixes en un lloc públic.
- **Programari espia** instal·lat al dispositiu on introdueixes la teva contrasenya (sigui el dispositiu propi o un d'aliè).
- **Observar les comunicacions** d'un dispositiu, quan es connecta a una xarxa pública i les comunicacions no són xifrades.
- **Phishing**. És l'atac més habitual, per la facilitat d'implementar-lo a gran escala de forma automatitzada.

DOCUMENTS D'INTERÈS

- Contrasenyes segures

RockYou2021.txt

Al 2021 es va publicar la recopilació de contrasenyes més gran mai feta, amb uns 8.000 milions d'entrades.

S'HAN FILTRAT?

Pots utilitzar la web https://haveibeenpwned.com per comprovar si s'han publicat les teves credencials. Fins i tot, t'hi pots subscriure perquè t'alerti si, en algun moment, les troba. Alguns gestors de contrasenyes ja ho fan automàticament.

Serveis com l'anterior no són infal·libles: convé canviar les contrasenyes periòdicament.

Altres formes d'autenticació

Tot i que les contrasenyes són el sistema més habitual d'autenticació, no són una solució perfecta. Hem vist que gestionar-les és complex i que, fins i tot fent-ho correctament, hi ha riscos. Però les contrasenyes no són l'únic sistema d'autenticació. N'hi ha d'altres, com ara l'ús de múltiples factors o la identificació biomètrica.

MÚLTIPLES FACTORS D'AUTENTICACIÓ

Les dificultats per gestionar contrasenyes segures i els múltiples atacs que hi ha posen en dubte la seguretat d'aquest sistema.

Els sistemes de múltiple factor busquen mitigar aquests riscos, requerint diferents elements per autenticar un usuari:

- **Una cosa que sé**. Per exemple, una contrasenya.
- **Una cosa que tinc**. Per exemple, el meu mòbil o una targeta.
- **Una cosa que soc**. Per exemple, la meva empremta digital.

Els sistemes de múltiple factor són una eina eficaç per millorar la seguretat. Cada capa d'autenticació afegeix una complexitat extra als atacs.

La combinació d'una contrasenya amb un codi enviat al dispositiu mòbil de l'usuari és una forma comuna d'autenticació de doble factor.

Encara que pocs llocs web tenen aquesta funcionalitat activada per defecte, n'hi ha molts que l'ofereixen. Pots consultar-ne una llista (no exhaustiva) a https://2fa.directory/

IDENTIFICACIÓ BIOMÈTRICA

Les característiques fisiològiques d'una persona són una manera de verificar la seva identitat. De fet, cada cop és més comú desbloquejar el mòbil amb l'empremta digital o la cara. És un mètode còmode per a l'usuari però, quin nivell de seguretat proporciona?

La precisió dels sistemes d'identificació biomètrica ha millorat molt en els darrers anys. Per exemple, s'estima que la probabilitat que una persona aleatòria accedeixi a un dispositiu amb Face ID és d'una entre un milió. Ara bé, un atacant no és una persona aleatòria. Per tant, cal valorar els riscos:

- Els sistemes d'identificació biomètrica necessiten guardar la nostra signatura (empremta, cara, etc.). Per tant, hi ha el risc que la nostra signatura biomètrica es filtri. Per exemple, un atac a l'Oficina de Gestió de Personal dels EUA va tenir com a resultat la filtració de més de 5 milions d'empremtes digitals de funcionaris.
- Com sempre en seguretat informàtica, hi ha una lluita entre els que desenvolupen els sistemes i els que els volen trencar. Per exemple, s'han descrit atacs per enganyar sistemes basats en empremtes i en la cara.
- Un problema físic de l'usuari pot comportar la denegació de l'accés. Per exemple, una ferida al dit pot fer fallar l'autenticació amb l'empremta digital.

Altres formes d'autenticació

Vigila amb qui comparteixes les teves dades biomètriques. Una contrasenya és fàcil de canviar si es filtra, però **les nostres característiques físiques no les podem canviar.**

- Data leak exposes unchangeable biometric data of over 1 million people
- A security breach in India has left a billion people at risk of identity theft

DOCUMENTS D'INTERÈS

- Guía de doble autenticación.
- Tecnologías biométricas aplicadas a la ciberseguridad

Phishing

La quantitat d'atacs informàtics és molt gran; alguns requereixen de grans coneixements tècnics, altres són una adaptació a l'entorn digital de l'estafa de tota la vida. El phishing (o pesca) és precisament això últim.

El fet de ser un atac relativament senzill no li treu impacte sinó al contrari, doncs es produeixen de forma massiva. Es calcula que diàriament s'envien sobre un 3.500 milions de correus electrònics de phishing i que provoca el 90% de les filtracions de dades.

QUÈ ÉS?

El phishing és una estafa feta mitjançant comunicacions electròniques. Té 3 característiques destacades:

- El correu electrònic és l'eina més habitual. També és comú el phishing telefònic (*vishing*), via SMS (*smishing*) i via WhatsApp o una altra xarxa social.
- L'atacant empra enginyeria social, fent-se passar per una persona o organització de confiança.
- L'objectiu pot ser robar informació personal (com ara credencials), infectar el dispositiu o robar diners.

EXEMPLES

En general, l'atacant vol fer-nos creure que s'ha de fer una acció amb una certa urgència.

- Un correu que simula ser del nostre banc i que afirma que, per seguretat, s'ha bloquejat el nostre compte. Aquest correu ens remet a una adreça maliciosa on introduir les nostres credencials per desbloquejar-lo.
- SMS on s'afirma que no s'ha pogut entregar un paquet i que cal accedir a un enllaç per reclamar-lo.

RECOMANACIONS

Eines com ara filtres de correu o programari que bloqueja contingut maliciós són útils contra el phishing, però no són infal·libles. Per no picar, convé ser prudent. Els consells següents ens poden ajudar:

- Sospita dels missatges no sol·licitats que transmeten la sensació d'urgència o que ens ofereixen coses a canvi de res.
- Si sospites d'un missatge, busca part del text en un cercador per comprovar si està associat a algun phishing conegut.
- Abans de seguir les indicacions (descarregar fitxers, seguir enllaços, etc.) de missatges poc habituals, confirma que és correcte per una altra via.
- Quan un correu no sol·licitat et remet a una web, vigila. Podria redirigir-te a una web maliciosa que aprofita alguna vulnerabilitat del navegador per infectar el teu ordinador.
- Quan un correu no sol·licitat et remet a una web d'un servei en el qual tens compte, revisa que l'adreça de l'enllaç sigui correcta. Sovint es creen webs que simulen ser-ne una d'autèntica per enganyar els usuaris. En cas de dubte, és millor anar a la web del servei directament, sense seguir l'enllaç del correu.
- Quan un correu no sol·licitat adjunti un fitxer o l'enllaç per descarregar-lo, pensa que alguns fitxers poden incloure comandes executables. És el cas dels documents ofimàtics, pdf i html.

SMISHING

Has rebut un SMS que parla d'una cosa urgent, d'un premi, d'un paquet que no s'ha pogut entregar, etc. Estigues alerta: les estafes també arriben per SMS.

L'smishing és una variant del phishing fet a través d'SMS. El missatge intenta que la víctima accedeixi a un enllaç inclòs al mateix SMS, truqui a un número de telèfon o respongui l'SMS.

A banda del robatori de dades personals, l'smishing té com a conseqüència molt comuna la utilització de serveis de telefonia prèmium (amb cost addicional força elevat).

TELEFONIA PRÈMIUM

Els números amb tarifació addicional s'han convertit en una forma habitual d'estafar. Si reps un SMS que intenta que truquis o enviïs un SMS a un d'aquests números, vigila.

Són números amb tarifació addicional:

- Els començats per 803, 806, 807 i 905
- Els SMS a números curts que comencen per 2, 3, 79 i 99.

Els SMS començats en 79 són especialment perillosos, ja que són serveis de subscripció i ens cobraran per cada missatge que ens enviïn.

Només necessitem les teves dades personals, envia un SMS des del teu mòbil amb la paraula OFERTA al 79... i et demanarem l'adreça. En un termini de 20 dies t'enviarem el rellotge.

Té un avís important. Truqui al (...).

DOCUMENTS D'INTERÈS

- Undestanding phishing techniques

Seguiment de les persones usuàries a internet

Internet està dominada per un reduït nombre d'empreses que ofereixen els seus serveis a milers de milions de persones, moltes vegades sense contraprestació econòmica per part dels usuaris. Això és possible perquè el principal benefici d'aquestes empreses té el seu origen en les dades que recullen. Això ha donat lloc a diverses tecnologies que permeten fer un seguiment força exhaustiu de les persones.

COOKIES

Les galetes (*cookies*) són uns petits fitxers de dades que guarda el nostre navegador quan visitem una web. La informació que guarda aquest fitxer la determina el propietari de la web i podrà recuperar-la la propera vegada que visitem el seu lloc.

Inicialment, van ser pensades per millorar l'experiència de l'usuari, ja que permeten guardar l'estat actual de la web. És a dir, permeten les sessions d'usuari. Aviat es van començar a utilitzar per rastrejar l'activitat de l'usuari per part de grans empreses d'internet que inserien les seves galetes (galetes de tercers) a gran quantitat de webs, cosa que els permetia rastrejar totes les persones usuàries d'aquestes webs.

Els navegadors permeten consultar les galetes que cada web emmagatzema en el nostre equip i gestionar-les. També podem bloquejar-les totalment o de forma selectiva.

EMPREMTA DIGITAL

Encara que desactivem les galetes, poden rastrejar-nos fent servir les característiques del nostre dispositiu. Cada dispositiu té unes característiques que són molt úniques (versió del sistema operatiu, versió del navegador, resolució de la pantalla, zona horària, llenguatges per defecte, etc.). Aquesta informació és necessària per presentar el contingut adequadament quan naveguem per internet, però alhora pot es utilitzar per rastrejar-nos.

IP I DNS

L'adreça IP és un conjunt de números que identifica el nostre dispositiu a internet. Cada comunicació que fem o rebem a internet fa servir aquest identificador.

La IP d'un dispositiu pot canviar però, per seguretat, els proveïdors de serveis d'internet (ISP), guarden la relació entre la IP i l'usuari. D'aquesta manera, en cas de necessitat es pot associar una IP amb una persona. En la mesura que totes les nostres comunicacions passen pel nostre ISP, aquest pot veure la IP dels serveis amb els quals ens comuniquem.

La IP també revela altra informació a terceres persones, com ara el proveïdor de serveis d'internet que utilitzes i una localització aproximada (per exemple, a nivell de ciutat, tot i que de vegades pot no ser correcta).

El servei de noms de domini (DNS) tradueix els noms de les webs (per exemple, apdcat.gencat.cat) a l'adreça IP que correspon. D'aquesta manera, podem navegar per internet sense haver de recordar identificadors complexos.

Normalment aquesta traducció la fa el nostre ISP, que d'aquesta manera pot rastrejar totes les webs que visitem.

NAVEGACIÓ ANÒNIMA

Ser completament anònim a internet és molt difícil, però hi ha algunes tecnologies senzilles que poden ajudar-nos a protegir el nostre anonimat.

- La recomanació més bàsica seria evitar les galetes. Així, evitem que ens puguin rastrejar de forma senzilla. Els navegadors inclouen opcions que ens permeten determinar les galetes que volem acceptar i que també permeten esborrar-les.
- VPN (xarxa privada virtual). Un dels usos de les VPN és evitar que rastregin la nostra activitat a internet. Establim una connexió xifrada amb un servidor VPN, que serà l'encarregat de fer totes les nostres peticions a internet; així, evitem que aquella activitat es pugui relacionar amb nosaltres. Ara bé, la VPN té un punt feble: com que tota la nostra activitat passa pel servidor VPN, no podem amagar-nos d'aquest servidor.
- Xarxa TOR. La xarxa TOR fa que la nostra activitat a internet passi per una xarxa de diferents nodes, on cada node fa un pas del desxifratge de la comunicació abans de passar-la al node següent. L'últim node pot veure la nostra activitat (si no està xifrada extrem a extrem) però, com que ha passat per nodes intermedis, no la pot relacionar amb nosaltres.

Quan utilitzis aquestes tècniques per navegar anònimament, pensa que no són infal·libles. Per exemple, si mentre naveguem anònimament entrem al nostre correu electrònic, estem revelant la nostra identitat al proveïdor d'aquest servei que, a partir d'aquell moment, ens podrà rastrejar. Tampoc podem amagar al nostre ISP que estem fent servir aquestes tecnologies per navegar anònimament.

DOCUMENTS D'INTERÈS

- A survey on web tracking

Seguretat física dels mòbils

El nostre mòbil s'ha convertit en una eina indispensable per fer tot tipus de tasques: comunicació i gestions personals, entreteniment i feina. Cal evitar que es produeixin accessos no autoritzats al nostre dispositiu, ja que les conseqüències poden ser importants. Per la seva naturalesa, la protecció física dels mòbils és una tasca complexa però imprescindible.

RECOMANACIONS

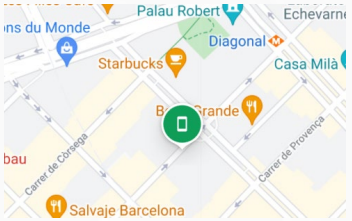
- No deixis el teu dispositiu desatès. Encara que només sigui un minut, és temps més que suficient perquè un lladre oportunista te'l robi.
- Configura un temps curt per al bloqueig de la pantalla. Un temps de bloqueig llarg (o no tenir bloqueig) podria permetre'n l'ús en cas de pèrdua o robatori.
- Utilitza contrasenya, PIN, patró o algun altre mètode per desbloquejar el dispositiu. A l'hora d'entrar el codi de desbloqueig, vigila que ningú el pugui veure, particularment si fas servir un patró.
- Fes una còpia de seguretat de les dades importants.
- Activa la funcionalitat de localització, bloqueig remot i esborrat del dispositiu en cas de pèrdua.
- Esborra les dades de forma segura abans de donar, vendre o reciclar el teu telèfon.

NO SAPS ON ÉS EL TEU MÒBIL

Tant Android com iPhone implementen un servei per localitzar el teu mòbil i gestionar-lo remotament. Pots accedir-hi a través de:

- Android. Web "Troba el meu dispositiu". https://www.google.com/android/find
- iPhone. Web "Find My". https://support.apple.com/find-my

Aquestes eines permeten:



- Mostrar la localització aproximada del dispositiu al mapa.
- Fer sonar el telèfon, encara que estigui en silenci.
- Bloquejar el telèfon remotament i mostrar un missatge que faciliti el retorn del telèfon si algú el troba.
- Esborrar el dispositiu de forma permanent. Un cop esborrat el dispositiu, aquestes funcionalitats deixaran d'estar disponibles.

Cal tenir en compte que aquestes funcionalitats només estaran disponibles si el dispositiu té connexió a internet.

Seguretat física dels mòbils

DOCUMENTS D'INTERÈS

- Mobile Device security: tips for IT pros

Manipulació de les persones

Internet, dades massives (*big data*) i intel·ligència artificial han estat grans avenços tecnològics, però tenen alguns aspectes foscos. La gran quantitat d'informació que hi ha sobre nosaltres, juntament amb la capacitat d'analitzar-la i prendre decisions de forma automàtica, ens fa susceptibles d'intents de manipulació.

FAKE NEWS

Les notícies falses sempre han existit, però és amb les xarxes socials que han proliferat. Les xarxes socials permeten que qualsevol persona esdevingui creadora de contingut (ja no ens limitem als mitjans tradicionals) i en faciliten la distribució.

Les notícies falses són un reflex de la postveritat, que fa referència a la situació en què els fets objectius són menys rellevants a l'hora de modelar l'opinió pública que les creences i les emocions.

La proliferació de notícies falses té efectes molt negatius: les persones no tenen informació veraç, la desinformació afecta la credibilitat dels mitjans tradicionals, poden generar hostilitat contra grups de persones vulnerables, etc.

Algunes recomanacions per evitar caure en la trampa de les notícies falses:

- Consulta les plataformes de verificació de fets (*fact-checking*).
- Verifica si la font de la notícia és creïble. Si la font és desconeguda, una cerca a internet pot dir-nos si altres fonts més reconegudes se'n fan ressò.
- Comprova els enllaços i les cites. Moltes vegades s'inclouen enllaços i cites falses per reforçar la credibilitat de la notícia.
- Si hi ha contingut gràfic, fes una cerca amb la imatge per veure si es tracta d'una imatge modificada o treta de context.

PERFILATGE DELS USUARIS

El perfil d'un usuari és un conjunt d'informació que ens indica com és aquell usuari. Entre altra informació, pot incloure localització, formació acadèmica, informació laboral, interessos, opinions.

Les nostres interaccions a internet generen una gran quantitat d'informació sobre nosaltres (notícies que llegim, objectes que comprem, cerques que fem, missatges que publiquem, les amistats que tenim, etc.). L'anàlisi de tota aquesta informació permet la creació de perfils molt detallats. Es pot dir que ens coneixen millor que nosaltres mateixos.

El perfil d'usuari permet la personalització dels serveis que rebem. Aquesta tasca la fan els sistemes de recomanació, basant-se en el nostre perfil: ens poden recomanar llibres, poden modificar els resultats de les nostres cerques, ens poden recomanar notícies, etc.

Mentre que moltes aplicacions són beneficioses per a les persones usuàries, els mals usos d'aquests perfils comporten riscos importants. Per exemple, aquests perfils es poden vendre o es poden utilitzar en un context electoral per fer publicitat personalitzada (dient a cada potencial elector allò que vol sentir).

Manipulació de les persones

FILTRE BOMBOLLA

El conegut filtre bombolla resulta d'una aplicació massa estricta de la personalització. L'algorisme restringeix massa la informació que es presenta a l'usuari segons el seu perfil i dona una visió molt limitada de la realitat.
En alguns casos, el filtre bombolla pot tenir efectes molt perniciosos. Per exemple, si només ens mostren les notícies que són afins a la nostra manera de pensar, podem acabar creient que la realitat és així.

DEEP FAKES

El desenvolupament de la IA permet coses que fa uns anys haurien estat impensables. Permet, per exemple, que una màquina llegeixi un text amb la veu d'una persona concreta. Però no només això: també permet modificar els trets facials d'una persona, per simular que està dient una cosa concreta. D'aquesta manera tenim els hipertrucatges (*deep fakes*).

DOCUMENTS D'INTERÈS

- ¿Qué son las fake news?
- ¿Burbujas de filtro? Hacia una fenomenología algorítmica
- What are deep fakes and how are they created?

Compra per internet

Als seus inicis, el comerç en línia provocava una forta desconfiança, sobretot a l'hora de fer els pagaments. Això s'ha superat en la darrera dècada i amb la pandèmia les compres en línia han marcat una fita. Ara bé, quina és la seguretat real que ofereix el comerç en línia?

BOTIGA DE CONFIANÇA

- Compra en botigues de confiança. Aquest és un punt realment important, sobretot perquè en botigues foranes reclamar pot ser força més complicat.
- Si no coneixes la botiga, l'avaluació feta per altres clients o els segells de confiança et poden ajudar a decidir.
- Vigila si l'oferta és massa bona. Especialment, si t'ha arribat a través d'un correu electrònic no sol·licitat.
- En la URL phishing es crea una web falsa que en simula una d'autèntica. La manera d'accedir a aquesta web acostuma a ser un enllaç en un correu no sol·licitat. Moltes vegades, l'adreça de la botiga falsa s'assembla a l'autèntica, però té alguna diferència.

SEGURETAT DE LES DADES

- Si crees un compte, assegura't que està ben protegit. Si un atacant aconsegueix entrar-hi, l'impacte pot ser elevat, fins i tot econòmicament, si el teu compte desa les dades de pagament. Utilitza una contrasenya forta i no la reutilitzis.
- La targeta és el sistema més habitual de pagament en línia. La seguretat depèn del sistema utilitzat:
    - Les passarel·les de pagament són més segures, perquè la botiga et redirigeix al web d'un banc a l'hora de fer el pagament. Així, evita gestionar dades bancàries.
    - Si no s'utilitza passarel·la de pagament, la seguretat de les teves dades és responsabilitat de la botiga.

SEGURETAT D'EQUIPS I COMUNICACIONS

Un cop tenim localitzat un lloc de confiança, cal que la compra es faci amb les millors garanties de seguretat, tant per al dispositiu utilitzat com per a les comunicacions.

- Mantingues l'equip en bon estat de seguretat: tingues el sistema operatiu i les aplicacions actualitzades, protegeix el teu compte amb algun sistema d'autenticació, utilitza programari antivirus, evita descarregar aplicacions de llocs no confiables, etc.
- No facis compres des de dispositius aliens, ja que no en coneixes l'estat de seguretat.
- Fes les compres des d'una connexió a internet confiable. Precaució amb les wifi públiques, perquè les teves dades podrien ser interceptades. A casa, la wifi xifrada i amb contrasenya forta.
- Verifica que la botiga utilitza el protocol https. El navegador ho indica amb una icona d'un cadenat tancat.

EN CAS DE DUBTE

En cas de dubte, és millor posposar la compra.

Compra per internet

UN COP FETA LA COMPRA

- Els productes comprats en línia tenen les mateixes garanties que els comprats presencialment.
- Llevat d'alguns productes, tens 14 dies per desistir de la compra.
- Recorda que tens drets sobre les teves dades personals: accés, rectificació, supressió, oposició, limitació del tractament, portabilitat de dades i no ser objecte de decisions automatitzades.

DOCUMENTS D'INTERÈS

- Compres i contractes per internet


apdcat
Autoritat Catalana de Protecció de Dades