UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Universitat Politècnica de València

Guia sobre ciberseguretat per a la comunitat UPV

12 PoliConsells

Àrea de Sistemes d'Informació y Comunicacions (ASIC)
Universitat Politècnica de València
upv.es/entidades/asic/

UPV

Guia sobre ciberseguretat per a la comunitat UPV: 12 PoliConsells

Crea un entorn digital segur amb la nostra guia amb eines, recomanacions i exemples pràctics sobre ciberseguretat per a la comunitat UPV.

1. Aprèn a detectar un correu maliciós

Pots detectar fàcilment si es tracta d'un correu fraudulent quan:

- **L'email del remitent és molt similar** a l'oficial, però no és el mateix. Pot canviar el domini o tindre més caràcters del normal.
- **Està mal redactat:** Faltes d' ortografia, frases mal construïdes o variacions d' idiomes, que cada vegada es noten menys.
- **Incita a actuar immediatament:** L'assumpte i el to inciten a actuar amb impulsivitat per conseqüències immediates com multes, cancel·lació de targetes o avisos de seguretat urgents, perquè no tinguis temps de pensar si es tracta d'un correu legítim.
- **Conté enllaços a pàgines diferents:** Si passes el ratolí per sobre dels enllaços del correu, apareixerà una finestra amb l'adreça de l'enllaç. Si la URL té un nom lleugerament diferent o no relacionat amb l' empresa probablement sigui un enllaç de phishing.

Pots comprovar tots els senyals de sospita en aquest exemple:

2. Trucs contra el Phising

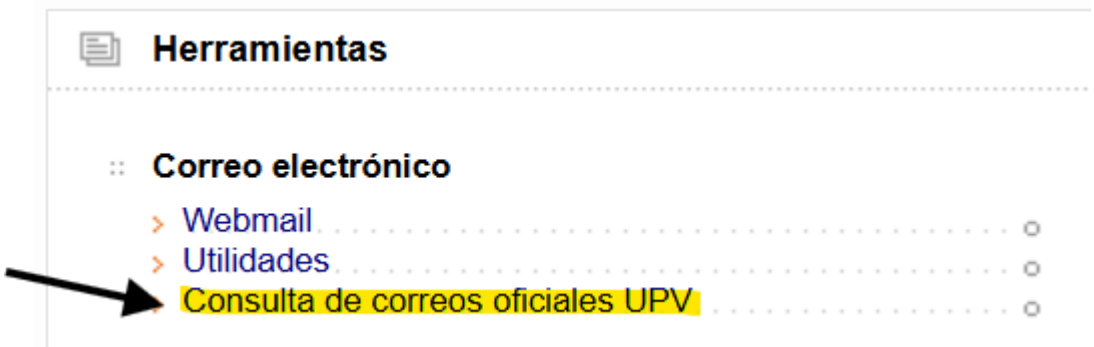
Què és el Phishing? Robatori de dades personals suplantant la identitat d'algú que coneixes, com l'exemple anterior. Algunes recomanacions pràctiques per evitar ser víctima d' aquests correus fraudulents:

- **No donar indiscriminadament dades personals** a qualsevol empresa o organització. La informació que proporciones pot ser utilitzada per crear missatges de phishing amb les nostres dades, i d'aquesta manera és més fàcil caure en el parany preparat pels atacants.
- **No publicar a internet la teva adreça de correu**. Evitar tot el possible publicar la teva adreça de correu en xarxes socials, com LinkedIn i d'altres.
- Pot ser convenient crear una adreça de correu electrònic que utilitzis **únicament per donar-te d' alta en pàgines web** i utilitzar-la com a **correu d' un sol ús.**
- Disposar d'una solució **antivirus** amb funcions anti-spam i anti-phishing instal·lada en tots els dispositius en els quals rebis el correu, tant els professionals com els personals.
- Mantenir **el programari** permanentment **actualitzat**.

3. Eines UPV

ANTIVIRUS UPV	Pots descarregar l'antivirus que et proporciona la UPV després d'identificar-te com a membre de la comunitat UPV.

En cas de dubte o activitat inusual, pots comprovar des de la secció d **'«Eines»** de la teua **Intranet** la ***Consulta de correus oficials UPV*** per a conéixer si el correu que has rebut és de la UPV si consta en el llistat de correus enviats.



Si tens algun dubte sobre algun correu sospitós que t'hagi arribat envia un correu a fraudeinternet@upv.es amb el correu sospitós com a adjunt

4. Usa contrasenyes segures

Per què les contrasenyes són importants? Les contrasenyes són la barrera que separa la teva informació personal i les dades de la universitat de possibles atacants. Si algú obté la teva contrasenya, pot accedir als teus comptes i realitzar accions en el teu nom. Això no només pot causar problemes personals, sinó que també pot comprometre la seguretat de la UPV i afectar altres persones amb les quals et relaciones, i fins i tot tota la comunitat universitària.

Normes i recomanacions UPV per a la gestió de contrasenyes segures

- **Utilitza** almenys **15 caràcters**, com més tingui, més difícil serà d'endevinar.
- **Utilitza minúscules, majúscules, números i caràcters especials** (&,%;@,#).
- **No incloguis** informació personal o paraules comunes com: els teus cognoms, DNI o data de naixement, dies de la setmana o refranys.
- **Evita** seqüències de teclat o de numeració com: qwerty, 1234567 o poiuy.
- **No reutilices la teva contrasenya.** Si utilitzes la mateixa contrasenya per a una xarxa social i té una bretxa de seguretat, un atacant podria fer servir aquesta contrasenya per accedir al teu compte de correu universitari.
- **Canvia la teva contrasenya** cada any.
- Fa servir un **gestor de contrasenyes** (com KeePass o del teu navegador web) i utilitza una contrasenya robusta per accedir al teu gestor; així només necessitaràs recordar una **contrasenya mestra**.
- **No escriguis** contrasenyes en un paper o en un arxiu al teu ordinador, **utilitza gestors de contrasenyes oficials**.
- Verifica **on introdueixes la teva contrasenya**, verifica el nom del domini que sigui correcte.

Utilitza una frase llarga fàcil de recordar i transfórmala afegint símbols i números.

Alguns exemples:

- La meva cançó favorita dels anys 80 és Livin' on a Prayer → «Mcfdla80eL'oaP!
- Jo naix un 7 de Març a les 3:15 → yn17M@3:15.

5. Protegeix els teus dispositius

- Les **xarxes WiFi públiques de llocs públics** són les que no tenen candau, per tant, no tenen certs nivells de seguretat. Les **dades** que enviïs poden ser **fàcilment interceptades** per algú que utilitzi aquesta xarxa WiFi. Pots configurar la VPN de la UPV, la Xarxa Privada Virtual (VPN) corporativa que xifra les teues dades quan navegues per internet.
- **Desactiva el Blueetooth i NFC** del teu mòbil mentre no els utilitzis.
- **Desconfia dels codis QR** sobre els quals no tens garantia d'autenticitat.
- **Evita els carregadors públics** poden ser modificats per controlar el teu mòbil en connectar-lo.
- **Mantenen actualitzat el sistema operatiu i les aplicacions**.
- Verifica que tens **activat el xifrat** per defecte al teu mòbil.
- Revisa els **permisos necessaris per al funcionament de les aplicacions**. Necessita una aplicació de llanterna accedir als teus contactes?
- **Descarrega aplicacions de botigues oficials (Google Play Store a Android i App Store en iOS)**

ANTIVIRUS UPV

Pots descarregar l'antivirus que et proporciona la UPV després d'identificar-te com a membre de la comunitat UPV.

Evita el robatori dels teus dispositius

- **Bloqueja el teu dispositiu** per empremta digital, imatge de la teva cara o per un pin prou llarg.
- **No deixis els teus dispositius sense supervisió** en llocs públics o en zones fàcilment accessibles com butxaques exteriors. Guardalls en llocs segurs.
- Tant Android com iOS tenen funcions integrades per **rastrejar dispositius perduts** («Trobar el meu dispositiu» a Android i «Buscar el meu iPhone» en iOS). Aquestes funcions també permeten bloquejar el dispositiu i esborrar les dades de forma remota, assegurant que la informació no caigui en mans equivocades.

Actua en cas de robatori dels teus dispositius

- En cas de robatori o pèrdua utilitza la **funció de rastreig per trobar el dispositiu**. Si no és possible recuperar-lo bloqueja i esborra les dades immediatament.
- **Acusa't d'informar del robatori a les autoritats**. Necessitaran el codi IMEI del mòbil, un identificador únic que ajuda els cossos de seguretat a localitzar-lo amb la col·laboració de les empreses de telefonia mòbil. Pots trobar el codi IMEI a la pantalla de configuració del mòbil o a la caixa on te'l van entregar. Anòtalo en un lloc segur per poder recuperar-lo en cas de robatori o pèrdua.

6. Activa el doble factor d'autenticació (2FA)

Pots afegir una **capa extra de seguretat** en iniciar sessió utilitzant el doble factor d'autenticació (2FA), a més de la teva contrasenya. Aquest tipus d'autenticació **requereix que verifiquis la teva identitat** amb un segon factor com: la teva empremta digital, un SMS, una notificació o mitjançant una aplicació d'autenticació oficial al teu mòbil per confirmar que ets tu qui està accedint. En utilitzar el doble factor de seguretat cal que configuris mètodes alternatius, com proporcionar un número de mòbil secundari perquè puguis iniciar sessió en cas que perdis el mòbil.

Pots utilitzar el doble factor d'autenticació de Microsoft 365 UPV, d'aquesta manera, cada vegada que inicies sessió en Microsoft 365 de la UPV, hauràs d'introduir un codi per a iniciar sessió amb l'aplicació Microsoft Authenticator.

7. Coneix el Malware

Què és?

Programes maliciosos dissenyats per danyar el teu dispositiu o robar informació.

Com arriba al meu equip?

A través de la instal·lació d'un programa des d'una font no segura, per exemple, d'un disc extraïble o un pendrive.

A través de la instal·lació de programari pirata o il·legal, té un risc molt alt de contenir malware.

A través d' un enllaç fraudulent de correu electrònic.

A través del navegador, obrint un enllaç fraudulent.

Com puc eliminar-lo?

Un cop un equip és infectat és molt difícil eliminar-lo per complet, per això, és molt important la prevenció. Per eliminar-lo cal reinstal·lar l'ordinador des de zero amb una instal·lació neta, que té un cost de temps i personal elevat.

8. Navega de forma segura

Per comprovar la seguretat d'un lloc web, fica't en aquests elements:

- **Enllaç quotidià:** La millor pràctica és sempre començar la navegació des d'una pàgina coneguda, guardada en marcadors, d'ús freqüent o escriure-la manualment i no des d'un enllaç que rebis per correu o navegant per la web.
- **Candau:** Busca l'arrel d'un candau a la barra de direccions.
- **Detalls del certificat del servidor:** Fes clic al candau per veure els detalls del certificat.
- **Barra d'adreces:** Assegura't que la URL comenci amb «https://».
- **Assegura't que la URL que estàs visitant és la URL original i no una còpia**. Que tingui un certificat no serveix per assegurar-nos que la pàgina és veritable. És important **comprovar que és la URL del certificat de servidor correspon a la pàgina que vols visitar** i no a una còpia.

Eines i extensions per millorar la seguretat

- **L' antivirus i EDR**: És l' eina principal. Tenir l'antivirus corporatiu instal·lat i actualitzat és el teu millor escut contra el malware. La major part de les webs fraudulentes o amb risc les va a bloquejar automàticament.
- **Bloquejadors d'anuncis**: Existeixen **extensions de navegador** denominats bloquejadors d'anuncis **(AdBlock)** que a més d'intentar eliminar la publicitat, eviten també que en la navegació se'ns dirigeixi a pàgines sospitoses.

9. Recomanacions preventives

No facis clic en enllaços sospitosos

- Abans de fer clic a qualsevol enllaç**, verifica la URL passant el cursor sobre l'enllaç** per veure l'adreça completa**. Desconfia d' URLs abreujades** o que contenen caràcters estranys.
- Els **escurçadors de direccions** suposen cada vegada un major risc, perquè no permeten comprovar quina és la URL a la qual ens dirigeixen i poden amagar un intent d'encaminar-nos a una pàgina fraudulenta o amb malware. En la mesura del possible, mai en enllaços escurçats.
- D' igual manera **es desaconsella l' ús de codis QR**, pel mateix motiu que els escurçadors d' URL. No podem tenir certesa del lloc al qual ens estan enviant abans de punxar. S'han arribat a cometre fraus enganxant una enganxada en espais públics amb un QR diferent al lícit, de manera que redirigeixen els usuaris a pàgines fraudulentes.

Evita descàrregues de fonts no verificades

- **Descàrrega programari i arxius només de llocs web oficials i confiables.** Les descàrregues de fonts no verificades com **a programari pirata o il·legal**, poden contenir malware.
- **Exemple pràctic:** En buscar un programa específic, assegura't de descarregar-lo del lloc web oficial del desenvolupador o de les botigues oficials del sistema operatiu (habitualment Microsoft Store o App Store de Mac).

10. No comparteixes informació personal en xarxes socials

Compartir dades personals en xarxes socials s'ha convertit en una pràctica comuna, però té certs riscos que poden passar per alt en el nostre dia a dia. És possible que comparteixes informació personal sense que et donin compte com: **fotografies de casa teva, els teus amics, els seus noms, on vius, treballes o estudies, i fins i tot dades de contacte.**

La informació que comparteixis pot ser utilitzada per tercers per **crear perfils falsos, suplantar la teva identitat, usar les teves fotos i cometre fraus en el teu nom**. Publicar la teva ubicació o plans de viatges proporciona informació sensible sobre **on estàs o sobre on no estàs, com per exemple casa teva.**

És important conèixer els riscos i compartir la informació que vols només amb persones que coneguis. Un **perfil privat** garanteix que ningú excepte qui tu permets, pugui veure el teu contingut.

11. Bloqueja la teva sessió quan no hi siguis present

L'ordinador del teu lloc de treball o d'estudi t'identifica per a qualsevol acció. És important bloquejar la sessió quan estiguis absent perquè ningú pugui fer servir el teu ordinador en el teu nom. Pots fer-ho ràpidament amb dreceres:

- **Windows**: Windows +L
- **MacOS**: Control + Comando +Q

12. Consciència sobre ciberseguretat

Per garantir la teva seguretat i la de totes les persones amb les quals et relaciones, cal **informar sobre els riscos, mesures i conseqüències de les nostres accions online** que és possible que altres persones no coneguin. Protegir les dades dels altres, també significa protegir els teus.