UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Universitat Politècnica de València

Guía sobre ciberseguridad para la comunidad UPV

12 PoliConsejos

Área de Sistemas de Información y Comunicaciones (ASIC)
Universitat Politècnica de València
www.upv.es

UPV

Guía sobre ciberseguridad para la comunidad UPV: 12 PoliConsejos

Crea un entorno digital seguro con nuestra guía con herramientas, recomendaciones y ejemplos prácticos sobre ciberseguridad para la comunidad UPV.

1. Aprende a detectar un correo malicioso

Puedes detectar fácilmente si se trata de un correo fraudulento cuando:

- **El email del remitente es muy similar** al oficial, pero no es el mismo. Puede que cambie el dominio o tenga más caracteres de lo normal.
- **Está mal redactado:** Faltas de ortografía, frases mal construidas o variaciones de idiomas, que cada vez se notan menos.
- **Incita a actuar inmediatamente:** El asunto y el tono incitan a actuar con impulsividad por consecuencias inmediatas como multas, cancelación de tarjetas o avisos de seguridad urgentes, para que no tengas tiempo de pensar si se trata de un correo legítimo.
- **Contiene enlaces a páginas diferentes:** Si pasas el ratón por encima de los enlaces del correo, aparecerá una ventana con la dirección del enlace. Si la URL tiene un nombre ligeramente distinto o no relacionado con la empresa probablemente sea un enlace de phishing.

Puedes comprobar todas las señales de sospecha en este ejemplo:

2. Trucos contra el Phising

¿Qué es el Phishing? Robo de datos personales suplantando la identidad de alguien que conoces, cómo el ejemplo anterior. Algunas recomendaciones prácticas para evitar ser víctima de estos correos fraudulentos:

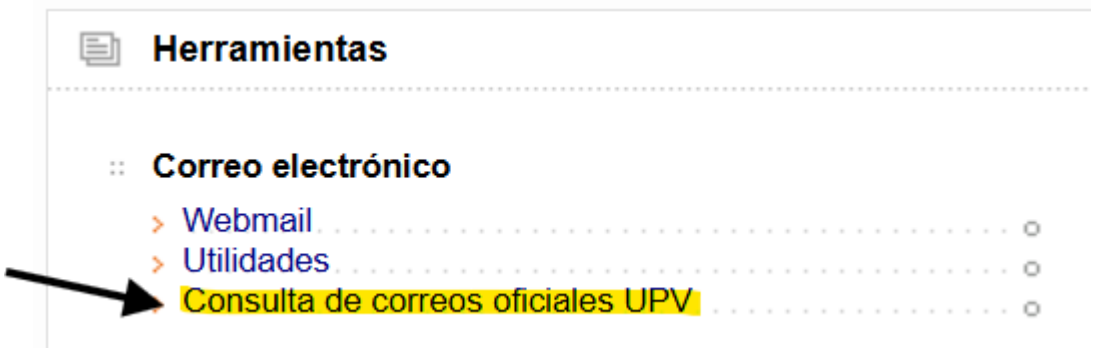
- No dar indiscriminadamente datos personales a cualquier empresa u organización. La información que proporcionas puede ser utilizada para crear mensajes de phishing con nuestros datos, y de esta manera es más fácil caer en la trampa preparada por los atacantes.
- No publicar en internet tu dirección de correo. Evitar todo lo posible publicar tu dirección de correo en redes sociales, como LinkedIn y otras.
- Puede ser conveniente crear una dirección de correo electrónico que utilices únicamente para darte de alta en páginas web y utilizarla como correo desechable.
- Disponer de una solución antivirus con funciones anti-spam y anti-phishing instalada en todos los dispositivos en los que recibas el correo, tanto los profesionales como los personales.
- Mantener el software permanentemente actualizado.

3. Herramientas UPV

ANTIVIRUS UPV

Puedes descargar el antivirus que te proporciona la UPV después de identificarte como miembro de la comunidad UPV.

En caso de duda o actividad inusual, puedes comprobar desde la sección de **«Herramientas»** de tu **Intranet** la ***Consulta de correos oficiales UPV*** para conocer si el correo que has recibido es de la UPV si consta en el listado de correos enviados.



Si tienes alguna duda sobre algún correo sospechoso que te haya llegado envía un correo a fraudeinternet@upv.es con el correo sospechoso como adjunto

4. Usa contraseñas seguras

¿Por qué las contraseñas son importantes? Las contraseñas son la barrera que separa tu información personal y los datos de la universidad de posibles atacantes. Si alguien obtiene tu contraseña, puede acceder a tus cuentas y realizar acciones en tu nombre. Esto no solo puede causar problemas personales, sino que también puede comprometer la seguridad de la UPV y afectar a otras personas con las que te relacionas, e incluso toda la comunidad universitaria.

Normas y recomendaciones UPV para la gestión de contraseñas seguras

- **Utiliza** al menos **15 caracteres**, cuantos más tenga, más difícil será de adivinar.
- **Utiliza minúsculas, mayúsculas, números y caracteres especiales** (&,%;@,#).
- **No incluyas** información personal o palabras comunes como: tus apellidos, DNI o fecha de nacimiento, días de la semana o refranes.
- **Evita** secuencias de teclado o de numeración como: qwerty, 1234567 o poiuy.
- **No reutilices tu contraseña.** Si utilizas la misma contraseña para una red social y tiene una brecha de seguridad, un atacante podría usar esa contraseña para acceder a tu cuenta de correo universitario.
- **Cambia tu contraseña** cada año.
- Usa un **gestor de contraseñas** (como KeePass o de tu navegador web) y utiliza una contraseña robusta para acceder a tu gestor; así solamente necesitarás recordar una **contraseña maestra**.
- **No escribas** contraseñas en un papel o en un archivo en tu ordenador, **utiliza gestores de contraseñas oficiales**.
- Verifica **dónde introduces tu contraseña**, verifica el nombre del dominio que sea correcto.

Utiliza una frase larga fácil de recordar y transfórmala añadiendo símbolos y números.

Algunos ejemplos:

- Mi canción favorita de los años 80 es Livin' on a Prayer → «Mcfdla80eL'oaP!
- Yo nací un 7 de Marzo a las 3:15 → yn17M@3:15.

5. Protege tus dispositivos

- Las **redes WiFi públicas de lugares públicos** son las que no tienen candado, por tanto, no tienen ciertos niveles de seguridad. Los **datos** que envíes pueden ser **fácilmente interceptados** por alguien que utilice esa red WiFi. Puedes configurar la VPN de la UPV, la Red Privada Virtual (VPN) corporativa que cifra tus datos cuando navegues por internet.
- **Desactiva el Blueetooth y NFC** de tu móvil mientras no los utilices.
- **Desconfía de los códigos QR** sobre los que no tienes garantía de autenticidad.
- **Evita los cargadores públicos**, ya que pueden ser modificados para controlar tu móvil al conectarlo.
- **Mantén actualizado el sistema operativo y las aplicaciones**.
- Verifica que tienes **activado el cifrado** por defecto en tu móvil.
- Revisa los **permisos necesarios para el funcionamiento de las aplicaciones**. ¿Necesita una aplicación de linterna acceder a tus contactos?
- **Descarga aplicaciones de tiendas oficiales (Google Play Store en Android y App Store en iOS)**

ANTIVIRUS UPV

Puedes descargar el antivirus que te proporciona la UPV después de identificarte como miembro de la comunidad UPV.

Evita el robo de tus dispositivos

- **Bloquea tu dispositivo** por huella digital, imagen de tu cara o por un pin lo suficientemente largo.
- **No dejes tus dispositivos sin supervisión** en lugares públicos o en zonas fácilmente accesibles como bolsillos exteriores. Guárdalos en lugares seguros.
- Tanto Android como iOS tienen funciones integradas para **rastrear dispositivos perdidos** («Encontrar mi dispositivo» en Android y «Buscar mi iPhone» en iOS). Estas funciones también permiten bloquear el dispositivo y borrar los datos de forma remota, asegurando que la información no caiga en manos equivocadas.

Actúa en caso de robo de tus dispositivos

- En caso de robo o pérdida utiliza la **función de rastreo para encontrar el dispositivo**. Si no es posible recuperarlo bloquea y borra los datos inmediatamente.
- **Acuérdate de informar del robo a las autoridades**. Necesitarán el código IMEI del móvil, un identificador único que ayuda a los cuerpos de seguridad a localizarlo con la colaboración de las empresas de telefonía móvil. Puedes encontrar el código IMEI en la pantalla de configuración del móvil o en la caja en la que te lo entregaron. Anótalo en un sitio seguro para poder recuperarlo en caso de robo o pérdida.

6. Activa el doble factor de autenticación (2FA)

Puedes añadir una **capa extra de seguridad** al iniciar sesión utilizando el doble factor de autenticación (2FA), además de tu contraseña. Este tipo de autenticación **requiere que verifiques tu identidad** con un segundo factor como: tu huella digital, un SMS, una notificación o mediante una aplicación de autenticación oficial en tu móvil para confirmar que eres tú quien está accediendo. Al utilizar el doble factor de seguridad es necesario que configures métodos alternativos, como proporcionar un número de móvil secundario para que puedas iniciar sesión en caso de que pierdas el móvil.

Puedes utilizar el doble factor de autenticación de Microsoft 365 UPV, de esta forma, cada vez que inicies sesión en Microsoft 365 de la UPV, deberás introducir un código para iniciar sesión con la aplicación Microsoft Authenticator.

7. Conoce el Malware

¿Qué es?

Programas maliciosos diseñados para dañar tu dispositivo o robar información.

¿Cómo llega a mi equipo?

A través de la instalación de un programa desde una fuente no segura, por ejemplo, de un disco extraíble o un pendrive.

A través de la instalación de software pirata o ilegal, tiene un riesgo muy alto de contener malware.

A través de un enlace fraudulento de correo electrónico.

A través del navegador, abriendo un enlace fraudulento.

¿Cómo puedo eliminarlo?

Una vez que un equipo es infectado es muy difícil eliminarlo por completo, por eso, es muy importante la prevención. Para eliminarlo es necesario reinstalar el ordenador desde cero con una instalación limpia, que tiene un coste de tiempo y personal elevado.

8. Navega de forma segura

Para comprobar la seguridad de un sitio web, fíjate en estos elementos:

- **Enlace cotidiano:** La mejor práctica es siempre empezar la navegación desde una página conocida, guardada en marcadores, de uso frecuente o escribirla manualmente y no desde un enlace que recibas por correo o navegando por la web.
- **Candado:** Busca el ícono de un candado en la barra de direcciones.
- **Detalles del certificado del servidor:** Haz clic en el candado para ver los detalles del certificado.
- **Barra de direcciones:** Asegúrate de que la URL comience con «https://».
- **Asegúrate que la URL que estás visitando es la URL original y no una copia**. Que tenga un certificado no sirve para asegurarnos que la página es verdadera. Es importante **comprobar que es la URL del certificado de servidor corresponde a la página que quieres visitar** y no a una copia.

Herramientas y extensiones para mejorar la seguridad

- **El antivirus y EDR**: Es la herramienta principal. Tener el antivirus corporativo instalado y actualizado es tu mejor escudo contra el malware. La mayor parte de las webs fraudulentas o con riesgo las va a bloquear automáticamente.
- **Bloqueadores de anuncios**: Existen **extensiones de navegador** denominados bloqueadores de anuncios **(AdBlock)** que además de intentar eliminar la publicidad, evitan también que en la navegación se nos dirija a páginas sospechosas.

9. Recomendaciones preventivas

No hagas clic en enlaces sospechosos

- Antes de hacer clic en cualquier enlace**, verifica la URL pasando el cursor sobre el enlace** para ver la dirección completa**. Desconfía de URLs abreviadas** o que contienen caracteres extraños.
- Los **acortadores de direcciones** suponen cada vez un mayor riesgo, porque no permiten comprobar cuál es la URL a la que nos dirigen y pueden esconder un intento de encaminarnos a una página fraudulenta o con malware. En la medida de lo posible, nunca pinches en enlaces acortados.
- De igual manera **se desaconseja el uso de códigos QR**, por el mismo motivo que los acortadores de URL. No podemos tener certeza del sitio al que nos están enviando antes de pinchar. Se han llegado a cometer fraudes pegando una pegatina en espacios públicos con un QR distinto al lícito, de manera que redirigen a los usuarios a páginas fraudulentas.

Evita descargas de fuentes no verificadas

- **Descarga software y archivos solo de sitios web oficiales y confiables.** Las descargas de fuentes no verificadas como **software pirata o ilegal**, pueden contener malware.
- **Ejemplo práctico:** Al buscar un programa específico, asegúrate de descargarlo del sitio web oficial del desarrollador o de las tiendas oficiales del sistema operativo (habitualmente Microsoft Store o App Store de Mac).

10. No compartas información personal en redes sociales

Compartir datos personales en redes sociales se ha convertido en una práctica común, pero tiene ciertos riesgos que pueden pasar por alto en nuestro día a día. Es posible que compartas información personal sin que te des cuenta como: **fotografías de tu casa, tus amigos, sus nombres, dónde vives, trabajas o estudias, e incluso datos de contacto.**

La información que compartas puede ser utilizada por terceros para **crear perfiles falsos, suplantar tu identidad, usar tus fotos y cometer fraudes en tu nombre**. Publicar tu ubicación o planes de viajes proporciona información sensible sobre **dónde estás o sobre dónde no estás, como por ejemplo tu casa.**

Es importante conocer los riesgos y compartir la información que quieres solamente con personas que conozcas. Un **perfil privado** garantiza que nadie excepto quien tu permites, pueda ver tu contenido.

11. Bloquea tu sesión cuando no estés presente

El ordenador de tu puesto de trabajo o de estudio te identifica para cualquier acción. Es importante bloquear la sesión cuando estés ausente para que nadie pueda usar tu ordenador en tu nombre. Puedes hacerlo rápidamente con atajos:

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

12. Conciencia sobre ciberseguridad

Para garantizar tu seguridad y la de todas las personas con las que te relacionas, es necesario **informar sobre los riesgos, medidas y consecuencias de nuestras acciones online** que es posible que otras personas no conozcan. Proteger los datos de los demás, también significa proteger los tuyos.