

SEMÁFORO DE PRÁCTICAS DE USO SEGURIDAD MÓVIL, SERVICIOS EN LA NUBE Y REDES PÚBLICAS

VERDES “seguras”

1. **Protege tu dispositivo con una buena funda que evite roturas si se te cae al suelo. (PROTECCIÓN FÍSICA)**

Los teléfonos smartphone son unos dispositivos muy frágiles (sobre todo la pantalla táctil) que suelen sufrir caídas, golpes y otros maltratos por parte de sus usuarios. Una buena funda protectora nos evitará gran parte de esos maltratos y hará que nuestro dispositivo aguante en perfectas condiciones de uso durante mucho más tiempo.

#CONSEJO: Un añadido estupendo son los protectores de pantalla. Teniendo en cuenta que es la parte más frágil de tu Smartphone, merece la pena invertir unos pocos euros más y comprar un protector de vidrio que nos permita una buena visión de la misma y una correcta experiencia táctil del dispositivo.

2. **Limpia con frecuencia los contenidos que almacenas en el dispositivo y procura no llevar en él contenidos sensibles innecesarios. (SEGURIDAD ANTE PÉRDIDAS O ROBOS)**

A veces llevamos en el teléfono contenido privado (fotografías personales, números de cuenta, fotografías de facturas, datos bancarios...) que, si bien no plantea ningún problema el perderlos, ya que los podemos recuperar después de la nube o mediante otros recursos, no deseamos que nadie tenga acceso a los mismos porque pueden suponer un problema de privacidad para nosotros en muchos sentidos.

3. **Activa tus conexiones inalámbricas: (WiFi, Bluetooth, NFC, AirDrop...) únicamente cuando vayas a hacer uso de ellas. (SEGURIDAD EN TUS CONEXIONES)**

Dejar abiertas ese tipo de conexiones sin necesidad es como dejar una posible puerta abierta a usuarios malintencionados. Aunque suelen ser bastante seguras, nunca está de más añadir un poco de protección extra y ahorrarse batería.

4. **Descarga aplicaciones sólo desde fuentes seguras y confiables. (SEGURIDAD DEL SOFTWARE)**

En Android, desactiva la opción 'Permitir orígenes desconocidos' (a través de los Ajustes de Seguridad del dispositivo) para que no se instalen aplicaciones de tiendas no oficiales. Sólo las tiendas oficiales aseguran que el software que instalas no tiene ningún error de seguridad ni es de carácter malicioso.

5. **Elimina las aplicaciones que no esté utilizando. (SEGURIDAD PARA TU PRIVACIDAD)**

Una aplicación que no utilizas ocupa un espacio innecesario en tu teléfono y, si no la actualizas, puede suponer un agujero de seguridad en tu dispositivo.

#CONSEJO: Elimina todas aquellas aplicaciones que lleves sin utilizar más de un año. Si alguna vez vuelves a necesitarla, bastará con que la vuelvas a descargar desde el repositorio oficial.

NARANJAS “con precaución”

6. **Apunta en algún lugar distinto al móvil el número IMEI de tu dispositivo. (SEGURIDAD ANTE PÉRDIDAS O ROBOS)**

Este código de identificación único de tu teléfono móvil puede ser requerido por la Policía a la hora de poner una denuncia y, llegado el caso, te permitirá pedirle a tu operadora que lo inhabilite.

#CONSEJO: Lo encontrarás, por norma general, en la parte de atrás de la batería, en la caja o en la factura de compra. También puedes consultarlo marcando en tu dispositivo *#06#

7. **Realiza con frecuencia copias de seguridad de los contenidos del dispositivo. (SEGURIDAD ANTE PÉRDIDAS O ROBOS)**

No te arriesgues a quedarte, además de sin la herramienta, sin tu agenda, calendario, textos, fotos, vídeos, apps, música...

#CONSEJO: Hay aplicaciones, como Dropbox, que, una vez instaladas y correctamente configuradas, sincronizan los datos de tu dispositivo en la nube, de forma que, por ejemplo, cada vez que sacas una fotografía, ésta se guarda también en la nube al conectarse a una red WiFi. También puedes guardar en la nube, de forma totalmente segura y privada, tus conversaciones de whatsapp, la configuración de tu teléfono, tu lista de contactos... De este modo, aunque pierdas tu dispositivo, siempre tendrás guardada en la nube una copia de tus datos más importantes.

8. **Sé prudente a la hora de conectarte a redes públicas.**
(SEGURIDAD EN TUS CONEXIONES)

Cuando te conectas a una red WiFi pública la seguridad de los datos que transmites queda en entredicho. Cualquiera que esté conectado a esa misma red WiFi abierta y que tenga unos ciertos conocimientos de informática podría acceder a tus comunicaciones e incluso a los datos que tienes almacenados en tu teléfono móvil (fotografías, archivos...).

#CONSEJO: Evita, en la medida de lo posible, conectarte a este tipo de redes públicas gratuitas, aunque ello te suponga ahorrarte unos pocos megas en tu consumo de datos.

9. **Evita utilizar tus memorias USB en ordenadores públicos.**
(SEGURIDAD DEL SOFTWARE)

Este tipo de ordenadores son un foco muy peligroso de contagio en cuanto a virus y software malicioso.

#CONSEJO: Si necesitas pasar archivos de un ordenador a otro, utiliza servicios de almacenamiento en la nube como Dropbox o WeTransfer (este segundo es para enviar archivos de gran tamaño).

10. **Utiliza con seguridad los servicios de almacenamiento en la nube.**
(SEGURIDAD PARA TU PRIVACIDAD)

Los servicios en la nube son un recurso estupendo para almacenar información con un nivel altísimo de seguridad. Pero nosotros mismos debemos cuidar de que esa seguridad no se vea en entredicho. Para ello deberemos utilizar contraseñas robustas, no conectarnos desde ordenadores públicos o redes WiFi abiertas, nunca anotar o compartir nuestras contraseñas con nadie...

#CONSEJO: A pesar de que son aplicaciones extremadamente seguras, se recomienda no almacenar en la nube datos que sean especialmente sensibles como tus contraseñas de acceso a servicios bancarios, datos personales, etc.

ROJAS “peligrosas”

11. **Protege tu dispositivo con contraseña.** (SEGURIDAD DE ACCESO)

Desde luego, es un fastidio tener que desbloquear el teléfono cada vez que lo vayas a usar. A veces lo tenemos que repetir decenas y decenas de veces cada día. Pero más fastidioso es perder el teléfono y que cualquiera, libremente, pueda acceder a tu información personal (contactos, conversaciones de whatsapp, correos electrónicos...) o pueda utilizar tu dispositivo haciéndose pasar por ti (podría escribir desde tu whatsapp, publicar en tus redes sociales, enviar correos desde tu cuenta...).

#CONSEJO: Lo conveniente es utilizar, como mínimo, una contraseña numérica o un patrón de desbloqueo. Si tu dispositivo cuenta con protección biométrica, como lectura de huella dactilar, el desbloqueo es muy rápido y muy sencillo.

12. **Protege tu teléfono con un código de acceso y la tarjeta SIM con un PIN.** (SEGURIDAD ANTE PÉRDIDAS O ROBOS)

En caso de pérdida o robo, no podrán acceder a tu teléfono (ya sea con tu tarjeta o con otra distinta) y no podrán utilizar tu tarjeta con otro teléfono distinto.

#CONSEJO: Guarda el código pin de tu tarjeta en un lugar seguro. Si lo pierdes, ésta quedará inservible y deberás hacer un duplicado de la misma.

13. **Mantén tu sistema operativo y tus aplicaciones actualizadas.** (SEGURIDAD DEL SOFTWARE)

Los desarrolladores trabajan continuamente para tratar de mejorar la seguridad y corrección de errores. Por ello es muy importante tener instaladas siempre las últimas versiones para que todo funcione a la perfección y estés protegido contra los últimos virus y errores conocidos.

#CONSEJO: activa las diferentes opciones de actualización automática que ofrece cada dispositivo para no tener que preocuparte por realizar estas importantes tareas de mantenimiento de forma manual.

14. Comprueba los privilegios de acceso que le otorgas a cada una de tus aplicaciones. (SEGURIDAD PARA TU PRIVACIDAD)

Hay algunas aplicaciones que te piden acceso a ciertos privilegios del teléfono (agenda de contactos, capacidad para realizar llamadas, publicar en tu nombre en algunas redes sociales, ubicación...) que realmente no necesitan y que pueden utilizar con fines maliciosos o para recopilar datos personales sobre tu actividad

#CONSEJO: Si bien es una auténtica tortura leer las cláusulas y condiciones de privacidad cuando instalas cada una de tus aplicaciones, además de que suelen utilizar una terminología ininteligible para la mayoría de nosotros, sí que debes prestar más atención a la hora de conceder los privilegios de acceso durante la instalación de cada una de ellas. Es normal que una aplicación de calendario te pida acceso a tu lista de contactos, para así poder mostrarte, por ejemplo, los cumpleaños de cada uno de ellos. Lo que no es normal es que te pida permiso para publicar en tu nombre en una red social, generalmente con fines de publicidad y difusión para esa aplicación.

15. Instala un antivirus y mantenlo convenientemente actualizado. (SEGURIDAD DEL SOFTWARE)

Un buen antivirus evitará que cualquier tipo de software malicioso pueda darte un disgusto enorme. Hoy en día nunca se sabe de qué forma, por muy cuidadosos que seamos, puede llegar a infectarnos un virus informático. Hay algunos antivirus gratuitos, como Avast, que hacen muy bien su trabajo.

#CONSEJO: Merece la pena invertir unos cuantos euros en las versiones mejoradas de algunos antivirus, ya que añaden muchas opciones extra en cuanto a la seguridad de nuestros datos y de nuestras conexiones. Piensa en la cantidad de fotos irrepetibles que guardas en tu ordenador, en la cantidad de horas de trabajo que hay detrás de todos esos archivos que guardas, en la cantidad de datos personales a los que nadie quiere que tenga acceso...

Álvaro Castillo Calvo
@alvarocastill
www.cuchuflete.es/portfolio

