Cultura de la Ciberseguridad

¿Por qué es tan importante la ciberseguridad?

Las tecnologías de la información y las comunicaciones (TIC) y, en particular, el uso de Internet nos han facilitado mucho la vida, pero debemos ser muy prudentes con el uso de la información que depositamos en la red, puesto que si no adoptamos las medidas de seguridad apropiadas, seremos vulnerables, y podremos ser atacadospor los ciberdelincuentes.Los ciberdelincuentes, que son conocedores de esta situación de vulnerabilidad,aprovechan la falta de concienciación o de conocimiento en ciberseguridad de la población para tratar de descubrir nuevas vías de acceso a nuestros dispositivos ymaterializar sus ataques. Solo si sabemos actuar frente a estas amenazas, podremos estar más seguros y protegidos.Un aspecto que adquiere especial relevancia en el ámbito de la ciberseguridad son las estafas, ya que suponen aproximadamente el 90 % de los delitos informáticos que se cometen en la actualidad. También existen otros delitos informáticos, como las injurias y las calumnias, las amenazas, el acoso o, incluso, la distribución de pornografía infantil, que utilizan las TIC como elemento facilitador de su comisión.En el caso de sufrir un delito debemos DENUNCIAR.

¿Cómo podemos denunciar?

Informar: si observas la comisión de alguna acción irregular que pudiera ser sospechosa de una infracción administrativa o penal.

colabora@guardiacivil.org

Denunciar: si deseas presentar una denuncia formal, teniendo la posibilidad de certificar los contenidos que deseas adjuntar a la misma, puedes hacerlo de forma presencial en los diferentes puestos de la Guardia Civil o través de la página web oficial.

Creación de los equipos @

La Guardia Civil ha creado los Equipos @. Estos equipos se encargan de asesorar, de prevenir y de proporcionar una respuesta ante la ciberdelincuencia, en particular, ante las estafas en la red, que, como se ha dicho, constituyen uno de los principales problemas en este ámbito. Se encuentran en todas las provincias, y una de sus funciones es asesorar y proporcionar atención presencial y a distancia a los ciudadanos y empresas, por lo que se puede acudir a ellos ante cualquier duda o cuestión.

PDF del tríptico informativo con información sobre cultura de la Ciberseguridad

Decálogo de ciberseguridad

Utilicemos contraseñas seguras y distintas

Aunque en muchas páginas ya es requisito, hay que procurar tener contraseñas lo suficiente robustas para que no puedan ser descubiertas por terceros. Hay que huir de nombre de familiares, mascotas, fechas de nacimiento o nº de DNI. Una buena solución es la combinación de letras, números y caracteres especiales. Pero no solo es importante la robustez de la contraseña. Es tan importante o más el usar una contraseña distinta para cada aplicación o servicio que nos lo requiera. Efectivamente cada vez estamos suscritos a más servicios y es imposible acordarse de todas las contraseñas. Quizá la solución intermedia es tener 3 o 4 contraseñas, con distinto nivel de seguridad y para escenarios bien diferenciados. Una para los servicios de la empresa o trabajo, otra para mis cuentas de correo y redes sociales, otra para los sistemas de pago o banca electrónica, y otra para los múltiples servicios no esenciales a los que nos suscribimos.

Utiliza software legal y desconfia del gratis total en internet

La piratería del software, música, cine y literatura tiene muy poco rechazo moral en el mundo digital. Bajo la bandera del acceso libre a la cultura, se enmascara la vulneración de los derechos de propiedad intelectual. Por desgracia es demasiado habitual utilizar programas, escuchar música, ver cine o leer libros descargados de portales que, por otro lado, obtienen beneficios por la vía de la publicidad. Y esta debilidad de los internautas la aprovechan los ciberdelincuentes para enmascarar malware en los contenidos pirateados, al igual que lo hacen con las aplicaciones que sirven para vulnerar la seguridad de los programas frente a la piratería, es decir, los típicos programas generadores de claves. Por otro lado, hay que ser muy cauteloso con los contenidos de acceso libre bajo la bandera de gratis total. Bajo la apariencia de programas totalmente gratuitos se esconden aplicaciones maliciosas que buscan robarte los datos personales o económicos, o bombardearte a

propaganda para la adquisición de determinados productos. Nadie regala nada sin esperar algo a cambio en el mundo real. Pensemos que Internet es igual, y si alguien diseña un portal que logos, tonos o lo que sea, busca un beneficio, que en ocasiones está en la información de los clientes.

Mantener actualizado el software de nuestros equipos, ya sean PCs de sobremesa, portatiles, tablets o smartphones

Es necesario mantener actualizados a su última versión tanto el sistema operativo como los programas y aplicaciones instalados. Periódicamente se detectan errores de programación o diseño que suponen una vulnerabilidad para la seguridad de nuestros equipos. Las empresas, en cuanto se detectan, se ponen manos a la obra para subsanar los errores, publicando parches de actualización del sistema. Y los ciberdelincuentes desarrollan aplicaciones de malware para explotar las vulnerabilidades. Cuanto antes actualicemos nuestros equipos, menos tiempo estaremos expuestos a los ataques de los ciberdelincuentes.

Protege tus datos personales

Cualquier dato personal tiene valor en Internet. Todo se compra y se vende. Filiación, datos bancarios, médicos… No caigamos en el error de creer que nosotros no somos importantes y que nuestros datos no sirven para nada. Yo no soy nadie y no tengo ahorros en el banco. Esto nos lleva a relajarnos y a confiarnos. Y nuestra información tiene valor. Con nuestros datos suplantan nuestra identidad para engañar y estafar a un tercero, con nuestros datos pueden solicitar un crédito personal, y con nuestros datos pueden acceder a nuestro círculo de amistades o compañeros laborales. Por eso debemos ser extremadamente celosos de nuestra información personal. Dudemos de todo aquel que nos solicita datos personales. Si tenemos la más mínima duda, antes de ceder nuestros datos, busquemos en la red. La propia internet es nuestra mejor aliada.

No te creas todo lo que se dice por Internet

Con la explosión de la web 2.0, en que los usuarios somos los protagonistas de la red, los que subimos contenidos, el mundo de la información ha dado un vuelco. Antes, nuestra referencia estaba en la prensa escrita, la radio y la televisión. La información tenía un respaldo y una confiabilidad, un medio concreto y un periodista, una emisora y un locutor, una cadena y un presentador. Ahora, cualquier de nosotros, con un smartphone y su cámara, es capaz de informar sobre cualquier hecho, notica, o lo que es peor, darnos su opinión, aunque no tenga información contrastada. Ello nos lleva a un escenario de muchísima información, a la infoxicación de noticias y opiniones que no tienen el respaldo de profesionales de la información. Nos llega mucha información sin contrastar, opiniones, noticias sesgadas, que nos hacen víctimas de la manipulación informativa. Por ello, es necesario un espíritu crítico con los contenidos de internet. Dudar por sistema e intentar contrastar las noticias es la mejor herramienta frente a la desinformación.

PDF del decálogo de ciberseguridad

Medidas de concienciación con dispositivos móviles

- **Desactivar** las funciones de geoposicionamiento siempre que sea posible.
- **Deshabilitar** la sincronización del dispositivo con la nube.
- **Utilizar** en la medida de lo posible conexiones de 3G, 4G o 5G en lugar de wifi.
- **Diferenciar** las contraseñas personales y las profesionales.
- **No compartirlas** nunca.
- **Establecer** una clave de acceso en el dispositivo móvil y activar la opción de bloqueo automático.
- **Utilizar** contraseñas seguras y cambiarlas de manera periódica.
- **Utilizar** sólo programas oficiales y aplicaciones legítimas.
- **Un dispositivo móvil se puede perder**, puede ser robado, roto o destruido. Más vale prevenir.
- **Mantener** siempre el dispositivo móvil actualizado y en perfectas condiciones.
- **Utilizar** sólo programas oficiales y aplicaciones legítimas.
- **Desconfiar** y evitar de las redes wifi gratuitas y públicas.

Para recordar

- **La información que se contiene en los dispositivos móviles es muy valiosa**, por lo tanto hay que velar por su protección. Y sino es necesario, no descargues nada que contenga información sensible a tu terminal.
- **El dispositivo móvil,** al transportarse, puede perderse o ser robado, además de averiarse o destruirse, por eso es necesario tener todas estas opciones previstas para evitar situaciones de peligro.
- Aplica **medidas adecuadas** para evitar accesos no autorizados al dispositivo móvil y evitar asi el visionado de la información contenida en el mismo.
- **Cifrar** el dispositivo móvil.
- **Evitar el uso de redes wifi públicas** o desconocidas, sobre todo cuando tratemos con información sensible.

- Si se utiliza **BYOD (Bring Own Your Device)**, que es traer tu propio dispositivo móvil pero para el uso corporativo, hay que configurarlo de manera adecuada, con el apoyo del servicio de informática.

PDF de las medidas de concienciación con dispositivos móviles

Guías de Ciberseguridad para niños y adolescentes

El Plan Estratégico contra la Cibercriminalidad recogido en la Instrucción 1/2021, de la Secretaria de Estado de Seguridad, tiene como uno de sus objetivos "promover la cultura de prevención de la cibercriminalidad entre la ciudadanía y la empresa", a este mismo objetivo se le da continuidad en el Plan de Acción Contra la Cibercriminalidad (PAC3) de la Guardia Civil, específicamente en su acción nº4 "Divulgación de la Cultura de Ciberseguridad".

Por ello, la Unidad de Coordinación de Ciberseguridad (UCCiber) ha elaborado material informativo sobre la Cultura de Ciberseguridad para su difusión entre el público infantil y adolescente que demande este tipo de conocimiento. Con ello se pretende conseguir que ese material sirva como refuerzo en la formación impartida por la Guardia Civil en los colegios e institutos de su demarcación.

Material

- Guía de Ciberseguridad (desde los más pequeños hasta los 12 años)
- Guía de Ciberseguridad (desde los 12 hasta los 18 años).

Las guías en papel se están distribuyendo por todas las Comandancias del Cuerpo.