GUARDIA CIVIL

CULTURA *de la* CIBERSEGURIDAD

DECÁLOGO DE CIBERSEGURIDAD

1 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.

2 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.

3 MANTENER ACTUALIZADO EL SOFTWARE DE NUESTROS EQUIPOS, YA SEAN PC,S 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.

4 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.

5 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 contratar, 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.

UNIDAD DE COORDINACIÓN DE CIBERSEGURIDAD

ALERTCOPS

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

EDITA: SECRETARÍA GENERAL TÉCNICA DEL MINISTERIO DEL INTERIOR
CATÁLOGO DE PUBLICACIONES DE LA ADMINISTRACIÓN GENERAL DEL ESTADO
https://cpage.mpr.gob.es
REALIZADO POR LA UNIDAD DE COORDINACIÓN DE CIBERSEGURIDAD
IMPRIME: ARTES GRAFICAS COYVE, S.L.

FSC MIXTO Papel FSC® C077825

NIPO (ED. PAPEL): 126-21-114-X
NIPO (ED. EN LÍNEA): 126-21-115-5
DEPÓSITO LEGAL: M-29553-2021

DIRECCIÓN GENERAL DE LA GUARDIA CIVIL
Oficina de Información y Atención al Ciudadano
C/ Guzmán El Bueno 110 - 28003 Madrid
www.guardiacivil.es