

10 CONSEJOS DE SEGURIDAD PARA **USUARIOS DIGITALES**

CONSEJO # 1

Cambiar las contraseñas de manera periódica y no usar la misma en más de un lugar. Deben tener una cierta longitud (más de 8 caracteres) y contener información alfanumérica (dígitos, letras y caracteres especiales). Hay que evitar basarse en información personal (DNI, nombres de amigos, conocidos, familiares, mascotas, etc.) o utilizar patrones muy sencillos (12345).

CONSEJO # 2

Realizar las compras en línea a proveedores con prestigio social consultando experiencias de clientes anteriores. Los sitios web tienen que ser seguros (usar el protocolo <https://>) y estar vinculados a pasarelas de pago electrónico reconocidas (como Visa, Mastercard, Paypal, entre otras). A su vez, hay que hacer un seguimiento de nuestra cuenta corriente para comprobar los cargos de las tarjetas, o incluso avisar al banco para que compruebe nuestra cuenta o nos informe ante determinados cargos.

CONSEJO # 3

Evitar abrir correos electrónicos que no van a nuestra atención, especialmente si incorporan adjuntos, y huir de todos aquellos que aunque van dirigidos directamente a nosotros nos redireccionan a páginas para corregir nuestros datos personales o de servicios diversos especialmente los bancarios o administrativos.

CONSEJO # 4

En los móviles está nuestra vida entera (comunicaciones sociales, contraseñas, acceso bancario o a servicios, entre otros). Hay que proteger bien, con palabras de paso o patrones, el acceso indebido a esta información. Cuando estemos sin el dispositivo por un periodo largo (por ejemplo, préstamo a terceros o reparación en servicio técnico), es adecuado restaurarlo a los valores de fábrica (tanto de software como de datos). Igualmente, debemos acostumbrarnos a hacer copias de seguridad de nuestro dispositivo periódicamente para minimizar la pérdida de datos.

CONSEJO # 5

En el acceso a redes, especialmente de líneas Wi-Fi abiertas o compartidas, hay que minimizar o evitar todo uso de servicios que conlleven la identificación personal o el acceso a información personal. Si no se dispone de mecanismos de cifrado ni redes privadas virtuales (VPN), hay que evitar usar estas redes abiertas salvo que sea una simple navegación sin acceso a datos personales.

CONSEJO # 6

Proteger las redes de casa. Los routers ADSL + Wi-Fi modernos son compatibles con diferentes niveles de seguridad: es recomendable cambiar las contraseñas por defecto del aparato y de sus servicios, y elevar el nivel de seguridad Wi-Fi (a protocolos WPA o WPA2, por ejemplo). En caso de incidencias o bajadas de rendimiento inexplicables, hay que controlar los dispositivos conectados a nuestra red para detectar intrusiones, así como cambiar las contraseñas y elevar los niveles de seguridad.

CONSEJO # 7

Vigilar también la seguridad en aparatos que se han incorporado últimamente a internet: televisores, videoconsolas, aparatos de reproducción en tiempo real (streaming) de vídeo o audio. En ese caso, hay que consultar a los fabricantes y realizar las actualizaciones necesarias.

CONSEJO # 8

Actualizar el software básico del ordenador, el teléfono móvil o la tableta, disponer de las últimas versiones de las actualizaciones del sistema operativo y paquetes tipo Office y de software de uso general como navegadores y sus complementos (plugins), lectores de archivos en formato PDF (por ejemplo, Acrobat), Java. En general, todos los programas que sean de un uso habitual, aunque sea indirecto y no seamos tan conscientes de ello (lectores de archivos PDF, Java, Flash Player, etc.), deben de estar actualizados.

CONSEJO # 9

Deshabilitar los complementos no deseados de los navegadores. Los navegadores suelen quedar llenos de buscadores o de utilidades especiales que, en algunos casos, recopilan nuestros datos de navegación o sencillamente pueden ser vías para introducir virus o software malicioso (malware) en nuestro ordenador. Todos los navegadores incluyen, en las opciones, controles para los complementos (plugins) instalados que permiten desinstalar o deshabilitar los complementos dudosos. Hay que vigilar porque algunos complementos se instalan como programas y pueden ser difíciles de encontrar. Por tanto, los tendremos que desinstalar.

CONSEJO # 10

Para favorecer la navegación y las búsquedas privadas se aconseja, entre otros:

- 1) activar los modos privados de los navegadores;
- 2) pedir a los buscadores principales (Google y similares) que borren nuestros datos (en Google se puede hacer mediante el panel de control);
- 3) avisar a las páginas visitadas de que no queremos ser rastreados (los navegadores incluyen opciones Do not track);
- 4) borrar y controlar el uso de las galletas en el navegador para que no se

recuerden nuestras visitas ni nuestra actividad en los sitios web que hemos visitado.