Plataforma de
Aprendizaje Virtual

Conceptos Fundamentales sobre Ciberseguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 4

Consejos de seguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 4

Consejos de seguridad

Este manual se realizó con la colaboración de la Dirección Nacional de Ciberseguridad, perteneciente a la Subsecretaría de Tecnologías de la Información de la Nación.

Seguridad en la navegación por Internet

Una de las herramientas más utilizadas en Internet son los llamados navegadores web: programas que nos permiten acceder a los distintos sitios alojados en la Web. Gracias al navegador, podemos explorar los textos, imágenes y videos que se encuentran en las páginas web y "navegar" por ellas a través de los enlaces que las conectan. Algunos de los navegadores más conocidos son Google Chrome, Microsoft Edge, Mozilla, Firefox, Safari y Opera, aunque existen muchos otros.

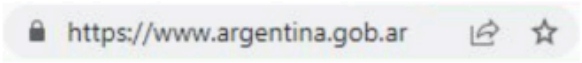
Muchas veces suele pensarse que Internet y la web son la misma cosa, pero no lo son. Como vimos en la Unidad 1, Internet es una red de computadoras conectadas entre sí, que surgió a mediados de los años '60. La web, en cambio, fue creada en 1989 por el físico inglés Tim Berners-Lee, y se trata de una inmensa colección de páginas web que funcionan a través de la conexión de internet. Podríamos pensar que la web es más parecida a una biblioteca llena de libros (o páginas web), mientras que Internet es la ciudad en la que se encuentran esas bibliotecas.

Sin embargo, a pesar de todas las posibilidades que nos abre el mundo de Internet, también vimos que existen amenazas de las que debemos protegernos. A la hora de navegarla, es importante tener en cuenta una serie de recomendaciones para hacerlo de modo seguro:

- Descargar e instalar programas de sitios oficiales.
- No abras correos electrónicos de personas desconocidas.
- No hacer click en fotos ni archivos adjuntos que aparezcan en correos electrónicos de personas desconocidas, aún cuando despierten mucho interés (como noticias de último momento, premios, beneficios, etc). Algunos de estos ataques pueden ser dirigidos a una persona específica, a sabiendas de sus intereses, por lo que es necesario no confiarse.
- No acceder a sitios webs desconocidos, ni hacer clic en enlaces dudosos o en ventanas emergentes, por más tentadoras que puedan parecer ya que pueden contener malware o ser enlaces hacia webs fraudulentas.
- Tener siempre instalado un antivirus en los dispositivos.
- Tener actualizadas las versiones del sistema operativo, del navegador web y del antivirus. De no hacerlo, es más probable que los ciberatacantes puedan vulnerar los dispositivos.
- Si vas a usar un dispositivo público o de uso común, utilizar el modo incógnito de navegación, para que no queden guardados los datos y contraseñas ni el historial

de sitios visitados. La opción de modo incógnito suele encontrarse en la barra de menú o de configuración de los navegadores web.

- Asegurate de estar navegando en un sitio seguro. Para eso, chequeá que aparezcan las letras “https” antes del nombre del sitio al que estás accediendo (muchas veces, tenés que hacer doble click sobre la barra de navegación para ver estas siglas). Además, debés constatar que en la barra de navegación aparezca un candado cerrado que indica que el sitio está certificado (es decir, que el sitio pertenece a la organización de la que dice ser) y es seguro. Cada navegador puede presentarlo con aspectos diferentes, pero te mostramos un ejemplo:



- Cuando el sitio no es seguro, en la barra de navegación aparecerá la frase “sitio no seguro” (o “not secure”) antes de la dirección web, o la misma dirección puede aparecer tachada. En cualquiera de los dos casos, nunca debés ingresar tus datos, descargar archivos ni acceder a enlaces de estas páginas, ya que podrías poner en peligro tu información personal, o dañar tus dispositivos. Lo ideal es abandonar el sitio web.

Protección de la información personal y dispositivos

Además de las medidas de seguridad que podemos tomar a la hora de navegar en la web, también debemos tener en cuenta otra serie de recomendaciones para proteger la información personal. En la unidad 2, vimos que muchos de los ciberataques se apoyan en fallas del “eslabón más débil”; es decir, en fallas humanas. Por eso, es imprescindible prestar mucha atención a la hora de exponer datos personales, así como tener especial cuidado en el resguardo de contraseñas. A continuación, compartimos algunas de las recomendaciones para preservar y proteger la información personal:

- Realizar periódicamente copias de seguridad de la información de los dispositivos. Descargar periódicamente las fotos y los documentos almacenados, para poder recuperar ese material en caso de que el dispositivo sea robado o perdido.
- Configurar el bloqueo automático del equipo tras un periodo de inactividad, que se sugiere sea breve. El desbloqueo debe

realizarse mediante un patrón de desbloqueo, contraseña o huella digital (este último es el mecanismo más confiable).

- Descargar programas y aplicaciones de sitios y tiendas de apps oficiales.
- No ingresar datos personales en sitios desconocidos.
- Leer los permisos que damos a la hora de instalar aplicaciones.
- Leer los términos y condiciones de uso de redes sociales, programas y aplicaciones. Los términos y condiciones establecen lo que esa aplicación o programa hará con tu información personal y con los datos que generes al utilizar sus servicios, así como qué medidas de seguridad tendrán con ellos, con quiénes pueden ser compartidos, cuáles son las responsabilidades de la empresa, etc. Es importante prestar atención a la letra chica y no aceptar nada sin leerlo previamente.
- No guardar contraseñas en lugares públicos, ni dejarlas escritas en archivos o papeles de fácil alcance.
- Crear contraseñas seguras, y cambiarlas periódicamente (cada 1 o 2 meses), según la criticidad de la información a proteger. Más adelante, veremos algunos consejos para generar contraseñas seguras.
- Nunca dejar desatendidos nuestros dispositivos y utilizar medidas de bloqueo de pantalla, tales como patrones, PIN, huella digital o contraseñas.

¿Cómo crear contraseñas seguras?

Una contraseña es una combinación de números, letras y símbolos, creada para proteger la información y los datos personales que tenés almacenados en tus dispositivos. Para que estas sean seguras y efectivas, deben ser difíciles de adivinar para terceros, pero fáciles de recordar para vos.

A continuación, te compartimos algunas recomendaciones tanto para crearlas como para protegerlas:

- Que tenga 8 caracteres como mínimo y que combine letras (mayúsculas y minúsculas), símbolos y números. Cuanta más cantidad y variedad de caracteres, más segura será.
- Evitá contraseñas que sean simples o que sean fáciles de adivinar. Por ejemplo, no incluyas tu nombre, apellido, número de DNI o teléfono, ni secuencias de números como 12345678.
- Podés armar combinaciones con iniciales o partes de palabras que te sean familiares. Por ejemplo: MG7rojo! (y lo recordás porque significa: MateGato7rojo!).
- No uses la misma clave para todas tus cuentas, ya que si consiguen averiguar una, podrán acceder a todas las cuentas en la que la hayas usado.
- No habilites la opción de “recordar contraseñas” en los programas que utilices ni en el navegador web, ya que si alguien tiene acceso a tu dispositivo podrá acceder a las cuentas fácilmente.
- No guardes contraseñas en lugares públicos, ni las dejes escritas en archivos o papeles de fácil alcance.
- Cuidá que no te vean cuando tipeas tu clave (ya sea en la computadora, el celular o en el cajero automático), así como tampoco debés observar a otros mientras lo hacen.
- No envíes la contraseña por correo electrónico ni por chat o WhatsApp, así como tampoco debés mencionarla en una conversación, por más que la otra persona sea de tu confianza.
- Cambiar las contraseñas cada cierto tiempo.
- No la compartas con nadie por más confianza o autoridad que tenga.

¿Qué hacer en caso de ser víctima de un ciberdelito?

A lo largo de este curso vimos algunos tipos de ciberataques y distintas estrategias de prevención, para evitar que nuestra información personal sea vulnerada. Sin embargo, es importante seguir una serie de recomendaciones en caso de ser víctima de uno de estos ataques. A continuación te sugerimos algunas:

En caso de ser víctima de un ciberdelito, lo mejor que podés hacer es denunciarlo. En Argentina existen diferentes alternativas para presentar la denuncia o solicitar asesoramiento:

- Dirección Nacional de Protección de Datos Personales: para denunciar delitos relacionados con la privacidad o la protección de datos personales.
- Unidad Fiscal Especializada en Ciberdelincuencia - (UFECI): para denunciar delitos informáticos.
- Fiscalía de CABA. Equipo Especializado en Delitos Informáticos: para denunciar delitos informáticos en la Ciudad de Buenos Aires.

Guardá los chats, correos electrónicos, imágenes y el historial de los dispositivos, ya que cualquier tipo de evidencia digital te servirá como prueba para tu denuncia.

¡Terminaste el curso de Conceptos Fundamentales de Ciberseguridad! Esperamos que hayas disfrutado este recorrido, te esperamos en próximos cursos.

Plataforma de
Aprendizaje Virtual

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología