Folleto del alumno sobre conceptos básicos de ciberseguridad

La ciberseguridad tiene que ver con la seguridad de la información (nuestra identidad, nuestros datos personales y nuestros activos financieros) cuando estamos en línea.

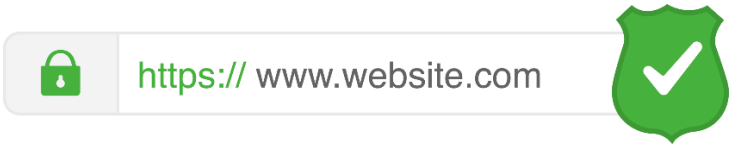
La ciberseguridad significa que 1) sus datos personales son accesibles solo para usted u otras personas que usted autorice, y 2) sus dispositivos (computadoras portátiles, computadoras de escritorio, teléfonos móviles, tabletas) funcionan correctamente y no tienen malware.

Sitios web seguros

Si va a ingresar información personal en un sitio web, asegúrese de que el sitio web sea seguro para proteger su información.

Hay dos cosas que debe buscar cuando visita un sitio web:

1) un ícono de candado junto a la barra de direcciones
2) una dirección de sitio web que comience con HTTPS



Consejos para crear contraseñas seguras

- Evite las palabras comunes, como "contraseña" o "123456".
- No incluya palabras comunes o información personal, como su dirección o su nombre.
- No use la misma contraseña en varios sitios web o cuentas.
- No comparta su contraseña con otros. Las contraseñas deben mantenerse privadas.
- Haga la contraseña más larga. La mejor defensa es la longitud. Las contraseñas largas no necesitan ser complejas y difíciles de recordar.
- Use frases cortas, como "vacasayudanahacerqueso".

Consejos para reconocer fraudes y estafas en línea

- ¿Ha escuchado hablar antes de la persona u organización?
- ¿Sabe de quién es el mensaje de correo electrónico?
- ¿Tiene errores el correo electrónico?
- ¿Le están solicitando su información?
- ¿Están intentando apresurarlo a tomar una acción rápida?

- ¿Es demasiado bueno para ser verdad?

Lo que se debe hacer y no hacer para evitar estafas

Lo que se debe evitar

- **Proporcionar información personal** a algo que podría ser una estafa. Esto incluye el nombre, la dirección de correo electrónico, el número de tarjeta de crédito o la contraseña.
- **Responder o comunicarse con el impostor.** Esto puede notificarle al estafador que se ha comunicado con una persona real, lo que puede dar lugar a más correos electrónicos fraudulentos.
- **Hacer clic en enlaces o botones.** Hacer esto puede llevarlo a sitios web no confiables.
- **Descargar cualquier archivo o documento adjunto.** Pueden contener virus o malware que dañan su computadora o que recolectan su información personal.

Lo que se debe hacer

- **Ser escéptico.** Si cree que algo es una estafa, probablemente lo es**.**
- **Leer los correos electrónicos con atención.** Recuerde leer atentamente los correos electrónicos y los mensajes de texto, asegurándose de que conoce al remitente. Aplique los otros consejos que presentamos para determinar si algo es una estafa.
- **Buscar información por su cuenta**. Busque por sí mismo la información de contacto, la información sobre una empresa o la información de su cuenta. Vaya directamente al sitio web de la empresa o a la información de su propia cuenta para verificar. No visite ningún sitio web a través del correo electrónico fraudulento que le enviaron.

Para obtener más información

Visite digitalliteracy.att.com para obtener más cursos y para ayudar a desarrollar habilidades y confianza en el uso de la tecnología.

La capacitación de hoy la ofrecen AT&T y la Asociación de Bibliotecas Públicas.