



Cómo mantenerse seguro en línea:

Consejos para evitar caer en manos de ciberdelincuentes

No importa si eres un joven que está comenzando a navegar el mundo digital, un adulto que realiza transacciones financieras en línea, o un adulto mayor que se comunica con sus amigos y familiares a través de las redes sociales.

Cuando usamos Internet, siempre debemos tomar algunas precauciones básicas para proteger nuestra seguridad personal y financiera. Así como cerramos la puerta con seguro y activamos la alarma al salir de casa, o subimos las ventanas y activamos los seguros del vehículo al estacionar, debemos ser igualmente cuidadosos en línea.

En esta guía encontrará conceptos básicos de seguridad y consejos prácticos que le ayudarán a disfrutar de los beneficios del Internet con tranquilidad.

Conceptos importantes

Cuando se trata de seguridad en línea, asegúrese de conocer los siguientes términos y conceptos.

Glosario

Autenticación

Método utilizado para corroborar su identidad, como una contraseña, huella digital, o autenticación de dos factores (2FA), que puede requerir un código ingresado en su teléfono móvil como un paso adicional.

Autorización

Proceso mediante el cual, una vez confirmada su identidad, el sistema determina el nivel de acceso permitido. Por ejemplo, permitirle ver un archivo sin permitir su edición.

Cifrado

Proceso que protege sus datos codificándolos para que solo las personas autorizadas puedan leerlos.

Hackear

Intentar obtener acceso a la información de una computadora mediante medios ilícitos.

Firewall

Filtros especiales que bloquean archivos y usuarios no autorizados para acceder a computadoras y redes. Eliminan el tráfico sospechoso y evitan que personas externas accedan a datos privados.

Malware y virus

El malware es cualquier software diseñado para causar daño intencional a una computadora, servidor o red. Un virus es un tipo de malware que puede copiarse a sí mismo y propagarse a otros dispositivos. Ambos pueden dañar su sistema, robar, cifrar o eliminar sus datos. El software antivirus/malware protege sus dispositivos.

Ransomware

Tipo específico de malware que bloquea el acceso a un sistema informático y trata de extorsionar al usuario solicitando un pago para restaurar el acceso.







Ingeniería social

Cualquier estafa que engaña a los usuarios para revelar información secreta como contraseñas o números de cuentas bancarias.

Redes Privadas Virtuales (VPNs)

Las VPNs le permiten crear una conexión segura a través del internet. Ocultan su dirección IP, cifran sus datos antes de enviarlos y ayudan a proteger su identidad en línea. Puede adquirir servicios VPN de varios proveedores, incluyendo a NordVPN, Surfshark, Private Internet Access y ExpressVPN, entre otros.

CONSEJOS y CONTRAINDICACIONES

PROCURE HACER	INTENTE EVITAR
<p> Use contraseñas seguras: Cree contraseñas largas y complejas, que incluyan una mezcla de letras mayúsculas y minúsculas, números y símbolos.</p>	<p> No sea obvio: Evite contraseñas fáciles de adivinar como “contraseña,” nombres de miembros de su familia o fechas de nacimiento.</p>
<p> Mantenga cada cuenta única: Use una contraseña distinta para cada cuenta.</p>	<p> No use la misma contraseña para múltiples cuentas: Una filtración de datos no debería comprometer todas tus cuentas.</p>
<p> Use un gestor de contraseñas: Como un llavero, un gestor de contraseñas le ayuda a mantener todas sus contraseñas en un solo lugar, para que no tenga que recordarlas. Así mismo crea y almacena contraseñas complejas por usted. Existen varios gestores de contraseñas en el mercado, como 1Password, NordPass, RoboForm y Keeper.</p>	<p> No anote sus contraseñas: Especialmente no las deje donde otros puedan encontrarlas.</p>
<p> Cámbielas frecuentemente: Cambie sus contraseñas de manera regular para mayor seguridad.</p>	<p> No comparta contraseñas: Manténgalas privadas. No las comparta con nadie.</p>
<p> Habilite la autenticación de dos factores: Agregue una capa adicional de seguridad a sus cuentas para que, si alguna vez su contraseña se ve comprometida, los criminales tengan mayor dificultad para acceder a su información y usted pueda recuperar el control más rápido.</p>	

10 contraseñas comúnmente utilizadas (Ojo: estas son demasiado fáciles de adivinar):

- | | | |
|---------------|------------|--------------------|
| 1. 123456789 | 5. 111111 | 8. tequiero |
| 2. contraseña | 6. querida | 9. NombreApellido1 |
| 3. admin | 7. qwerty | 10. root |
| 4. abc123 | | |

El 80% de las fugas de datos son causadas por contraseñas que se pierden, son robadas o se adivinan mediante un “ataque de fuerza bruta,” en el cual las computadoras prueban varias combinaciones de palabras comunes y contraseñas frecuentemente usadas hasta encontrar una coincidencia.

Expediciones de pesca (phishing)

El phishing (un juego con la palabra inglesa “fishing” – pesca) es un tipo de fraude en línea donde los criminales intentan engañarle para que les proporcione su información personal, como contraseñas, números de cuentas bancarias o detalles de tarjetas de crédito usando ingeniería social. Lo hacen enviándole correos electrónicos, mensajes de texto o sitios web falsos que parecen provenir de organizaciones legítimas como su banco, su empleador o una agencia gubernamental. Si usted hace clic en un enlace o abre un archivo adjunto a esos mensajes, podría descargar un malware que puede dañar su computadora o robar sus datos. Aquí hay algunos consejos para evitarlo:

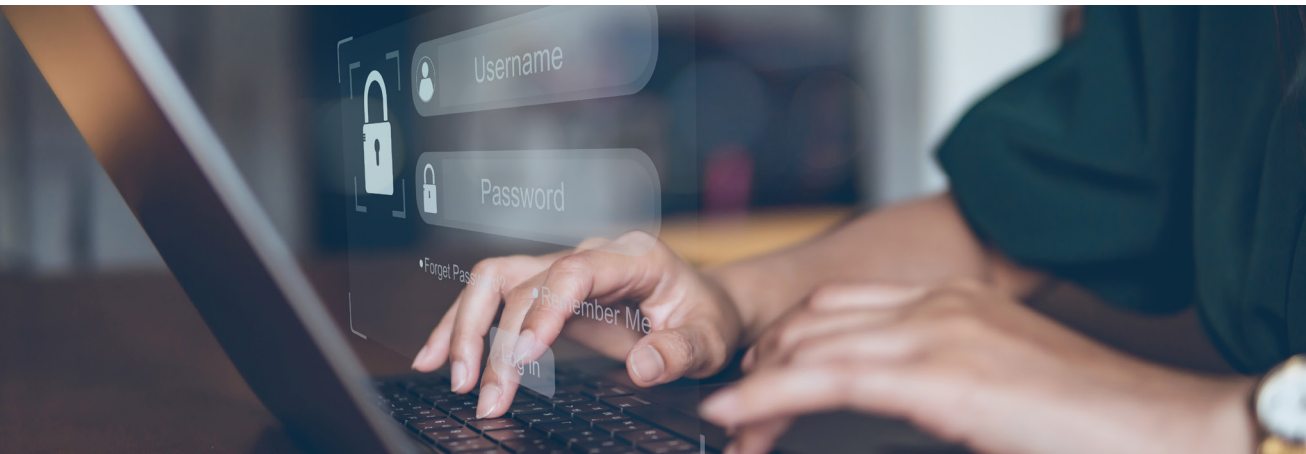
Verifique el remitente: Siempre compruebe que la dirección de correo electrónico del remitente sea del sitio web oficial de la organización que dice representar. Si la dirección de correo no coincide, o si contiene letras o números aleatorios, es probable que sea un intento de phishing.

Corrobore el contenido: Busque errores de ortografía y gramática, lenguaje vago o urgente, o solicitudes de información personal o financiera. Todos estos ejemplos son señales de phishing. No responda a estos mensajes ni haga clic en ningún enlace o archivo adjunto. Si no está seguro de que un mensaje es legítimo, contacte a la organización directamente usando un canal diferente, como el teléfono o un navegador web.

Use un software de seguridad: Instale y actualice software antivirus y anti-malware en su computadora y dispositivos móviles. Estos programas pueden ayudar a detectar y bloquear sitios web y descargas maliciosas. También debería usar un firewall y cifrar su red inalámbrica para prevenir el acceso no autorizado.

No se deje presionar: Los cibercriminales suelen crear un falso sentido de urgencia para que usted cometa un error. Amenazas de cerrar su cuenta, ser bloqueado o recibir una multa pueden desorientarle y hacerle caer en la trampa.

Reporte: Si recibe un correo electrónico de phishing, además de eliminarlo, repórtelo. La mayoría de las plataformas de correo electrónico tienen una opción para reportar correos como phishing. También puede reenviarlo a spam@uce.gov, que es un servicio de la Comisión Federal de Comercio (FTC). Al reportar el phishing, ayuda a proteger a otros del fraude en línea.



9 maneras de asegurar su vida digital

- 1 Actualice regularmente los sistemas:** Mantenga su software, aplicaciones y sistema operativo actualizados. Las actualizaciones a menudo incluyen parches de seguridad que protegen contra nuevas amenazas.
- 2 Sea cauteloso con enlaces y archivos adjuntos:** No haga clic en enlaces ni descargue archivos adjuntos de fuentes desconocidas o correos electrónicos sospechosos. Podrían llevar a sitios web peligrosos o contener malware.
- 3 Use redes seguras:** Evite usar Wi-Fi públicos para realizar compras en línea o transacciones bancarias sensibles. Si debe usar Wi-Fi público, siempre utilice una VPN para asegurar su conexión.
- 4 Respalde sus datos:** Realice copias de seguridad regularmente de archivos importantes en almacenamiento externo o en la nube. Esto protege sus datos en caso de un ciberataque (o una falla en sus equipos).
- 5 Habilite configuraciones de privacidad:** Ajuste las configuraciones de privacidad en sus cuentas de redes sociales y otras cuentas en línea para limitar la información personal que comparte públicamente. Evite publicar contenido en modo “público”, a menos que quiera que todo el mundo (incluidos los cibercriminales) tengan acceso.
- 6 Asegure sus dispositivos:** Use contraseñas seguras, huellas digitales o identificación facial para bloquear sus dispositivos. Esto previene el acceso no autorizado si su dispositivo se pierde o es robado.
- 7 Nunca habilite macros:** Si una ventana de diálogo solicita realizar cambios en su computadora o le pide que haga clic en “sí” para habilitar macros, tenga mucho cuidado. Lo preferible es evitarlo a menos que esté completamente seguro de que no proviene de una fuente maliciosa.
- 8 Sea escéptico:** Sea cauteloso cuando reciba llamadas telefónicas, correos electrónicos y mensajes no solicitados, especialmente si piden información personal o dinero. Si parece demasiado bueno para ser cierto, probablemente sea falso.
- 9 Manténgase informado:** Infórmese de las últimas estafas en línea y aprenda a reconocer las señales de fraude. El sitio web de la FTC ofrece una gran cantidad de recursos:
<https://consumer.ftc.gov/identity-theft-and-online-security>

Acerca de Brightspeed

Lanzada en 2022, Brightspeed está construyendo un futuro donde un mayor número de comunidades puede beneficiarse de una vida más conectada. Creemos que el lugar donde una persona elige vivir no debería estar limitado por sus opciones de conexión, y por ello estamos construyendo la infraestructura necesaria para ofrecer Fibra Óptica rápida y confiable, y así llegar a millones de hogares y empresas. Brightspeed Fiber Internet, brinda una experiencia ininterrumpida para ver videos, estudiar, jugar en línea o trabajar. Si desea conocer más información ingrese a: www.brightspeed.com.

In collaboration with

ciena