Seguridad en Internet

¿Por qué es importante la ciberseguridad?

Internet y las redes sociales son plataformas asombrosas que nos ayudan a compartir información y a mantenernos en contacto con amigos y familiares.

Sin embargo, los delincuentes y otras organizaciones ilícitas también las utilizan para obtener dinero o información de la gente, o para intimidarla.

Pueden actuar desde cualquier lugar del mundo, hablar la mayoría de los idiomas con fluidez y crear sitios web falsos y convincentes. Se ponen en contacto con las personas a través del correo electrónico, las redes sociales y los mensajes de texto, e intentan asustarlas o angustiarlas para que no piensen con claridad.

Todo ello significa que hay que prepararse y estar siempre al tanto de las artimañas que utilizan.

¿Cuáles son los problemas más comunes que se pueden encontrar en Internet?

Las siguientes son algunas de las situaciones más comunes que se presentan:

- Usted recibe un correo electrónico o mensaje de texto sospechoso en el que se le pide que haga clic en un enlace.
    - Esos enlaces a menudo conducen a sitios web falsos que están diseñados para robar sus datos financieros o de inicio de sesión.
- Usted recibe una llamada sospechosa en la que le piden información personal.
    - Como en el caso anterior, la persona que llama puede fingir que es de su banco y pedirle información.
- Usted recibe un mensaje de alguien que se hace pasar por una persona que tiene autoridad y pretende que usted haga algo.
    - Con frecuencia la persona hace algún tipo de amenaza.
- Alguien accede a una o varias de sus cuentas en línea (por ejemplo, las del correo electrónico o las redes sociales).
    - Si alguien accede a su cuenta en línea, podría robar información, redirigir pagos y comunicarse con sus amigos o familiares haciéndose pasar por usted.
- Le roban los datos de su tarjeta de crédito o lo estafan para sacarle dinero con una venta o inversión falsas.
    - Los estafadores esperan que usted vea una buena oferta y pague sin pensar. O puede que se vulnere la seguridad de un sitio web real y que sus datos se filtren en Internet.

Aquí podrá encontrar más ejemplos:
Obtener ayuda ahora - Own Your Online

¿Cómo puede una persona preservar su seguridad en Internet?

- Crear contraseñas largas y no repetirlas
    - Cuanto más larga sea una contraseña, más segura será.
    - Cree una contraseña fácil de recordar de más de 16 caracteres uniendo cuatro palabras al azar (por ejemplo: TriánguloPerroOperaciónZapatos) y agregando números, letras mayúsculas y símbolos, si es necesario (por ejemplo: Triángulo&"Perro"Operación2Zapatos).
    - Es importante no repetir las contraseñas. Si un delincuente obtiene una de sus contraseñas, también la probará en otras cuentas.
    - Crear contraseñas seguras - Own Your Online
- Tener activada la autenticación de dos factores
    - Se trata de un dato adicional (normalmente un código que se envía al teléfono) que se necesita para iniciar sesión en un sitio web.
    - Esta técnica es muy fuerte y puede detener la mayoría de los intentos de ingresar a sus cuentas.
    - Recomendamos utilizar una aplicación de autenticación cuando sea posible.
    - Configurar la autenticación de dos factores (2FA) - Own Your Online
- Activar la configuración de privacidad en línea
    - La mejor opción para preservar la seguridad en las redes sociales es tener la configuración de privacidad activada.
    - Esto evitará que las personas que usted no conoce, incluidos los ciberdelincuentes, puedan ver sus publicaciones o enviarle mensajes.
    - Proteger la privacidad en línea - Own Your Online
- Mantener todo actualizado
    - Al actualizar el teléfono, la computadora o el software, también se solucionan los posibles problemas de seguridad.
    - Los delincuentes siempre están buscando formas de entrar, y las actualizaciones corrigen las vulnerabilidades.
    - Mantener las actualizaciones al día - Own Your Online
- Tener cuidado siempre
    - El mejor consejo es estar al tanto de estas maneras de estafar y prestar atención por si los delincuentes intentan comunicarse con usted en cualquier plataforma en línea.
    - Si le parece que algo anda mal, no se comunique con la persona que lo contactó. Tenga especial cuidado si le piden dinero, aunque la persona parezca amigable.
    - Fíjese que no haya enlaces ni direcciones de correo electrónico extraños (por ejemplo, su banco no le enviará un correo electrónico desde una cuenta de gmail).

- En caso de duda, comuníquese directamente con la organización y no haga clic en ningún enlace ni se comunique con ningún número de teléfono que le envíen.

¿Qué hago si me estafan o si ocurre algo peor?

Hay muchas organizaciones a las que puede acudir para obtener ayuda. Ninguna de ellas compartirá sus datos con nadie, a menos que usted dé su consentimiento.

- A través del portal CERT NZ puede denunciar incidentes cibernéticos ante nosotros, el NCSC, y le brindaremos ayuda o lo pondremos en contacto con otro organismo: Denunciar un incidente | CERT NZ
- Si ha perdido dinero, debe ponerse en contacto con su banco de inmediato.
- Los mensajes de texto fraudulentos pueden reenviarse gratuitamente al 7726, un servicio gestionado por el Ministerio del Interior.