Octubre de 2022

Boletín de Bienestar y Seguridad – Prevención de los Ciberdelitos

Departamento de Servicios de Desarrollo de California

¿Este boletín es útil?

Haga clic

Prevención de los Ciberdelitos

Internet es una excelente herramienta para conectarse en línea, pero también puede ser peligrosa. De la misma forma que se prepara para salir de su casa, debe tomar precauciones antes de usar el internet para asegurarse de que usted y su información estén seguros y protegidos y no ser víctima de un ciberdelito.

Cómo mantenerse seguro en Internet

¿Qué son los ciberdelitos?

Los ciberdelitos son delitos que se cometen en Internet. Pueden consistir en el robo de la información personal o el dinero de una persona, que quizás no sepa que ha sido víctima de un delito. Por eso es importante saber cómo reconocer los ciberdelitos para prevenirlos u obtener ayuda para evitar que vuelvan a ocurrir.

Internet es un espacio público

- Otras personas pueden ver los sitios que visita y, a veces, la información que ingresa.
- La información que comparte en Internet es posible que sea visible para cualquier otra persona.

- Tenga cuidado de compartir información personal (como los números de Seguro Social, la información de sus cuentas bancarias y la información médica) en Internet cuando no sea por un motivo comercial justificado, como hacer operaciones bancarias.
- Las redes Wi-Fi de acceso público en las tiendas y restaurantes que permiten el uso gratuito siempre se deben usar con precaución.
- Aunque estas redes son convenientes, en general no son seguras. Esto significa que otras personas pueden ver o robar su información personal (como el nombre de usuario y la contraseña de su cuenta bancaria, por ejemplo).

Verifique la configuración de privacidad regularmente

- Los ajustes de privacidad le permiten elegir qué información desea compartir y quién tiene acceso a esta información.
  - En las redes sociales (como Facebook o Instagram), puede usar los ajustes de privacidad para controlar la información que comparte con otros.
- Configure los ajustes de privacidad para las diferentes aplicaciones en su teléfono celular para limitar la información que se comparte en ellas (como los permisos para compartir ubicación o datos).
- Asegúrese de que los ajustes de privacidad en sus cuentas en línea exijan el ingreso de una contraseña para acceder a sus cuentas.
  - Con la autenticación de doble factor, usted recibe un mensaje de texto, una llamada o un correo electrónico con un código especial cada vez que inicia sesión en su cuenta en línea (por ejemplo, en la cuenta de su banco o de la compañía emisora de su tarjeta de crédito). Esto ayuda a verificar que sea realmente usted quien está iniciando sesión en la cuenta.
  - Es una buena idea configurar la autenticación de doble factor para las cuentas en línea.

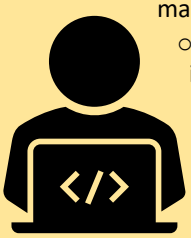
El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a las personas, a sus familias y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín

Use contraseñas seguras para las cuentas en línea

- Fortalezca su contraseña y recuerde cambiarlas con regularidad. Esto protegerá sus cuentas en línea.
- Una contraseña segura tiene al menos 8 caracteres e incluye una combinación de letras mayúsculas y minúsculas, símbolos y números. Cuanto más larga sea la contraseña, más segura será.
    - **Ejemplos de contraseñas débiles**: contraseña, SuNombre, 12345
    - **Ejemplos de contraseñas seguras**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- Evite contraseñas fáciles de adivinar, como su cumpleaños o su nombre.
- Cada una de sus cuentas debe tener su propia contraseña única.
- No mantenga una lista de contraseñas en una hoja que quede al alcance de cualquier persona, en especial, cerca de su computadora.
- Solo se deben compartir las contraseñas con personas conocidas y de su confianza, y se deben guardar en un lugar seguro.

Esté atento a los virus y al software malicioso

- El ***software malicioso*** es un tipo de software dañino para su computadora. Los ***virus*** son un tipo de software malicioso.



    - Los virus y el software malicioso ingresan al sistema de una computadora sin su permiso y la "infectan".
    - Los virus y el software malicioso pueden robar su información, ralentizar o destruir su computadora, o tomar el control absoluto de su dispositivo.
- Los virus y el software malicioso ingresan a su computadora al hacer clic en un enlace o abrir un correo electrónico infectados.
    - Tenga cuidado antes de hacer clic en un enlace que le ofrezca un premio o cualquier otro beneficio gratuito.
    - Pueden parecer enlaces a juegos, protectores de pantallas o descargas pero ser en realidad un software malicioso o un virus.

Piense antes de hacer clic

- Preste atención a los remitentes de los correos electrónicos y mensajes que recibe en línea.
    - Compruebe las direcciones de correo electrónico para ver si coinciden con la dirección que usted ya tiene guardada.

- Tenga un cuidado adicional si el remitente lo apura para obtener una respuesta inmediata o le presenta una aparente crisis, como un problema con su cuenta bancaria. En general, estos tipos de mensaje son estafas.
- El phishing es una estafa por Internet que utiliza mensajes falsos que parecen reales para engañar a las personas para que compartan su información personal.
    - Antes de responder a estos mensajes, verifique si hay algún remitente desconocido, errores de ortográficos o gramaticales, enlaces que no coinciden con el contenido del mensaje, adjuntos aleatorios y una solicitud de acción inmediata.

- No abra archivos adjuntos ni haga clic en enlaces que no reconoce. Podrían ser falsos y permitir el ingreso de virus que pueden dañar su computadora o teléfono o robarle información.
    - Cuando reciba un correo electrónico inesperado con enlaces o archivos adjuntos, siempre verifique con el remitente (por teléfono o mensaje de texto) para asegurarse que realmente proviene de ellos.
- El IRS solo envía notificaciones por correo postal de los Estados Unidos. No responda llamadas, correos electrónicos ni mensajes de texto que digan que provienen del IRS.

El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a las personas, a sus familias y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín

Sepa a quién envía un correo electrónico o un mensaje de texto

- Recuerde que es posible que los usuarios de Internet no sean quienes dicen ser.
- Nunca comparta información personal ni envíe fotografías suyas a un extraño o a alguien a quien nunca ha conocido en persona.
- Nunca envíe dinero a una persona a quién recién a conocido o a quien nunca ha visto en persona.
- Antes de ingresar su número de Seguro Social o los números de cualquier cuenta en un formulario en línea o en una página web, asegúrese de que la persona que solicita la información es realmente quien dice ser.
    - Pase el cursor sobre el enlace o el nombre del remitente para comprobar la dirección de correo electrónico y asegurarse de que su información va a ser recibida por la empresa que corresponde.

- Las personas pueden copiar logotipos y redactar correos electrónicos que parezcan y suenen reales. Por ello, revíselos con atención para detectar faltas de ortografía, contenido extraño o imágenes confusas.
- Si no está seguro de que el remitente sea real, comuníquese con la compañía o la organización de su cuenta en línea o llámelos directamente

Qué hacer si ha sido víctima de un ciberdelito

- Comuníquelo de inmediato a una persona de su confianza.
- Si el delito involucró el acceso a sus cuentas personales, llame a su banco o a la compañía emisora de su tarjeta de crédito y notifíquelo de inmediato. Deje de usar cualquiera de las tarjetas de débito o de crédito para las cuentas a las que se ha accedido.
- Cambie la contraseña para cualquier cuenta o inicio de sesión que haya sido objeto de un ataque.
- Revise sus cuentas para detectar signos de cualquier actividad inusual.

El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a las personas, a sus familias y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín