Ready HoCo
choose preparedness

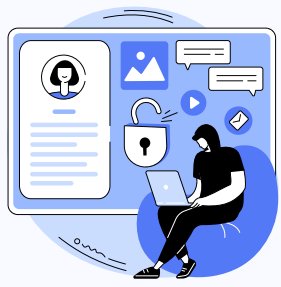
Calvin Ball
County Executive

SEGURIDAD CIBERNÉTICA

Los ataques cibernéticos son intentos maliciosos de acceder o dañar un sistema de computadoras o redes. Los ataques cibernéticos pueden ocasionar pérdidas de dinero o resultar en el robo de información personal, financiera o médica. Estos ataques pueden afectar su reputación y su seguridad.

La seguridad cibernética se trata de prevenir, detectar y responder ante los ataques cibernéticos que podrían afectar ampliamente a las personas, las organizaciones, la comunidad y la nación.

PARA EVITAR LOS RIESGOS CIBERNÉTICOS, TOME MEDIDAS CON ANTELACIÓN:



- Limite los datos personales que comparte por internet. Cambie las configuraciones de privacidad y no utilice las funciones de localización.
- Mantenga actualizados sus aplicaciones de software y sistemas operativos.
- Cree contraseñas fuertes con letras mayúsculas y minúsculas, números y caracteres especiales. Use un administrador de contraseñas y dos métodos de verificación.
- Esté atento a las actividades sospechosas en que se le indica a usted que debe hacer algo de inmediato, se le ofrece algo que parece demasiado bueno para ser verdad o se requiere su información personal. Piense antes de hacer clic. Cuando tenga dudas, NO haga clic.
- Tenga cuidado cuando comparta su información financiera personal, como el número de su cuenta bancaria, su número de Seguro Social o el número de su tarjeta de crédito. Solamente debe compartir información en páginas web seguras que comienzan con https://. No acceda a páginas web con certificados inválidos. Use una Red Privada Virtual (VPN, por sus siglas en inglés) que ofrece una conexión más segura.
- No haga clic en los enlaces en mensajes de texto o correos electrónicos de personas desconocidas. Los estafadores generan enlaces a páginas web falsas.

DURANTE UN ATAQUE CIBERNÉTICO

- Verifique que no haya cargos que no reconoce en el estado de cuenta de su tarjeta de crédito o del banco.
- Verifique en sus informes crediticios que no haya cuentas o préstamos nuevos que usted no haya abierto.
- Esté atento a correos electrónicos y usuarios en redes sociales que piden su información privada.
- Si nota alguna actividad extraña, debe cambiar de inmediato todas sus contraseñas para cuentas de internet para limitar los daños.
- Avise a los dueños de los sistemas de su trabajo, su escuela y otros sobre lo que ha ocurrido.

DESPUÉS DE UN ATAQUE CIBERNÉTICO

- Comuníquese con los bancos, compañías de tarjetas de crédito y otras compañías de servicios financieros donde usted tiene sus cuentas. Podría tener que suspender las cuentas que han sido atacadas. Cierre todas las cuentas de crédito o pago no autorizadas. Informe que otra persona podría estar usando su identidad.

- Si entiende que alguien está usando su número de Seguro Social de manera ilegal, presente una denuncia con la Oficina del Inspector General (OIG, por sus siglas en inglés).

- Denuncie el robo de identidad a la Comisión Federal de Comercio. Si recibe mensajes de alguien que dice ser un agente del gobierno, comuníquese con la Comisión Federal de Comercio (FTC, por sus siglas en inglés) en ftc.gov/complaint.

- Comuníquese con otras agencias según el tipo de información robada.