CÓMO MANTENERSE SEGURO

CUANDO UN CIBERATAQUE AMENAZA

AHORA Prevenir

Mantenga su software antivirus actualizado.

Use contraseñas seguras de 12 caracteres o más. Use letras mayúsculas y minúsculas, números y caracteres especiales. Cambie las contraseñas mensualmente. Utilice un administrador de contraseñas.

Use una autenticación más segura, como un PIN o una contraseña, que solo usted conocería. Considere usar un dispositivo separado que pueda recibir un código o use un escaneo biométrico
(por ejemplo, escáner de huellas digitales).

Esté atento a las actividades sospechosas que le pidan que haga algo de inmediato, ofrezca algo que suene demasiado bueno para ser verdad o necesite su información personal. Piensa antes de hacer clic.

Revise sus estados de cuenta e informes de crédito regularmente.

Utilice comunicaciones seguras por Internet. Use sitios que usen "HTTPS" si

accederá o proporcionará cualquier información personal. No use sitios con certificados no válidos. Utilice una red privada virtual (VPN) que cree una conexión segura.

Utilice soluciones antivirus, malware y firewalls para bloquear amenazas.

Haga copias de seguridad periódicas de sus archivos en un archivo cifrado o dispositivo de almacenamiento de archivos cifrados.

Limite la información personal que comparte en línea. Cambie la configuración de privacidad y no utilice las funciones de ubicación.

Proteja su red doméstica cambiando las contraseñas administrativas y Wi-Fi regularmente. Al configurar su router, elija la configuración Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES), que es la opción de cifrado más fuerte.

DURANTE Límite de daños

Limite el daño. Busque cargos inexplicables, cuentas extrañas en su informe de crédito, denegación inesperada de su tarjeta de crédito, publicaciones que no hizo que aparecieran en sus redes sociales y personas que reciben correos electrónicos que nunca envió.

Cambie inmediatamente las contraseñas de todas sus cuentas en línea.

Escanee y limpie su dispositivo.

Considere apagar el dispositivo. Llévelo a un profesional para escanearlo y arreglarlo.

Deje trabajar, la escuela u otro

Los propietarios del sistema lo saben. Los departamentos de tecnología de la información (TI) pueden necesitar advertir a otros y actualizar los sistemas.

Póngase en contacto con bancos, compañías de tarjetas de crédito y otras cuentas financieras. Es posible que deba retener las cuentas que han sido atacadas. Cierre cualquier cuenta de crédito o cargo no autorizada. Informe que alguien puede estar usando su identidad.

Informe AFTER

Presente un informe ante la Oficina del Inspector General (OIG) si cree que alguien está usando ilegalmente su número de Seguro Social. La OIG revisa los casos de despilfarro, fraude y abuso. Para presentar un informe, visite www.idtheft.gov.

También puede llamar a la línea directa de la Administración del Seguro Social al

1-800-269-0271. Para obtener recursos adicionales y más información, visite http://oig.ssa. gov/informe.

Presente una queja ante el Centro de Quejas de Delitos en Internet (IC3) del FBI en www.IC3.gov. Ellos revisarán

la queja y remitirla a la agencia apropiada.

Aprenda consejos, herramientas y más en www.dhs.gov/stopthinkconnect.

Tome un activo Rol en su Seguridad

Vaya a Ready.gov y busque ciberataque. Descargue la aplicación de FEMA para obtener más información sobre cómo prepararse para un ataque cibernético.

MIDDLETOWN
City of Middletown Health Department
Public Health

July 2023