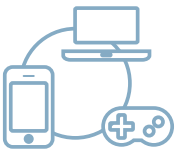
ESTÉ PREPARADO PARA UN ATAQUE CIBERNÉTICO

FEMA

FEMA V-1002/Mayo de 2018

Los ataques cibernéticos pueden generar pérdidas de dinero, robo de información personal y daños a su reputación y seguridad.

Los ataques cibernéticos son las tentativas por parte de los piratas informáticos de acceder a un sistema informático o dañarlo.



Pueden usar computadoras, teléfonos celulares, sistemas de juegos y otros dispositivos.

Pueden incluir fraude o robo de identidad.

Pueden interrumpirle el acceso o eliminar sus documentos personales y fotografías.

Pueden atentar contra los niños.

Pueden provocar problemas en los servicios comerciales, el transporte y la energía.

PROTÉJASE CONTRA UN ATAQUE CIBERNÉTICO

Mantenga el software y los sistemas operativos actualizados.

Use contraseñas seguras y la autentificación de dos factores (dos métodos de verificación).

Esté atento a actividades sospechosas. Ante la duda, no haga clic. No proporcione información personal.

Use comunicaciones en Internet cifradas (seguras).

Cree copias de seguridad.

Proteja la red de wifi de su casa.

CÓMO MANTENERSE SEGURO
ANTE UNA AMENAZA DE ATAQUE CIBERNÉTICO

AHORA
Prevenga

Mantenga el software actualizado.

Use contraseñas seguras que contengan 12 caracteres o más. Use mayúsculas y minúsculas, números y caracteres especiales. Cambie la contraseña todos los meses. Use un administrador de contraseñas.

Use una autentificación más segura. Use **algo que conozca,** como un número de identificación personal o una contraseña; **algo que tenga** por separado, como un teléfono que pueda recibir un código o **un escaneo biométrico**, como el escaneo de sus huellas digitales.

Esté atento a actividades sospechosas mediante las cuales se le solicite hacer algo de inmediato, que le ofrezcan algo que sea demasiado bueno para ser verdad o para las que se necesite su información personal. **Piense antes de hacer clic**.

Controle sus estados de cuenta e informes crediticios periódicamente.

Use comunicaciones en Internet que sean seguras. Utilice sitios que usen HTTPS si desea acceder o proporcionar todo tipo de información personal. No use sitios con certificados inválidos. Use una Red Virtual Privada (VPN) que establezca una conexión segura.

Use soluciones de antivirus, programas maliciosos y cortafuegos para interrumpir amenazas.

Cree copias de seguridad periódicamente.

Limite la información personal que comparta en Internet. Cambie las configuraciones de privacidad y no use funciones de ubicación.

Proteja la red de su casa cambiando la contraseña administrativa y de wifi periódicamente. Elija el cifrado "WPA2".

MIENTRAS OCURRA
Limite el daño

Limite el daño. Esté atento a cargos injustificados, cuentas extrañas en su informe crediticio, rechazos inesperados de su tarjeta de crédito, publicaciones que no haya hecho pero que aparezcan en sus medios sociales, y las personas que reciban correos electrónicos que nunca haya mandado.

Cambie inmediatamente las contraseñas de todas sus cuentas en Internet.

Analice y limpie su dispositivo.

Considere apagar su dispositivo. Llévelo a un profesional para que lo analice y lo repare.

Infórmeselo a los encargados de trabajos, escuelas y de otros sistemas. Es posible que los departamentos de Tecnología de la Información (IT) necesiten advertir a otros y actualizar sistemas.

Comuníquese con bancos, empresas de tarjeta de crédito y otras cuentas financieras. Es posible que necesite dejar inactivas las cuentas que se hayan atacado. Cierre toda cuenta de cargo o crédito no autorizada. Denuncie que es posible que alguien esté usando su identidad.

DESPUÉS
Reporte

Presente una denuncia ante la **Oficina del Inspector General (OIG)** si cree que alguien esté usando su número de Seguro Social de forma ilícita. **La OIG revisa casos de despilfarros, fraudes y abusos**. Para presentar una denuncia, visite http://www.idtheft.gov.

Además, puede llamar a la línea directa de la Administración de Seguridad Social marcando 1-800-269-0271. Para obtener recursos adicionales y mayor información, visite http://oig.ssa.gov/report-fraud-waste-or-abuse.

Para presentar una queja ante el Centro de Quejas contra Delitos en Internet (IC3) del **FBI** diríjase a www.IC3.gov. La revisarán y la remitirán a la agencia correspondiente.

FEMA
FEMA V-1002
Catalog No. 17233-3

Tome un rol activo en su seguridad

Diríjase a **Ready.gov** y busque **ataque cibernético**. Diríjase a **dhs.gov/stopthinkconnect** para enterarse de consejos, herramientas y mucho más.