Seguridad de su organización en Internet

¿Por qué es importante la ciberseguridad para las organizaciones y los grupos comunitarios?

En esta página encontrará recomendaciones y algunas medidas que puede tomar para proteger a su organización o grupo comunitario de las amenazas a la ciberseguridad. También hay una guía independiente que se refiere a lo que los particulares pueden hacer para preservar su seguridad en Internet.

Estas recomendaciones se refieren a las amenazas más frecuentes y graves.

- Actualizaciones. Mantenga actualizado el software de sus dispositivos para que no haya brechas de seguridad.
    - Mantenga actualizados los dispositivos de su organización o grupo comunitario. Esto abarca los teléfonos, las computadoras, los *routers* wifi y cualquier otro dispositivo que se conecte a Internet, incluidos los inteligentes.
    - Utilice las actualizaciones automáticas siempre que sea posible.
- Autenticación de dos factores (2FA). Aporta seguridad adicional a sus cuentas al exigir una contraseña y un paso más, por ejemplo, el código de una aplicación del teléfono.
    - Nota: Este tipo de autenticación también tiene otros nombres, como autenticación multifactor (MFA), verificación de dos pasos (2SV) y varios más.
    - Active la autenticación de dos factores en todas las cuentas de su organización o grupo comunitario.
    - Si es posible, intente utilizar una forma de autenticación que sea resistente a la suplantación de identidad (*phishing*), de modo que no puedan engañarle para que la facilite. Puede ser una clave de seguridad física u otro medio, como una huella dactilar o un identificador facial.
- Controle sus cuentas en línea. Asegúrese de que los antiguos miembros no conserven el acceso a las cuentas tras dejar la organización o el grupo comunitario.
    - Si hay más de una persona que accede a la misma cuenta, compruebe que todas tengan datos de acceso diferentes y que todas tengan activada la autenticación de dos factores.
    - Lleve una lista de todas las cuentas de usuario y desactive las que no sean necesarias, por ejemplo, las correspondientes al personal que deja su puesto.
    - Lleve un registro de todos los dispositivos que haya entregado a sus miembros, y recuerde recuperarlos y restablecer la configuración de fábrica cuando una persona deja la organización. También es posible que tenga que cambiar los códigos físicos de acceso a los edificios.
- Compruebe quién tiene acceso a sus cuentas en línea. Las personas de su organización o grupo comunitario solo deben tener acceso a lo que necesiten.

    - Si la cuenta de una persona es pirateada, estas medidas limitan el daño que puede causar el atacante.
    - Compruebe y elimine periódicamente los permisos innecesarios.
    - Si tiene una sola cuenta de administrador (admin) que utilizan varias personas, vigílela para detectar actividades inusuales. Intente limitar el uso de este tipo de cuentas, sobre todo para las tareas cotidianas.
    - Estas normas también se aplican al acceso de administrador a los dispositivos, como los *routers*.

- Revise sus contratos con los proveedores de servicios, si ha contratado a alguien para que le preste servicios informáticos.
    - Cerciórese de que dispongan de protecciones de ciberseguridad que satisfagan las necesidades de su organización o grupo comunitario.
- Sepa cómo funcionan conjuntamente todas sus cuentas y sistemas. Conocer las conexiones le ayudará a saber por dónde podría entrar un atacante.
    - Revise las conexiones entre sus sistemas, por ejemplo, el correo electrónico, el almacenamiento en la nube y las plataformas de contabilidad.
    - Considere la posibilidad de utilizar una red privada virtual (VPN) para aumentar la seguridad en Internet. Usar una red de este tipo le permite ocultar su actividad en Internet de cualquiera que intente rastrearla. Esto es muy útil si algún miembro de la organización o grupo comunitario se conecta a distancia.
- Procure que su personal sea ciberinteligente. Las personas de su organización o grupo comunitario tienen más probabilidades de ser víctimas de un ataque que sus sistemas.
    - Capacite a todo el personal en materia de ciberseguridad básica. En el sitio Own Your Online | NCSC encontrará una amplia gama de consejos y sugerencias para preservar su seguridad en Internet y detectar estafas.
    - Recuérdele al personal que la ciberseguridad es importante tanto en el caso de sus cuentas personales como en el de las que utilizan para la organización.
    - También disponemos de una guía dirigida a los particulares sobre cómo preservar su seguridad en Internet.
- Planifique en caso de que ocurra un incidente. Es importante disponer de un plan de respuesta para evitar que cunda el pánico cuando se produce un incidente.
    - En un plan de respuesta ante incidentes se describe quién hace qué durante un incidente. En el siguiente documento se pueden encontrar modelos de planes: Incident Management | NCSC.
    - Planifique qué hacer si fallan los teléfonos, las computadoras u otros sistemas. Mantenga actualizado el plan.
    - Conserve los datos de contacto de todas las personas necesarias y también datos alternativos en caso de que se interrumpa la principal vía de contacto (como el correo electrónico).

- Guarde una copia del plan en algún lugar externo al sistema, por si no puede acceder a él.