SEGURIDAD INFORMÁTICA

La privacidad de los datos es un área que se encuentra en constante cambio, y los gobiernos a lo largo de los Estados Unidos están promulgando nuevas leyes y reglamentaciones para ayudar a proteger la información personal de los estadounidenses en una sociedad cada vez más digital.

Indiana no ha escapado a las crecientes amenazas a la seguridad informática. De acuerdo con la Oficina Federal de Investigación (FBI), más de 23,000 habitantes de Indiana fueron víctimas de ataques a la seguridad informática en línea durante 2024 únicamente, lo que supuso pérdidas de más de $125 millones. Los ataques a la seguridad informática también son una principal amenaza para gobiernos, escuelas, empresas y otras organizaciones de Indiana. En 2021, entró en vigor una ley de Indiana sobre notificación de incidentes de seguridad informática, que exige a todas las subdivisiones políticas que notifiquen los incidentes de seguridad informática a la Oficina de Tecnología de Indiana.

A medida que los ataques se vuelven más comunes y sofisticados, es importante que todas las familias y empresas de Indiana sepan cómo identificar y evitar las amenazas en línea. Los habitantes de Indiana pueden obtener más información sobre la seguridad informática y cómo proteger mejor la privacidad de sus datos consultando los consejos que figuran a continuación y visitando el Centro de Seguridad Informática de Indiana.

CONSEJOS RÁPIDOS

- Cree contraseñas seguras de al menos ocho caracteres y utilice combinaciones de letras mayúsculas y minúsculas, números y signos de puntuación.
- Utilice diferentes nombres de usuario y contraseñas para sus cuentas, y asegúrese de implementar la autenticación multifactor.
- No abra ni descargue archivos, responda preguntas ni siga instrucciones en correos electrónicos enviados por remitentes desconocidos o no solicitados. Nunca les envíe información personal ni financiera.
- Mantenga actualizados los programas antivirus en todos los dispositivos.
- Haga copias de seguridad de los archivos importantes en un disco duro externo, una unidad flash o una cuenta de almacenamiento en la nube en línea.

CONSEJOS DE SEGURIDAD INFORMÁTICA

CONTRASEÑAS

Las contraseñas son las claves de la información y los datos personales. Tener una contraseña segura ayudará a mantener alejados a los intrusos.

- Las contraseñas deben tener al menos ocho caracteres y utilizar combinaciones de letras mayúsculas y minúsculas, números y signos de puntuación.
- Nunca utilice el mismo nombre de usuario y contraseña en varios sitios web.
- Nunca utilice información personal, como nombres, edades, cumpleaños ni nombres de mascotas.
- Evite introducir contraseñas personales en dispositivos compartidos.
- Implemente la autenticación multifactor en sus cuentas, incluso en correos electrónicos, redes sociales, compras en línea, servicios financieros, juegos y entretenimiento.

COMPRAS

Las ventas en línea han aumentado de manera constante durante la última década y ahora representan más del 10% de los ingresos totales del comercio minorista en Estados Unidos, lo que significa que cada vez se transmite y almacena más información financiera confidencial en línea. Proteja esta información siguiendo estos consejos:

- Antes de comprar algo, consulte el sitio web para ver los avisos de autenticación y seguridad.
- Tenga cuidado con los precios muy reducidos.
- En los sitios de subastas, compruebe la reputación del vendedor, lea las reseñas sobre el vendedor y lea detenidamente la descripción del artículo.
- Al finalizar la compra, utilice un método de pago seguro, como una tarjeta de débito o crédito.
- Evite comprar en una computadora pública o en una red Wi-Fi pública.

COMUNICACIÓN

Actualmente, se comparte gran cantidad de información a través de algún tipo de comunicación en línea. Mantener la discreción ayudará a que la información quede en las manos adecuadas.

- Nunca abra, responda ni siga instrucciones enviadas en correos electrónicos por remitentes desconocidos o no solicitados.
- Nunca envíe información personal ni financiera a una persona desconocida o que no la haya solicitado.
- No descargue archivos ni programas de una compañía o fuente desconocida.
- Cambie la configuración de privacidad de las redes sociales para que solo las personas de confianza puedan ver la información que publique.
- Limite la cantidad de información personal que comparte en las redes sociales.
- Nunca comparta información financiera, información de cuentas ni contraseñas en las redes sociales.

DISPOSITIVOS

De acuerdo con el Centro de Investigación Pew, el 97% de los estadounidenses posee un teléfono celular, la mitad posee una tableta y alrededor del 75% posee una computadora de escritorio o portátil. Dado que estos dispositivos contienen información personal, es importante protegerlos de los delincuentes informáticos.

- Durante los viajes, mantenga siempre las computadoras portátiles y los dispositivos móviles cerca o bloqueados con una contraseña segura, especialmente si no están a su alcance.
- Nunca responda llamadas ni mensajes de contactos desconocidos.
- Proteja los dispositivos con contraseñas seguras.
- Encripte toda la información confidencial o personal.

SOFTWARE

Además de tener precaución y utilizar contraseñas seguras, los programas de software también pueden proporcionar una capa de protección para los dispositivos. Investigue los programas y decida cuál es el más adecuado para el hogar o la empresa.

- Haga copias de seguridad de los archivos importantes en un disco duro externo, una unidad flash o una cuenta de almacenamiento en la nube en línea.
- Instale un software antivirus que detecte y elimine virus de los dispositivos electrónicos.
- Mantenga actualizados los sistemas operativos de los dispositivos, las aplicaciones y el software de seguridad. Active las actualizaciones automáticas.
- Instale un cortafuegos para bloquear el material perjudicial.

QUÉ HACER Y QUÉ NO HACER EN EL LUGAR DE TRABAJO

Qué hacer en el lugar de trabajo

Recordar poner en práctica los consejos de seguridad digital en el trabajo podría evitar que una compañía tenga que gastar millones de dólares para hacer frente a las consecuencias de un ataque a la seguridad informática.

- Comprenda la terminología común sobre seguridad informática. Una excelente manera de prevenir los ataques a la seguridad informática es comprender qué son y cómo funcionan.
- Use contraseñas que tengan al menos ocho caracteres y utilice combinaciones de letras mayúsculas y minúsculas, números y signos de puntuación. Una contraseña segura reduce la posibilidad de que los delincuentes informáticos encuentren información personal.
- Mantenga actualizados los programas antivirus en todos los dispositivos electrónicos. Estos programas pueden detectar y eliminar posibles ataques a la seguridad informática.
- Cambie la configuración de privacidad de las redes sociales para que solo las personas de confianza puedan ver las publicaciones
- Cambie regularmente las contraseñas de todas las cuentas.
- Bloquee la computadora cuando se aleje del escritorio o lugar de trabajo. Dejar la computadora desbloqueada permite que personas no autorizadas accedan a información confidencial relacionada con el trabajo.
- Verifique el remitente del correo electrónico antes de abrir un mensaje. El mensaje puede parecer legítimo, pero podría contener un virus.
- Pregunte a sus empleadores sobre los cursos de formación sobre seguridad informática disponibles.
- Durante los viajes, mantenga siempre las computadoras portátiles y los dispositivos electrónicos cerca o bloqueados con una contraseña segura, especialmente si no están dentro de su alcance.

Qué no hacer en el lugar de trabajo

Evitar algunos errores comunes puede hacer que el lugar de trabajo sea más seguro y disminuir la probabilidad de un ataque a la seguridad informática.

- Nunca utilice el mismo nombre de usuario y la misma contraseña en varios sitios web. Usar la misma contraseña puede aumentar la posibilidad de que los delincuentes informáticos roben información de varias cuentas.
- Nunca use información personal como nombres, nombres de mascotas ni fechas de nacimiento en las contraseñas.
- Nunca comparta contraseñas con otras personas.
- Nunca haga clic en enlaces ni siga instrucciones en correos electrónicos de remitentes desconocidos o no solicitados.
- Nunca descargue imágenes, documentos ni software de fuentes desconocidas o no solicitadas.
- Nunca comparta información confidencial relacionada con el trabajo con personas no autorizadas.
- Nunca deje la computadora encendida de forma permanente.