



CONCIENCIA EN CIBERSEGURIDAD

Cómo Evitar que Los Hackers se aprovechen de Tí?

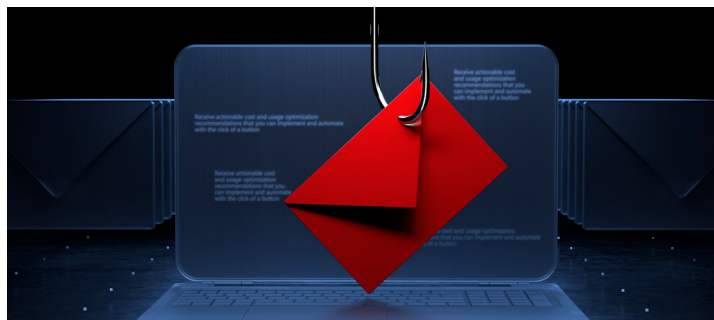
Aprenda a detectar y evitar los peligros cibernéticos.

La capacitación en concientización sobre ciberseguridad puede ayudar a los empleados a aprender cómo detectar peligros y brindarles las herramientas necesarias para evitar ser explotados por delincuentes para acceder a los datos comerciales y de los clientes.

Uno de los tipos más comunes de amenazas a la ciberseguridad es el phishing, en el que los atacantes intentan engañar a las personas para que les proporcionen información confidencial. El ransomware es otro tipo de amenaza que puede resultar especialmente perjudicial para las empresas.

¿Por qué realizar una capacitación en sensibilización en ciberseguridad Para tus empleados?

- Comprender y reconocer los riesgos de ciberseguridad
- Saber cómo protegerse a sí mismos y a su empresa de estos riesgos.
- Saber qué hacer si sospechan o experimentan una violación de la ciberseguridad
- Manténgase actualizado sobre las últimas amenazas y tendencias de ciberseguridad
- Aprender a detectar cuando un email es spam o Phishing



Capacita a tus empleados para que se conviertan en tu primera línea de defensa contra los ciberataques.

Tres de los peligros cibernéticos comunes que causan problemas a las empresas y les cuestan dinero son:

- Estafas de phishing
- Ransomware
- Malware y virus

La preparación es clave en cualquier esfuerzo, pero es aún más crítica para proteger su empresa de ataques cibernéticos.

La capacitación en concientización sobre ciberseguridad puede ayudar a los empleados a aprender cómo detectar y evitar estas amenazas. Además, contar con un plan de ciberseguridad puede ayudar a minimizar el daño si una empresa se ve afectada por un ciberataque.

1. **Concientización** - Para proteger a su empresa de amenazas cibernéticas, todos los empleados deben conocer las mejores Prácticas para la ciberseguridad.
2. **Links** - Los empleados nunca deben hacer clic en enlaces o archivos adjuntos de remitentes desconocidos, incluso si el correo electrónico parece legítimo.
3. **Email** - Si un empleado recibe un correo electrónico sospechoso, debe informarlo a su departamento de TI o equipo de seguridad inmediatamente.
4. **Compartir Credenciales** - Los empleados nunca deben darse por vencidos su nombre de usuario o contraseña a cualquier persona, incluso si parecer digno de confianza.
5. **Credenciales Robustas** - Los empleados deben practicar buenas Higiene de las contraseñas mediante el uso de contraseñas seguras y únicas para cada cuenta.
6. **Autenticación Multifactor** - Los empleados deben habilitar autenticación de dos factores (2FA) siempre que sea posible para agregar una capa adicional de seguridad a sus cuentas.
7. **Plataformas Públicas** - Los empleados deben tener cuidado con la información que comparten en las redes sociales o lugares públicos.
8. **Reportar** - Si un empleado sospecha que su cuenta ha sido comprometida, debe informarlo inmediatamente a su departamento de TI o al equipo de seguridad.



El beneficio empresarial de ser ciberconsciente

- Reduzca su perfil de riesgo cibernético
- Mejore su potencial de tiempo de actividad
- Reducir el riesgo financiero de la empresa.
- Ayudar a cumplir con los requisitos de capacitación en concientización cibernética para seguros.
- Ayudar a proteger los datos de empleados, clientes y empresas

Necesitas mas información?

ZITSEC

<https://www.zitsec.com>

info@zitsec.com

+593 98 495 5546