NEWSLETTER

CIBERSEGURIDAD

septiembre 2024

FRASE DEL MES:

Tu contraseña es tu escudo. Asegúrate de que sea fuerte e impenetrable.

PROTEGE TU MUNDO DIGITAL: 3 PASOS CLAVE

- **Actualiza todo:** Mantén tu sistema operativo, aplicaciones y antivirus siempre actualizados. Las actualizaciones suelen incluir parches de seguridad que protegen contra las últimas amenazas.
- **Desconfía de los enlaces**: No hagas clic en enlaces sospechosos, especialmente en correos electrónicos o mensajes de texto de remitentes desconocidos. Podrían llevarte a sitios web maliciosos diseñados para robar tu información.
- **Usa contraseñas fuertes**: Crea contraseñas únicas y complejas para cada una de tus cuentas. Combina mayúsculas, minúsculas, números y símbolos para hacerlas más difíciles de descifrar.

S&T

SOLUCIONES & TECNOLOGIA S.A.S.

Sus desafios digitales, nuestras soluciones personalizadas

www.solytec.com.co

Especialistas en Ciberprotección

✓ Guardianes Digitales: Agradecimiento y Consejos en Ciberseguridad

Capacitar a los empleados en ciberseguridad es fundamental por varias razones:

1. **Primera línea de defensa**: Los empleados son a menudo el primer punto de contacto con posibles amenazas cibernéticas. Al estar capacitados, pueden identificar y reportar a tiempo cualquier actividad sospechosa, evitando así grandes problemas.
2. **Reducción de riesgos**: Una fuerza laboral con conciencia en ciberseguridad disminuye significativamente el riesgo de sufrir ataques cibernéticos como phishing, ransomware o intrusiones.
3. **Protección de datos sensibles**: La información confidencial de la empresa y de los clientes es un activo valioso. La capacitación garantiza que los empleados manejen estos datos con cuidado y sigan los protocolos de seguridad adecuados.
4. **Cumplimiento normativo**: Muchas industrias tienen regulaciones específicas sobre la protección de datos. Capacitar al personal ayuda a cumplir con estos requisitos legales y evitar sanciones.
5. **Mejora de la reputación**: Un incidente de ciberseguridad puede dañar gravemente la reputación de una empresa. La capacitación demuestra un compromiso con la seguridad y la confianza de los clientes.
6. **Ahorro de costos**: Los ataques cibernéticos pueden tener un costo económico significativo. La prevención a través de la capacitación es mucho más rentable que tener que lidiar con las consecuencias de un incidente.

En resumen, capacitar a los empleados en ciberseguridad es una inversión en la seguridad de la empresa, la protección de los datos y la tranquilidad de todos los involucrados.

NEWSLETTER

CIBERSEGURIDAD

septiembre 2024

FRASE DEL MES:

Tu contraseña es tu escudo. Asegúrate de que sea fuerte e impenetrable.

PROTEGE TU MUNDO DIGITAL: 3 PASOS CLAVE

- **Actualiza todo:** Mantén tu sistema operativo, aplicaciones y antivirus siempre actualizados. Las actualizaciones suelen incluir parches de seguridad que protegen contra las últimas amenazas.
- **Desconfía de los enlaces**: No hagas clic en enlaces sospechosos, especialmente en correos electrónicos o mensajes de texto de remitentes desconocidos. Podrían llevarte a sitios web maliciosos diseñados para robar tu información.
- **Usa contraseñas fuertes**: Crea contraseñas únicas y complejas para cada una de tus cuentas. Combina mayúsculas, minúsculas, números y símbolos para hacerlas más difíciles de descifrar.

✓ Guardianes Digitales: Agradecimiento y Consejos en Ciberseguridad

Capacitar a los empleados en ciberseguridad es fundamental por varias razones:

1. **Primera línea de defensa**: Los empleados son a menudo el primer punto de contacto con posibles amenazas cibernéticas. Al estar capacitados, pueden identificar y reportar a tiempo cualquier actividad sospechosa, evitando así grandes problemas.
2. **Reducción de riesgos**: Una fuerza laboral con conciencia en ciberseguridad disminuye significativamente el riesgo de sufrir ataques cibernéticos como phishing, ransomware o intrusiones.
3. **Protección de datos sensibles**: La información confidencial de la empresa y de los clientes es un activo valioso. La capacitación garantiza que los empleados manejen estos datos con cuidado y sigan los protocolos de seguridad adecuados.
4. **Cumplimiento normativo**: Muchas industrias tienen regulaciones específicas sobre la protección de datos. Capacitar al personal ayuda a cumplir con estos requisitos legales y evitar sanciones.
5. **Mejora de la reputación**: Un incidente de ciberseguridad puede dañar gravemente la reputación de una empresa. La capacitación demuestra un compromiso con la seguridad y la confianza de los clientes.
6. **Ahorro de costos**: Los ataques cibernéticos pueden tener un costo económico significativo. La prevención a través de la capacitación es mucho más rentable que tener que lidiar con las consecuencias de un incidente.

En resumen, capacitar a los empleados en ciberseguridad es una inversión en la seguridad de la empresa, la protección de los datos y la tranquilidad de todos los involucrados.