FASTREANDO

Toma el control: Implementa buenas prácticas en tu email y contraseñas.

Resumen.

El correo electrónico se ha convertido en una herramienta fundamental para la comunicación personal y profesional. Sin embargo, también es un vector de ataque común para los ciberdelincuentes. Por lo que las contraseñas se convierten en la primera línea de defensa en esta era digital. Estas nos permiten proteger información confidencial, acceder a plataformas virtuales y realizar diversas actividades en línea. Sin embargo, su uso adecuado no siempre es intuitivo, y muchos usuarios las utilizan de forma incorrecta, poniendo en riesgo su seguridad.

Razones para tener una contraseña segura:

- **Protección contra hackers:** Las contraseñas seguras son más difíciles de descifrar por software de ataque automatizado, lo que reduce el riesgo de ser vulnerado.
- **Prevención de robo de identidad:** Una contraseña segura protege la información personal y financiera, evitando que los hackers la roben y la usen para suplantar.
- **Seguridad contra ataques de fuerza bruta:** Los ataques de fuerza bruta prueban millones de combinaciones de caracteres para adivinar su contraseña. Una contraseña larga y compleja aumenta el tiempo que tarda un ataque de este tipo en tener éxito.
- **Reducción del riesgo de phishing:** En los ataques de phishing intentaran engañarlo para que revele la contraseña. Una contraseña segura te protege de estos ataques, ya que es menos probable que la compartas con alguien que se hace pasar por una entidad legítima.

Consejos para crear una contraseña segura:

- Utilizar una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Crear una contraseña larga, de al menos 12 caracteres.
- Evitar usar palabras comunes, información personal o secuencias fáciles de adivinar.
- No usar la misma contraseña para diferentes cuentas.
- Utilizar un gestor de contraseñas para almacenar y administrar las contraseñas.
- Cambiar todas las contraseñas regularmente.

Seis prácticas recomendadas para mejorar la seguridad y el filtrado del correo electrónico:

1. Contraseñas seguras:

   Utiliza contraseñas únicas y complejas para cada cuenta de correo electrónico. Evitando usar palabras comunes, información personal o secuencias fáciles de adivinar. Combina letras mayúsculas y minúsculas, números y símbolos especiales.

2. Autenticación de dos factores (2FA):

   Activa 2FA para agregar una capa adicional de seguridad a la cuenta. Esto requiere un segundo factor de autenticación, como un código temporal enviado a el teléfono móvil, aparte de la contraseña.

3. Software actualizado:

   Mantener actualizado el software de correo electrónico, navegador web y sistema operativo. Las actualizaciones de software a menudo incluyen parches de seguridad críticos. Instalar un antivirus de confianza y mantenerlo actualizado.

4. Precaución con correos electrónicos sospechosos:

   No abra correos electrónicos de remitentes desconocidos, tenga cuidado con los enlaces y archivos adjuntos en correos electrónicos, incluso de remitentes conocidos. Verifique la dirección de correo electrónico del remitente para detectar falsificaciones.

5. Filtrado de correo electrónico:

   Utilizar un filtro de correo electrónico para bloquear correos no deseados, spam y phishing. Hay opciones de filtrado del lado del servidor, en la nube y de escritorio. El filtrado basado en la nube ofrece la mejor protección en tiempo real.

6. Conciencia y educación:

   Mantener informado sobre las últimas amenazas de seguridad cibernética, capacitar a los empleados sobre prácticas seguras de correo electrónico y fomentar una cultura de seguridad en la organización.

La seguridad debe ser una prioridad constante para proteger la información confidencial, los datos de los clientes y la buena imagen de la organización. Implementar medidas de seguridad robustas es crucial para prevenir ataques cibernéticos, fugas de datos y daños a la reputación de la empresa. Recuerde que la seguridad es un proceso continuo y requiere atención constante.