

Reconociendo y evitando estafas por correo electrónico

El correo electrónico nos brinda una herramienta de comunicación conveniente y poderosa. Sin embargo, también proporciona a estafadores y otros individuos maliciosos un medio fácil para atraer a posibles víctimas. Las estafas que intentan van desde operaciones de cebo y cambio tradicionales hasta esquemas de phishing que utilizan una combinación de correo electrónico y sitios web falsos para engañar a las víctimas y hacer que divulguen información sensible. Para protegerte de estas estafas, debes comprender qué son, cómo se ven, cómo funcionan y qué puedes hacer para evitarlas. Las siguientes recomendaciones pueden minimizar tus posibilidades de convertirte en víctima de una estafa por correo electrónico:

- Filtra el correo no deseado.
- No confíes en correos electrónicos no solicitados.
- Trata los archivos adjuntos de correo electrónico con precaución.
- No hagas clic en los enlaces en los mensajes de correo electrónico.
- Instala software antivirus y manténlo actualizado.
- Instala un firewall personal y manténlo actualizado.
- Configura tu cliente de correo electrónico para la seguridad.

Estas recomendaciones se explican en la sección «Lo que puedes hacer para evitar convertirte en una víctima». Ignorarlas puede dejarte vulnerable al robo de identidad, robo de información, abuso de tu computadora para actividades ilegales, recepción de mercancías falsas o ilegales y pérdida

financiera.

Las estafas por correo electrónico generalmente comienzan con correo electrónico comercial no solicitado, o «spam». Antes del correo electrónico, un estafador tenía que contactar a cada posible víctima individualmente por correo postal, fax, teléfono o contacto personal directo. Estos métodos a menudo requerían una inversión significativa en tiempo y dinero. El correo electrónico ha cambiado el juego para los estafadores, proporcionando conveniencia y anonimato, y permitiendo el contacto con miles de personas a la vez.

Las estafas de correo electrónico pueden incluir oportunidades comerciales falsas, esquemas de salud y dietas fraudulentos, ofertas de software a precios bajos, estafas de tarifas avanzadas 419, y correos electrónicos de ingeniería social y phishing.

Es importante tratar el correo electrónico no solicitado con escepticismo, tener precaución con los archivos adjuntos, no hacer clic en enlaces en correos electrónicos desconocidos y configurar adecuadamente tu cliente de correo electrónico para la seguridad. Además, instala y mantén actualizado el software antivirus y el firewall personal para proteger tu sistema contra amenazas potenciales.