# Phishing al acecho: cómo detectarlo y evitar que roben tus datos

*Recopilado por Amalia Beltrán*


El phishing es una de las formas más comunes de robo de información en la actualidad. Representa el 16% de todos los casos de filtración o robo de datos, lo que lo convierte en el método más utilizado para obtener información de manera ilegal según estudios de instituciones internacionales.

Aunque internet ofrece numerosas ventajas al simplificar nuestras actividades diarias, también crea un ambiente propicio para diversos tipos de fraudes. El anonimato y la posibilidad de interacción global facilitan a los delincuentes engañar a las personas.

Por eso, es crucial estar bien informados sobre las amenazas y esquemas de fraude más comunes y adoptar medidas preventivas adecuadas.

## Principales amenazas a tener en cuenta

Phishing: se trata de correos electrónicos o mensajes que se hacen pasar por entidades legítimas con el fin de robar tu información personal. Estos mensajes suelen parecer auténticos, pero están diseñados para engañarte y obtener datos sensibles.

Malware: este software malicioso está diseñado para robar tus datos o tomar control de tu sistema informático. Puede llegar a través de descargas, correos electrónicos o sitios web comprometidos.

Anuncios maliciosos: publicidad con enlaces que redirigen a sitios peligrosos o que descargan malware en tu dispositivo. Estos anuncios pueden parecer legítimos pero esconden amenazas.

Páginas fraudulentas: sitios web que imitan a los legítimos con el propósito de obtener tu información personal. A menudo tienen un diseño similar al de las páginas auténticas, pero con ligeras diferencias.

Smishing: mensajes de texto fraudulentos que contienen enlaces o solicitan información personal. A menudo buscan crear un sentido de urgencia para que actúes rápidamente sin pensar.

## Medidas preventivas para reducir riesgos

Desconfía de correos electrónicos y mensajes sospechosos: si recibes un mensaje inesperado que te pide información personal, como contraseñas o números de tarjeta de crédito, no respondas ni hagas clic en enlaces. Verifica siempre la autenticidad del remitente.


Revisa el remitente con atención: los correos de phishing suelen proceder de direcciones que parecen legítimas pero tienen ligeras diferencias. Fíjate en detalles como faltas de ortografía o dominios extraños.

No hagas clic en enlaces ni descargues archivos adjuntos: si un mensaje te pide que hagas clic en un enlace o descargues un archivo, verifica primero su autenticidad. Es más seguro visitar el sitio web directamente escribiendo la dirección en tu navegador.

No compartas información personal: nunca respondas a mensajes que soliciten información personal como contraseñas, números de seguridad o token, incluso si parecen provenir de una fuente confiable.

Activa la autenticación en dos pasos (2FA): la autenticación en dos pasos añade una capa adicional de seguridad, incluso si alguien obtiene tu contraseña. Actívala en todas las cuentas que lo permitan.

Mantén tu software actualizado e instala un buen antimalware/antivirus: asegúrate de que tu sistema operativo, navegador y software de seguridad estén actualizados. Las actualizaciones suelen incluir parches para vulnerabilidades.

Sé cauteloso con las solicitudes urgentes: los intentos de phishing y smishing suelen intentar crear un sentido de urgencia, como la amenaza de bloqueo de cuentas o urgencias médicas. Tómate el tiempo para investigar antes de actuar.

Verifica los sitios web antes de ingresar información: asegúrate de que la dirección del sitio comience con «https://» y de que haya un ícono de candado en la barra de direcciones, lo que indica una conexión segura.

Bloquea números sospechosos: si recibes mensajes de texto sospechosos o correos electrónicos, bloquea el número o el correo y repórtalos como spam.

Concientiza a tu equipo y familiares: Comparte estos consejos con amigos, familiares y colegas para crear una red más consciente y menos vulnerable a los ataques.

¿Qué tan segura está tu información en la red? Mantente alerta y sigue estas recomendaciones para protegerte de los intentos de phishing y otras amenazas digitales. La prevención es clave para mantener tu información segura en un mundo cada vez más y más digital.