
# Los ataques de phishing se vuelven cada vez más engañosos

Estos se han convertido en el método más común que utilizan los actores malintencionados para atacar a las personas en el trabajo y en el hogar. Los ataques de phishing han sido tradicionalmente correos electrónicos enviados por ciberatacantes para engañarte, con el objetivo de que hagas algo que no deberías hacer, como abrir un archivo adjunto infectado en el correo electrónico, hacer clic en un enlace malicioso, o compartir tu contraseña. Si bien los ataques de phishing tradicionales continúan hoy en día, muchos ciberdelincuentes están creando correos electrónicos phishing más avanzados que son más personalizados y difíciles de detectar. También, están usando tecnologías como mensajes de texto, redes sociales o incluso llamadas telefónicas para atraerte y engañarte. Aquí están sus últimos trucos y cómo puedes detectarlos.

## Los atacantes cibernéticos realizan investigación

Los correos electrónicos de phishing solían ser más fáciles de detectar porque eran mensajes genéricos enviados a millones de personas al azar. Los ciberatacantes no tenían idea de quién sería la víctima; simplemente sabían que cuantos más correos electrónicos enviaban, más personas podían engañar. A menudo, podíamos detectar estos ataques más simples al buscar correos electrónicos extraños con "Estimado cliente" al principio, errores ortográficos o mensajes que eran demasiado buenos para ser verdad, como príncipes nigerianos ofreciendo millones de dólares.

Los atacantes de hoy son mucho más sofisticados. Ahora investigan a sus posibles víctimas para crear un ataque más personalizado. En lugar de enviar un correo electrónico de phishing a cinco millones de personas, o que parezcan correos electrónicos genéricos enviados por corporaciones, pueden enviarlo solo a cinco personas y modificar el ataque para que parezca enviado por alguien que conocemos. Los atacantes cibernéticos lo logran:

- Investigando nuestros perfiles de LinkedIn o lo que publicamos en redes sociales. También utilizando información que está disponible públicamente o que se encuentra en la Dark Web.
- Redactando mensajes que parecen provenir de la gerencia, compañeros de trabajo o proveedores que conoces y con los que trabajas.
- Aprendiendo cuáles son tus pasatiempos y enviarte un mensaje fingiendo ser alguien que comparte un interés mutuo.
- Determinando que has estado recientemente en una conferencia o que acabas de regresar de un viaje y luego redactar un correo electrónico que haga referencia a tus viajes.

Los atacantes están utilizando otros métodos para enviar los mismos mensajes, como enviar SMS o incluso llamarte directamente por teléfono.

## Cómo detectar estos ataques de phishing más sofisticados

Debido a que los atacantes cibernéticos se toman su tiempo e investigan a sus posibles víctimas, pueden ser más difícil detectar estos ataques. La buena noticia es que aún puedes detectarlos si sabes lo que estás buscando. Hazte las siguientes preguntas antes de hacer alguna acción debido a un mensaje sospechoso:

1. ¿El mensaje crea un gran sentido de urgencia? ¿Estás siendo presionado para pasar por alto las políticas de seguridad de tu organización? ¿Te están apresurando para que cometas un error? Cuanto mayor sea la presión o el sentido de urgencia, es más probable que se trate de un ataque.
2. ¿Tiene sentido el correo electrónico o el mensaje? ¿El director ejecutivo de tu empresa te enviaría un mensaje de texto urgente pidiéndote ayuda? ¿Tu supervisor realmente necesita que te apresures a comprar tarjetas de regalo? ¿Por qué tu banco o compañía de tarjeta de crédito te pediría información personal que ya debería tener sobre ti? Si el mensaje parece extraño o fuera de lugar, puede ser un ataque.
3. ¿Estás recibiendo un correo electrónico relacionado con el trabajo de un compañero de confianza o quizás de tu supervisor, pero el correo electrónico está utilizando una dirección personal como @gmail.com?
4. ¿Recibiste un correo electrónico o mensaje de alguien que conoces, pero la redacción, el tono de voz o la firma del mensaje son incorrectos e inusuales?

Si un mensaje parece extraño o sospechoso, puede ser un ataque. Si deseas confirmar si un correo electrónico o mensaje es legítimo, una opción es llamar a la persona u organización que te envió el mensaje, a un número de teléfono confiable.

Tú eres por mucho la mejor defensa. Usa el sentido común.

## Editor invitado

Phil Hoffman es un consultor de TI semiretirado con 40 años de experiencia, enfocado en infraestructura y seguridad. Es colaborador y editor desde hace mucho tiempo de OUCH! y le apasiona la tecnología, el ciclismo y la fotografía.

## Recursos

**Ingeniería social:** https://www.sans.org/newsletters/ouch/social-engineering-attacks/
**Top tres de estafas:** https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
**Smishing- Ataques a través de mensajería instantánea:** https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
**Ataques a través de llamadas telefónicas**: https://www.sans.org/newsletters/ouch/vishing/
**Inteligencia de fuentes abiertas (OSINT)**: https://www.sans.org/newsletters/ouch/search-yourself-online/

**Traducido para la comunidad por:** Célica Martínez Aponte and Iván Galindo, UNAM-CERT