

¡NO LO ABRAS!

O ¿Cómo detectar la amenaza
del phishing?

Departamento de IT

vgmedical

¿Qué es el phishing?

El *phishing* es un ataque cibernético donde los ciberdelincuentes se hacen pasar por entidades legítimas para hurtar todo tipo de información confidencial de sus víctimas a través del envío de correos electrónicos fraudulentos.

¿Cómo protegerme del phishing?

Dependiendo de la habilidad del delincuente para que el contenido del correo parezca legítimo, el *pishing* puede detectarse haciéndose las siguientes preguntas:

1) ¿Conozco a quien lo envía?

Lo primero que se debe hacer ante la recepción de un correo es reconocer al remitente. Si su nombre es absurdo, contiene caracteres inusuales o simplemente no lo recuerdas, desconfía de su contenido y ábrelo con precaución.

Ejemplo: emisores visiblemente fraudulentos podrían ser:

- reclamotuverencia@princeofafrica.net
- w1n-promo-reward@mega-lotterybig.win
- ayuda-buscando-amor@encuentratupareja.love
- pndsz00aywxfp78q@secure-mail.eu
- 8trb5upn3@verification-check.global
- no-reply@upupdate-confirm.update.ru

2) ¿Proviene de la dirección auténtica?

Este es el caso donde la dirección del correo electrónico parece empresarial. Compara el correo dudoso con uno confiable si tienes alguna relación con quien supuestamente lo envía.

Ejemplo:

alertasynotificaciones@notificacionesbancolombia.com es la dirección de los correos informativos transaccionales de Bancolombia. Sería sospechoso recibir un correo con el mismo propósito de bancolombia1234@gmail.com o alertasynotificac1ones@notificacionesbancolombia.com (¿identificaste que ésta última dirección difiere con la real en un solo carácter?).

3) ¿Es impersonal?

Las compañías usan los datos de sus usuarios para crear mensajes personalizados sobre sus productos. Una clara señal de que un correo hace parte de un mensaje masivo es el uso de saludos genéricos. **Identifica si el correo electrónico no se dirige a nadie en particular.**

Ejemplo: Los saludos que podríamos encontrar en un correo engañoso podrían ser “Estimado cliente”, “Querido usuario”, “Señor [inserta cualquier inicial de tu nombre aquí]” o simplemente “Saludos”.

4) ¿Erra en la escritura?

Las comunicaciones provenientes de entidades oficiales suelen escribirse correctamente y tener una estructura clara. Una gran ventaja que tienen los usuarios es ser conscientes de que algunos ciberdelincuentes no se esforzarán por escribir de manera pulcra. **Revisa minuciosamente el correo en busca de faltas de ortografía y errores gramaticales.**

Ejemplo: un correo electrónico con el mensaje “su cuenta bancaria sera bloqueada por razones de seguridad” probablemente no sería escrito por una entidad bancaria.

5) ¿Solicita datos sensibles?

Actualmente las empresas instan a sus usuarios a realizar todo tipo de operaciones por medio de sus aplicaciones y páginas web. Detecta si el correo desea confirmar tu información por medio de canales no oficiales.

Ejemplo: El texto “Complete el formulario con sus datos personales y las credenciales de su cuenta” podría hacer parte de un correo de estafa. Además de proveer datos personales con prudencia, bajo ninguna circunstancia se deben revelar a nadie usuarios, contraseñas, imágenes de seguridad, códigos de verificación, claves dinámicas o cualquier tipo de dato en tarjetas débito o crédito.

6) ¿Contiene enlaces inseguros?

Muchos correos seguros contienen enlaces a sitios web de internet; sin embargo, un signo de alarma de un correo malicioso es la presencia de enlaces acortados que dirigen a sitios web fraudulentos.

Utiliza herramientas confiables para detectar malware en cualquier enlace antes de abrirlo.

Ejemplo: Un enlace seguro podría verse como <https://banco-oficial.com/inicio>; un enlace acortado podría parecerse a <https://bit.ly/abc1234> (oculta el verdadero sitio al que dirige).


7) ¿Adjunta archivos maliciosos?

Un correo no es necesariamente malicioso por contener archivos adjuntos, no obstante, si estos resultan irreconocibles o con nombres extraños, podrías estar expuesto a un correo falso. Se recomienda no descargar ni abrir ningún archivo de correos desconocidos.

Ejemplo: cualquier archivo, desde una imagen hasta un documento de la suite Office, puede contener código malicioso. Ten mucha más precaución ante archivos ejecutables como .exe, .bat, .com, .scr, .msi y archivos de programación como .js, .vbs, .ps1, .sh.

8) ¿Genera urgencia?

El contenido de correos oficiales suele ser pertinente y no apelar a las emociones (a excepción de ciertos correos de carácter comercial y/o promocional). **Analiza el verdadero propósito del correo electrónico; si infunde alarma o temor para que comprometas tus datos, no confíes en su legitimidad.**

Ejemplo: Un correo no confiable podría tener el asunto y contenido de “ ADVERTENCIA ¡Cuenta bancaria bloqueada!”, “Detectamos actividad sospecha en su cuenta bancaria. Es necesario que actualice su información dentro 24 horas o su cuenta será suspendida indefinidamente”.

9) ¿Tiene un formato usual?

La automatización ha permitido que las marcas envíen todo tipo de correos con un formato propio y común; tipografías, logotipos y otros elementos constituyen la identidad visual de la marca. **Observa atentamente si la disposición de texto, colores e imágenes parece sobrecargada, demasiado simple o falsificada.**

Ejemplo: muchos correos fraudulentos contienen solamente texto sin formato; algunos pretenden ser de una marca pero son visiblemente diferentes; otros usan demasiados colores o emojis; los más difíciles de detectar presentan plantillas parecidas a las originales pero con enlaces y archivos maliciosos.