

# Phishing: No muerda el anzuelo

El phishing se produce cuando usted recibe emails, mensajes de texto o llamadas de teléfono que parecen provenir de compañías o gente que conoce. Pero en realidad provienen de los estafadores. Ellos quieren que haga clic en un enlace o que les dé información personal (como una contraseña) para poder robarle su dinero o su identidad, y tal vez para acceder a su computadora.



## La carnada



Los estafadores usan nombres de compañías que suenan familiares o se hacen pasar por alguien que usted conoce.



Le piden que haga clic en un enlace o que les dé contraseñas o números de cuentas bancarias. Si usted hace clic en el enlace, le pueden instalar programas que le impiden acceder a su computadora y robarle su información personal.



Lo presionan para que actúe de inmediato, o de lo contrario, le sucederá algo malo.

## Evite morder el anzuelo



### Verifíquelo.

- » Busque el sitio web o número de teléfono de la compañía o persona que se está comunicando con usted.
- » Llame directamente a la compañía o a la persona. Use un número que le conste que es el correcto, no llame al número de teléfono que aparezca en el email o mensaje de texto.
- » Cuénteles sobre el mensaje que recibió.

### Busque indicios de estafa.

- » Usted no tiene una cuenta en esa compañía.
- » Al mensaje le falta su nombre o tiene errores de gramática u ortografía.
- » La persona le pide información personal, incluidas contraseñas.
- » **Pero tenga en cuenta que algunos esquemas de phishing son sofisticados y parecen muy reales, así que verifíquelo y protéjase.**



### Protéjase.

- » Mantenga actualizada la seguridad de su computadora y haga copias de seguridad de sus datos con frecuencia.
- » Considere usar la autenticación de múltiples factores para las cuentas que le ofrezcan este sistema: un segundo paso para verificar quién es, como un mensaje de texto con un código.
- » Cambie de inmediato cualquier contraseña comprometida y no las use para ninguna otra cuenta.



## Reporte el phishing

- » Reenvíe los emails phishing a [spam@uce.gov](mailto:spam@uce.gov) y [reportphishing@apwg.org](mailto:reportphishing@apwg.org).
- » Repórtelo ante la FTC en [ftc.gov/queja](http://ftc.gov/queja).



Para más información, visite [ftc.gov/phishing](http://ftc.gov/phishing)  
[aba.com/phishing](http://aba.com/phishing)

