Cómo detectar los correos fraudulentos

Los estafadores confían en la curiosidad de la víctima para que haga clic o descargue algo peligroso. Piénsalo dos veces antes de descargar algo en internet, especialmente si se trata de un archivo adjunto de un remitente anónimo.

Fecha de la publicación:
19 de julio de 2021

¿De qué se trata el Phishing o pesca de información?

Los estafadores se hacen pasar por alguien que conoces para engañarte para que compartas tus datos personales. Estos utilizan esta información para acceder a tus cuentas. Los correos electrónicos y mensajes de texto phishing pueden parecer originar de una empresa que conoces o en la que confías. Ejemplos de correos phishing:

- Un correo que se hace pasar por una agencia estatal de Colorado, y que te pide que confirmes la información de tu cuenta de beneficios.
- Un correo que finge ser de una compañía de seguro médico y que te pide que confirmes tu número de Seguro Social.
- Un correo que parece provenir de un sitio web conocido para compartir documentos, y que te pide que colabores en un documento e ingreses tus credenciales de acceso.
- Un correo que intenta hacerse pasar por un software antivirus, y que te pide que ingreses tus datos para evitar un virus.
- Un correo electrónico de una compañía de tarjetas de crédito o de un banco que te pide que tomes medidas inmediatas sobre una factura sin pagar y que ingreses tus datos.

¿Cómo te pueden perjudicar las estafas de phishing?

En cada una de las situaciones anteriores el estafador te pedirá que hagas clic en un enlace o que ingreses tus datos personales. Te pueden perjudicar de las siguientes maneras:

- **Pueden poner tus cuentas en riesgo.** Si ingresas tu número de tarjeta de crédito, credenciales de acceso, número de Seguro Social u otra información en un enlace sospechoso, esa información ya no está segura. Si utilizas las mismas contraseñas para varias cuentas, debes cambiar las contraseñas para todas esas cuentas.
- **Robo de identidad.** Una vez que un estafador tenga acceso a tus datos personales, se puede hacer pasar por ti, obtener tu crédito, abrir cuentas o utilizar tu información sin autorización.
- **Programas maliciosos en tu dispositivo.** Si un hacker logra engañarte para que ingreses tus credenciales de acceso, él puede infectar tu sistema, bloquear tus archivos y exigir un pago para devolverlos.

¿Qué debes hacer si un correo parece sospechoso?

- **Confirma la identidad del remitente.** Pasa el ratón o indice por encima del nombre del remitente para confirmar que la dirección de correo electrónico es correcta. Si conoces al remitente, pero sigues sospechando, comunícate con él por otro medio, cómo una llamada telefónica, para confirmar que el remitente es realmente quien envió el correo.
- **Confirma que el enlace es lo que dice ser.** Pasa el ratón o indice por encima de los hipervínculos para confirmar que te dirigen a un sitio web conocido y fiable.
- **Busca errores tipográficos o inexactitudes en el correo.** Examina la dirección de correo electrónico, la dirección URL y la ortografía utilizada en cualquier correspondencia y que el contexto tenga sentido.
- **Configura la autenticación de dos factores.** Utiliza contraseñas seguras y no utilices nunca la misma contraseña en varias cuentas. Hay muchos programas o aplicaciones de contraseñas que te pueden ayudar a llevar un control de tus contraseñas.

¿Es el correo electrónico sospechoso?

Alto riesgo

Un correo que proviene de alguien que no conoces con un adjunto o enlace que no esperabas.

Riesgo moderado

Un correo que proviene de alguien que conoces con un adjunto o enlace que no estabas esperando.

Bajo riesgo

Un correo que proviene de alguien que conoces y que contiene un adjunto o enlace que estabas esperando.

Si notas cualquier estafa, fraude, aumento abusivo de precios, u otros intentos para aprovecharse de los residentes de Colorado, comunícate con No Más Fraude Colorado al 800-222-4444 o visita www.NoMasFraudeColorado.gov.