¡No se deje atrapar por el phishing!

Phishing es el delito de engañar a las personas para que compartan información confidencial. Existe más de una forma de atrapar a una víctima.

Dentro de las más comunes consiste en que las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita o suplanta la identidad de una persona u organización de confianza, un banco o una entidad gubernamental.

Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado en asustarle, con la intención de confundir e infundir miedo.

El mensaje solicita ir a un sitio web y al hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña, la información de inicio de sesión llega al atacante, que la utiliza para robar

identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

¿Cómo reconocer el *phishing?*

Los estafadores suelen actualizar sus tácticas, pero hay algunos indicios que lo ayudarán a reconocer un email o mensaje de texto tipo phishing.
Los mensajes podrían:

- Indicar que se ha detectado alguna actividad sospechosa o intentos de inicio de sesión.
- Afirmar que hay un problema con su cuenta o con su información de pago.
- Decir que debe confirmar algunos datos personales.
- Incluir un documento falso.
- Pedirle que haga clic en un enlace para hacer un pago.
- Decir que usted es elegible para registrarse para recibir un reembolso del gobierno.
- Ofrecerle un cupón para algo gratis.

Recomendaciones

1. Evite el correo basura (*spam*) ya que es el principal medio de distribución de mensajes engañosos.

   Los mensajes de phishing se distribuyen mediante el correo electrónico de la misma forma que los mensajes de correo normales, por lo cual toda acción que contribuya a disminuir el *spam* que se recibe, contribuirá también en reducir los mensajes de *phishing*.

2. Findeter nunca le solicitará datos confidenciales por correo electrónico, teléfono ni solicitando el ingreso de alguna clase de datos.

3. Verifique la fuente de la información: No conteste correos que soliciten información personal o financiera. Si duda, comuníquese telefónicamente con Findeter mediante los números de contacto que

están disponibles en nuestro sitio web (no llame a los números que aparecen en el mensaje recibido).

4. Si el correo electrónico contiene un enlace a un sitio web, escriba usted mismo la dirección en su navegador de Internet, en lugar de hacer clic en el enlace.

De esta forma podrá estar seguro de que está ingresando al sitio real de la empresa o entidad y que no está siendo redirigido a un sitio falso.

Adicionalmente, si el sitio le solicita información personal, verifique que el envió y la recepción de datos se realiza sobre un canal seguro (la dirección web debe comenzar con https:// y debe aparecer un pequeño candado cerrado en la pantalla del navegador.