¿Cómo reconocer la existencia de correos de phishing?

Los correos fraudulentos son una amenaza a la que tienen que hacer frente los usuarios de Internet a diario. Cada vez son más las personas que hacen pedidos cómodamente por Internet o que realizan transacciones bancarias online, por lo que el correo electrónico sigue siendo, a este respecto, el medio de comunicación online más importante. Los timadores aprovechan estas circunstancias para inmiscuirse en la comunicación electrónica con **información fraudulenta** utilizando enlaces (que suelen redirigir a páginas web falsas) y direcciones sospechosos que tienen como objetivo los datos de los usuarios más ingenuos. En la presente guía te ofrecemos información acerca de cómo protegerte del **robo de datos**.

¿Qué es el phishing?

El término phishing hace referencia a un método de estafa por el cual un remitente de correo electrónico se hace pasar por otro para acceder a los datos relativos a su cuenta y a su identificación sin que la víctima tenga ninguna sospecha. La palabra, que procede del inglés y que originariamente significa “pescar”, se basa en un principio similar a lo que describe: en el fenómeno del phishing, los estafadores emplean correos electrónicos fraudulentos como anzuelo para “pescar” contraseñas. La grafía “ph” procede del vocabulario que usan los hackers.

¿Cómo funciona?

Se envían supuestos correos electrónicos relativos a bancos, servicios de pago, mercados online o proveedores de servicios de eCommerce, para no crear ninguna sospecha al respecto, donde solicita rellenar formularios de correo electrónico o a hacer clic en un enlace que redirige a una página de registro falsa o indica que trae un archivo adjunto que es importante para el usuario, soliciatando en estos revelar **datos sensibles**. El objetivo de dichos ataques de phishing es conseguir **nombres de usuario**, **contraseñas** o **códigos PIN** y efectuar reservas y pedidos en nombre de sus propietarios. Las víctimas de estos ataques pueden saber si sus cuentas bancarias o sus cuentas de servicios de pago han sido blanco de este ataques si ven reflejadas en dichas cuentas la realización de compras o transferencias sin su conocimiento.

¿Cómo detectar este tipo de correos?

Una manera de reconocer el phishing es por medio de **indicios evidentes**, como por ejemplo, un remitente desconocido, un tratamiento impersonal, faltas de ortografía, enlaces dudosos y formularios online.

- **Remitente:** lo primero que debes tener en cuenta antes de abrir un supuesto correo electrónico oficial de tu banco o de un proveedor de servicios online es reconocer quién es el remitente. En este sentido, puedes plantearte varias preguntas: ¿quién ha enviado el correo?, ¿mantienes una relación comercial con el proveedor?, ¿le has facilitado tu correo electrónico? Observa cuál es la dirección completa del remitente y compárala con los mensajes anteriores. Si encuentras contradicciones, es conveniente que tengas cuidado.

- **Conteido:** el texto del correo electrónico es otro indicio que pone al descubierto mensajes dudosos. Los proveedores de servicios que se dirigen a sus clientes emplean, por lo

general, un tono personal y le llaman por su nombre. En el caso de los timadores, esto no ocurre siempre así. Si un mensaje empieza con “Estimados señores y señoras” o con cualquier otro tipo de fórmula de cortesía estándar, deberías preguntarte por qué tu banco o un supuesto socio comercial no sabe cómo te llamas.

- **Ortografía y gramática:** si uno de los mensajes de tu bandeja de correo electrónico está lleno de errores gramaticales y ortográficos, esto indica con total seguridad que no se trata de un error de uno de los trabajadores de tu banco. Las faltas de ortografía y textos no coherentes o con mala gramatica son un claro indicio de correos fraudulentos o phishing ya que estos emails se han escrito en otro idioma y se han traducido automáticamente. Lo mismo ocurre con los textos de correos electrónicos que no contienen acentos o diéresis o sí incluyen caracteres en otros idiomas.

- **Enlaces:** si un correo electrónico contiene un enlace, esto no tiene por qué constituir, *a priori*, un factor negativo. Sin embargo, antes de hacer clic en él, debes cerciorarte de que este te lleva a una página seria. Para ello, mueve el ratón por encima del texto que contiene el enlace y comprueba cuál es la dirección web que se muestra en la parte inferior izquierda en la ventana del navegador. ¿Se asemeja al URL del proveedor? ¿Contiene características de seguridad como HTTPS para una transmisión de datos segura? En caso de dudas, es recomendable no hacer clic sobre el enlace ni tampoco escribir manualmente la dirección en el navegador.

- **Introducción de datos:** no hay ningún proveedor online que exija a sus clientes la introducción de datos por medio del correo electrónico. Recibir un formulario en formato HTML en el que haya que introducir los datos de identificación así como las contraseñas es un claro indicio de que se trata de un correo electrónico de phishing. Asimismo, tampoco es conveniente facilitar ningún código de seguridad como el código PIN por teléfono o por correo electrónico. Lo recomendable es facilitar este tipo de datos a través de las páginas de los proveedores, cuya autenticidad puede comprobarse por medio de certificados de seguridad.

- **Archivos adjuntos:** hay que actuar con escepticismo cuando se reciben mensajes inesperados que contienen archivos adjuntos. En este sentido, la regla fundamental es que si se desconoce al remitente, lo mejor es no descargar dichos archivos, ya que estos pueden contener software malintencionado, como, por ejemplo, virus o troyanos, que puede infectar tu ordenador y leer datos sensibles, por lo que ya no sería posible comprar en Internet ni hacer uso de servicios bancarios online de manera segura.

¿Cómo reconocer la existencia de correos de phishing?

¿Qué medidas se pueden adoptar en caso de recibir correos de phishing?

- Este alerta a cualquier correo inesperado, mensajería instantánea, correo de voz o fax que dice ser de un banco, tarjeta de crédito o tienda en línea con quien usted tiene una cuenta. En el caso de que usted reciba un mensaje de este tipo, es una buena idea llamar primero al número de servicio al cliente de su banco o tarjeta de crédito (pero no el número que aparece en el mensaje) y verificar si el mensaje es legítimo.
- No responda a ningún correo electrónico, teléfono o fax, que le solicite divulgar su información personal.
- No haga click en ningún enlace o correo electrónico sospechoso. Al hacer click en un vínculo de este tipo puede causar la descarga de la clave de registro o software "spyware" en su computadora.
- Utilice un antivirus actualizado.
- Tenga su sistema operativo actualizado.