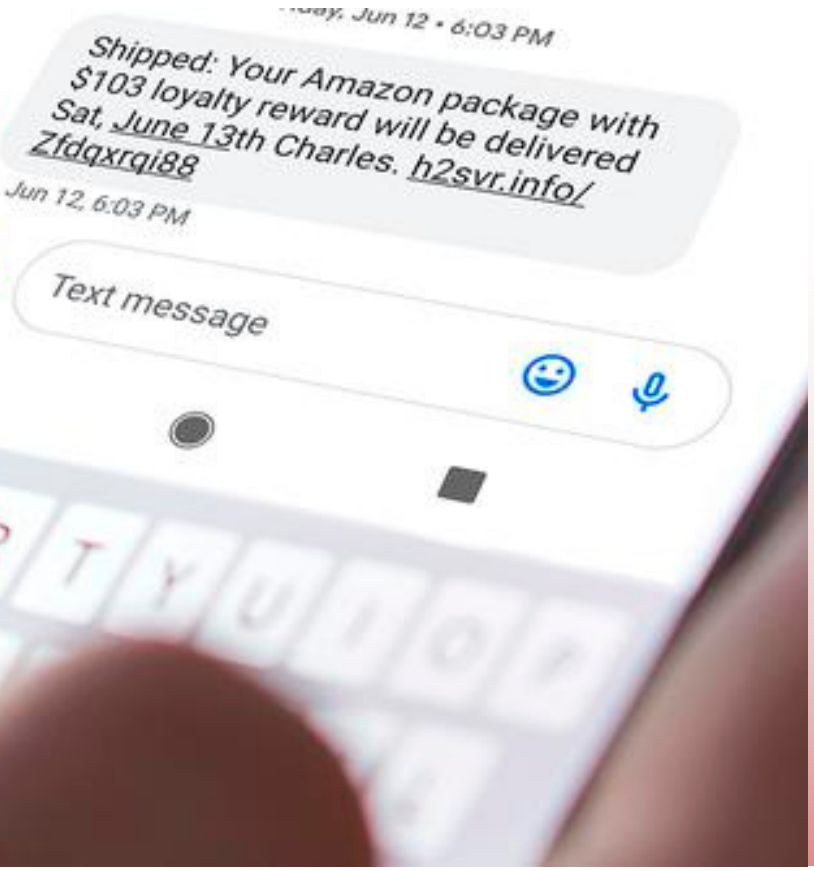
¿QUE ES EL SMISHING?

IMG



¿Que es el SMISHING?

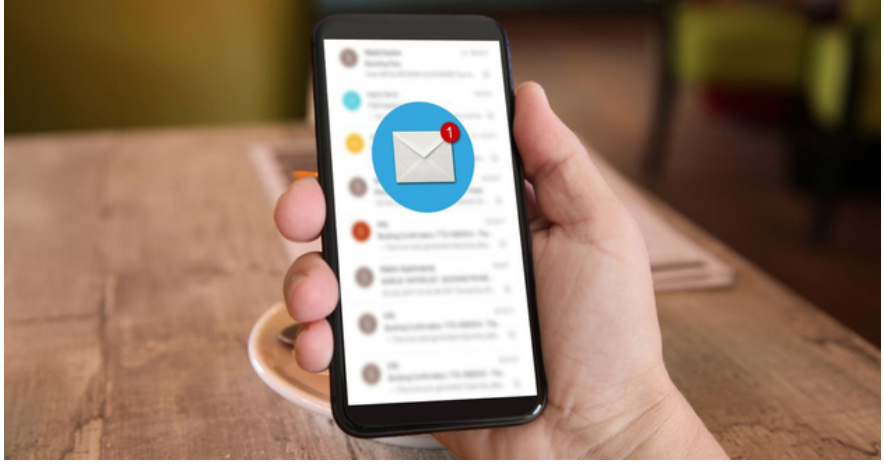
Este fenómeno preocupante se conoce más comúnmente como smishing, que proviene de las palabras SMS y phishing . La palabra SMS es un acrónimo de servicio de mensajes cortos (simplemente conocido como mensajería de texto). El phishing es un tipo de estafa en línea que utiliza mensajes, como correos electrónicos, así como enlaces maliciosos y archivos adjuntos de correo electrónico. El objetivo del phishing es hacer que alguien revele sus datos personales e información, como contraseñas, identificación personal o detalles financieros, incluidos los números de cuentas bancarias.

S M I S H I N G

Esto lo hace el remitente actuando como una entidad confiable, como el banco del destinatario, un servicio de redes sociales o alguna autoridad en la que confíe el receptor del mensaje.

El estafador puede intentar acceder al banco en línea, correo electrónico u otro servicio de la víctima que puede abrir puertas a otros lugares.

Al ganarse la confianza de la víctima, el objetivo del phishing es obtener ganancias financieras.



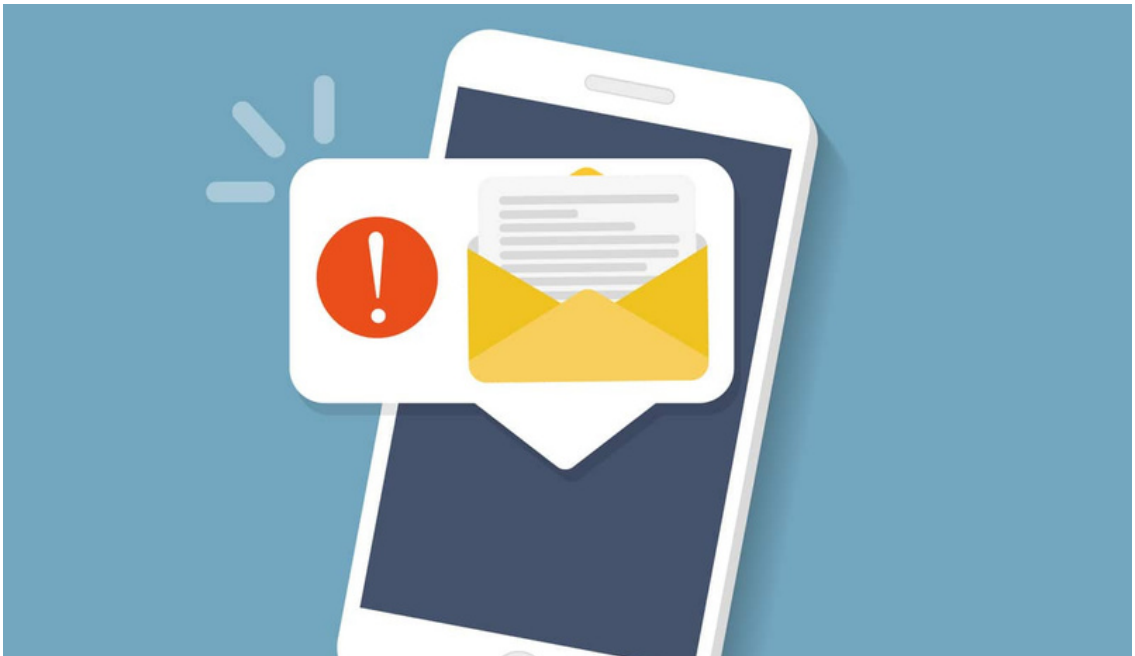
¿En qué se diferencia el Smishing del Phishing?

Entonces, ¿en qué se diferencia el smishing del phishing? Aunque el objetivo del smishing no difiere del phishing, los medios para robar su información personal o financiera e infectar su computadora de escritorio o dispositivos móviles son diferentes. Mientras que el phishing se refiere a los delitos en línea realizados por correo electrónico, los ataques de smishing utilizan un teléfono móvil o algún otro dispositivo móvil y mensajes de texto para atraer a la víctima. En otras palabras, smishing es solo una forma de phishing realizada a través de mensajes de texto.

Un mensaje de smishing podría tener más éxito para engañar a su víctima que un correo electrónico de phishing porque muchos no consideran que los mensajes de texto sean una amenaza para su seguridad y privacidad. Sin embargo, esto está lejos de la verdad. Además de los mensajes de texto habituales, los servicios de mensajería como WhatsApp tampoco son seguros cuando se trata de robar datos confidenciales, detalles de inicio de sesión y otra información personal.

IMG

Incluso las cadenas de mensajes existentes pueden suponer un riesgo de smishing. Los delincuentes pueden inyectar mensajes smishing en cadenas de mensajes antiguos que la víctima ha iniciado con el remitente real . En un caso como este, el smishing se puede realizar en nombre de una fuente conocida y confiable, como el servicio postal o una empresa de entrega. El mensaje de smishing se convertirá en parte de la cadena de mensajes anterior, entre otros mensajes que la víctima haya recibido anteriormente. Esto puede ser muy engañoso y hacer que la gente caiga en la trampa, especialmente si el SMS de smishing se parece a los otros mensajes.



¿Cómo identificar los mensajes de SMISHING?

En cuanto a los correos electrónicos de phishing y otros mensajes de estafa, un mensaje de smishing se puede identificar buscando ciertos signos en el mensaje en sí, así como en su remitente.

El mensaje puede provenir de su banco, por ejemplo, o de un servicio de redes sociales que utiliza.

Es que los mensajes de texto tienen menos opciones cuando se trata de imágenes, como logotipos, formato y colores. Mientras que un correo electrónico de phishing puede identificarse como falso simplemente mirando su estilo visual, un mensaje SMS solo tiene texto para usar.

Puede disfrazarse como una notificación de un paquete enviado o recibido que, supuestamente, ordenó.

Puede decirle que ha ganado una lotería o algún otro premio que está esperando a ser recogido por su afortunado ganador.

¿Cómo se puede usar el SMISHING para robar información personal o financiera?

El phishing por SMS, al igual que el phishing normal por correo electrónico, utiliza enlaces que lo dirigen a un sitio web. Sin embargo, al hacer clic en el hipervínculo en un mensaje de smishing, a menudo lo lleva a un sitio web que está diseñado para parecerse al sitio web real del supuesto remitente.

El enlace en un mensaje de smishing también puede llevarlo a una página de inicio de sesión que se parece a la de una fuente conocida y confiable. Por ejemplo, los mensajes de smishing se pueden enviar en nombre de servicios de redes sociales, bancos o empresas de entrega. Sin embargo, en lugar de iniciar sesión , al insertar un nombre de usuario y una contraseña, la víctima está regalando sus credenciales de inicio de sesión. Estos se utilizan luego para acceder a su cuenta bancaria y correo electrónico o recopilar información personal.

¿Cómo protegerse contra los ataques de SMISHING?

Es aconsejable tener cuidado al hacer clic en los enlaces que provienen de remitentes cuya autenticidad y confiabilidad no puede verificar. Después de que la víctima haya hecho clic en un enlace en un mensaje de Smishing e ingresado a un sitio falso, los medios para robar su información son similares a los de un fraude de phishing.

Tenga también en cuenta los mensajes no solicitados que se le envían en una aplicación de mensajería como WhatsApp y Facebook Messenger. Estas plataformas son otra herramienta popular para atraer a las víctimas para que revelen su información confidencial.

Esto puede parecer que ya no puede confiar en ningún SMS, mensaje instantáneo o correo electrónico. Por suerte, hay una forma infalible de evitar que te conviertas en víctima de un ataque de Smishing. Es decir: no hagas nada que te pida un mensaje sospechoso.

Leer un mensaje de smishing por sí solo no se puede utilizar para robar su información. Sin embargo, hacer clic en un enlace en un mensaje de texto malicioso o enviar su información personal o financiera como respuesta puede usarse para obtener ganancias financieras, robo de identidad y muchos otros delitos.

PARA MÁS INFORMACIÓN CONTÁCTANOS EN NUESTRAS REDES SOCIALES

IMAGENTI

IMG