PRINSOTEL

Recomendaciones actuación a nuestros clientes tras el ciberataque sufrido el 16 de mayo de 2024

Como consecuencia del ataque sufrido, es nuestra obligación darles algunas pautas para garantizar la seguridad de sus datos personales:

1. **Nunca** y bajo ningún concepto, le pediremos sus datos bancarios por medios electrónicos. Si reciben una llamada o mensaje solicitando este tipo de datos, no los compartan NUNCA.

2. En caso de recibir publicidad PRINSOTEL por correo electrónico, por SMS, o redes sociales **verifique siempre la identidad** del remitente y, en caso de duda, nunca haga clic en ningún enlace en el que no confíe.

3. **Desconfíe de llamadas en nuestro nombre** o desde cualquiera de nuestros hoteles. Verifique que se trata de una llamada desde un operador conocido y de nuevo, nunca aporte datos privados.

Adicionalmente, nos gustaría, a través del presente documento prevenirle de todos los posibles intentos de fraude como consecuencia del incidente como Phising, Spear Phising, Vishing, Smising, Pharming, Whaling …etc. con el fin de que puedan estar atentos a cualquiera de estas maliciosas acciones.

A continuación, se detallan este tipo de ataques o fraudes para que puedan identificar cualquier conducta anómala y puedan prevenir cualquiera de estas acciones:

- ***Phising:*** El phishing es una técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario. A través de un enlace incluido en el email, intentan redirigirlo a una página web fraudulenta para que introduzca su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca online, etc.

  Estos correos electrónicos fraudulentos suelen incluir el logotipo o la imagen de marca de la entidad, pueden contener errores gramaticales y en ocasiones intentan transmitir urgencia y miedo para que el usuario realice las acciones que le solicitan.
  Un email de tipo phishing también puede llevar un archivo adjunto infectado con software malicioso. El objetivo de este malware es infectar el equipo del usuario y robar su información confidencial.

- ***Spear Phising:*** Los atacantes crean correos electrónicos, páginas web e incluso mensajes cortos de carácter falso que parecen auténticos y que solicitan información de inicio de sesión de los usuarios. Es así como los estafadores se hacen con los datos de acceso para tiendas online, redes sociales o espacios de almacenamiento en la nube. En el peor de los casos, se hacen incluso con información bancaria o datos de la tarjeta de crédito. Los estafadores saben que hay muchos usuarios que no se toman en serio la seguridad de las contraseñas y que usan una misma contraseña para diferentes servicios. De esta forma, con una página web de phishing sencilla se pueden obtener datos sensibles, información que tiene un alto valor económico en el mercado negro digital.

- ***Vishing:*** El término vishing es una combinación de las palabras voice (voz) y phishing, por lo que también se denomina en ocasiones voice phishing. Con esta técnica, los atacantes usan la tecnología VoIP (voz sobre IP) para realizar de forma asequible o

gratuita numerosas llamadas fraudulentas y conseguir así códigos, contraseñas o datos bancarios de la víctima, que no suele sospechar nada.

- ***Smising:*** El término smishing surge de unir los elementos SMS y phishing. De manera similar al phishing, los ciberdelincuentes que envían estos mensajes se hacen pasar por representantes de una empresa u organización fiable, solo que, en lugar de correos electrónicos, utilizan SMS (Short Message Service). Estos mensajes de móvil sirven, o bien para instar a la víctima a revelar datos de su cuenta, o bien para instalar malware y troyanos en su dispositivo sin que se percate.

- ***Pharming:*** El pharming, una combinación de las palabras "phishing" y "farming", es una estafa en línea similar al phishing, en la que se manipula el tráfico de un sitio web y se roba información confidencial. Este es un tipo de ciberataque de ingeniería social en el que los delincuentes redirigen a los usuarios que intentan acceder a un sitio web específico a un sitio diferente y falso. Estos sitios "falsos" pretenden capturar la información de identificación personal de la víctima y sus credenciales de inicio de sesión, como contraseñas, números de la seguridad social, números de cuenta, etc. o bien intentan instalar malware de pharming en su equipo.

- ***Whaling:*** Un ataque de whaling es un método que usan los cibercriminales para simular ocupar cargos de nivel superior en una organización y así atacar directamente a los altos ejecutivos u otras personas importantes dentro de ella, con el objeto de robar dinero, conseguir información confidencial u obtener acceso a sus sistemas informáticos con fines delictivos. El whaling, también conocido como CEO fraud, es similar al phishing en cuanto a que usa métodos, como la suplantación de sitios web y correos electrónicos, para engañar a la víctima y hacer que revele información confidencial o haga transferencias de dinero, entre otras acciones.

Lamentamos mucho esta situación que nos ha sobrevenido, pero sepa que para nosotros su tranquilidad es lo primero y hemos atajado y contenido esta situación de una forma rápida y eficaz.

Prinsotel ya se encuentra trabajando en el plan de acción generado tras el incidente y, en concreto, en la implantación de medidas de seguridad reforzadas para evitar situaciones similares en el futuro.
