HORNETSECURITY

INFOPAPER:
DETECTA PHISHING Y TOMA MEDIDAS

Contenido

¿QUÉ ES EL PHISHING?

El phishing es una forma de fraude, en que a la víctima se le envía un correo electrónico falso que, normalmente, no se reconoce como tal. El atacante usa **phishing para engañar al destinatario para que revele datos confidenciales.** Esto incluye datos personales y contraseñas.

La Oficina Federal de Seguridad de la Información estima que el daño económico de los ataques cibernéticos, que comienzan con ataques de phishing dirigidos, asciende a millones de dígitos al año. Para los usuarios, hay **varios riesgos** eso puede variar según el motivo del atacante. Por ejemplo, los datos robados se utilizan para el robo de cuentas u otros ataques de hackers a las empresas. **El método común utilizado para el phishing es el envío masivo de correos electrónicos con contenido falso.**

Pero los ataques dirigidos también se están volviendo cada vez más populares: en el spear phishing, los atacantes investigan a sus víctimas por adelantado. Fingen conocer a sus víctimas personalmente, tratando de ganarse su confianza y así obtener datos valiosos.

¿Cómo reconozco un correo electrónico de phishing?

No suele ser fácil reconocer un correo electrónico de phishing diseñado por un ciberdelincuente, pero tampoco es imposible. Los **siguientes puntos fueron desarrollados junto con los expertos del Security Lab de Hornetsecurity** y ayudan a identificar correos electrónicos de phishing en función de diferentes características.

Remitente

A menudo los ciberdelincuentes escriben **en nombre de tiendas on line, como Amazon y eBay, o de plataformas de banca on line, como PayPal.** La vista detallada de la dirección de correo electrónico puede proporcionar información sobre el verdadero origen del mensaje.

Si no es creíble o contiene caracteres mal escritos o números cifrados, esto sería una señal de advertencia. **Un ejemplo: noreply@amzon.com en lugar de noreply@amazon.com.** Mientras tanto, las direcciones de los remitentes son completamente falsas, por ello, los correos deben verificarse para tener en cuenta otras características de phishing. El Security Lab también recomienda **comprobar el encabezado del correo electrónico** para obtener información detallada sobre el mensaje.

Información que contiene el origen del correo electrónico, se puede encontrar en el **remitente.** Estos documentan todos los servidores y hosts a través de los cuales pasa el correo electrónico. Como regla, puedes ver la vista detallada del encabezado en el programa de correo electrónico en "Ver" o en "Opciones".

Receptor

Además del remitente, el destinatario también puede proporcionar información sobre la fiabilidad de un correo electrónico. Por ejemplo, si un usuario ha iniciado sesión en PayPal con una cuenta de Google Mail, pero ha recibido un correo electrónico de PayPal a una dirección de yahoo, puede ser phishing. Por supuesto, esto es solo un indicador de si el usuario también está utilizando varias direcciones de correo electrónico.

Saludo

En las campañas de phishing a gran escala, los ciberdelincuentes envían sus mensajes falsos a cientos, a veces miles de destinatarios. A menudo, **la dirección correcta del destinatario se queda por el camino.** Especialmente cuando un supuesto socio contractual de repente ya no sabe el nombre del destinatario y usa **saludos generales** en este caso, se recomienda precaución.

Diseño, ortografía y gramática.

Los ciberdelincuentes del extranjero a menudo usan programas de corrección ortográfica para escribir sus correos electrónicos falsos. Dependiendo de la complejidad de los temas y oraciones, suelen tener errores más o menos serios. La puntuación también juega un papel en el reconocimiento de un correo electrónico de phishing: además de **las comillas y guiones fuera de lugar, los caracteres extranjeros también pueden aparecer en un correo electrónico falso.** Los expertos del Security Lab de Hornetsecurity también recomiendan prestar atención a la **calidad del diseño** del correo electrónico. A menudo, los errores gráficos indican un ataque de phishing.

Presión psicológica

Los **esfuerzos por presionar a la víctima** juegan un papel crucial en la composición de los correos electrónicos de phishing. Los ciberdelincuentes ejercen presión sobre el destinatario de un correo electrónico para que el "pensamiento crítico" no funcione.

A menudo, el **destinatario está amenazado** con graves consecuencias y sanciones sin no hace nada, lo que hace que la víctima actúe de manera rápida y precipitada. Que el hacker conozca tantos detalles hace que la víctima crea al remitente. Un ejemplo de esto es el truco de "sextortion". El ciberdelincuente finge estar en posesión de imágenes de vídeo que han sido pirateadas. Incluso afirmando que se usó la webcam de la víctima durante actos sexuales o similares. Para demostrar que el cibercriminal realmente hackeó la computadora de la víctima, a veces **se enumeran las contraseñas correctas**, aunque estos casos provienen de antiguas filtraciones de datos.

Los ciberdelincuentes chantajean a sus víctimas con estas grabaciones y les piden que hagan un pago, generalmente en forma de Bitcoins u otras criptomonedas.

Enlaces, páginas de phishing y archivos adjuntos

Los ciberdelincuentes a menudo intentan que el destinatario abra una URL. El **usuario desprevenido es dirigido a un sitio web falso donde ingresa datos personales** y sin saberlo los comparte con el hacker. Para identificar enlaces dañados o falsos, es importante verificar, entre otras cosas, si el enlace coincide con el remitente que lo envió.

Se debe prestar especial atención a: enlaces que contienen números y al nombre de la institución respectiva. Algunos enlaces se esconden detrás de una URL que parece de confiaza. Para ver el destino real del enlace, los usuarios pueden pasar el ratón sobre la URL sin hacer clic en ella para leer el texto que aparece en la pantalla. **texto emergente muestra la URL de destino completa.** Los ciberdelincuentes a menudo usan subdominios y una extensión del enlace con caracteres adicionales para ocultar el verdadero dominio al que se dirige realmente el usuario. A menudo es difícil saber si un sitio web es verdadero o falso.

La abreviatura https:// alguna vez se consideró un signo de una conexión segura, pero esto solo significa que el operador del sitio web ha adquirido un certificado SSL. **Los ciberdelincuentes también pueden adquirir este certificado** para su sitio web, por lo que la abreviatura no significa necesariamente que se haya otorgado la autorización completa. Sin embargo, una indicación de un sitio web de phishing podría ser la solicitud de un número de transacción sin que se haya realizado una transacción previa.

Enlaces, páginas de phishing y archivos adjuntos

También se recomienda precaución si, por ejemplo, después de iniciar sesión a través de banca online, **se deben ingresar datos que realmente se conocen, como el nombre y la dirección o el IBAN.** Si uno no está seguro de si la URL proporcionada en el correo electrónico realmente conduce al sitio web correcto, los usuarios deben usar la dirección del sitio web que conocen directamente en el navegador e ingresar los datos de la cuenta allí. Los archivos adjuntos de correo electrónico también pueden conllevar riesgos. Los hackers a menudo usan archivos adjuntos maliciosos, especialmente cuando atacan a las empresas. Ellos envían **supuestos extractos de cuenta de facturas o cartas comerciales en formatos como * .xls, * .doc o * .pdf.**

Contienen troyanos, que registran las entradas de datos y transmiten la información al ciberdelincuente. Antes de abrir un archivo adjunto, el destinatario del mensaje siempre debe verificar al remitente, por ejemplo, con la vista detallada del encabezado del correo electrónico (Capítulo: Remitente) o por teléfono.

Solicitud de datos confidenciales.

Los usuarios deben estar particularmente atentos cuando se trata de **correos electrónicos provenientes de empresas del sector financiero.** Si un correo electrónico solicita información personal o números secretos y contraseñas, esto es una indicación de phishing. Los bancos serios generalmente solicitan datos confidenciales, como números PIN, por carta.

MEDIDAS DE SEGURIDAD

Para protegerse contra ataques de phishing, los usuarios pueden tomar algunas precauciones de seguridad que pueden proteger las cuentas en caso de emergencia. Incluso después de que un usuario haya sido víctima de un ataque, tomar las precauciones correctas no solo puede servir para limitar el daño, sino **también para proteger a otros de este tipo de ataques.**

Seguridad de la contraseña

El **uso responsable de contraseñas** puede limitar más daños en el caso de un ataque de phishing exitoso. Los usuarios deben usar una contraseña diferente para cada cuenta. Si un hacker obtiene datos de inicio de sesión que se usan en diferentes cuentas. **En el peor de los casos, todas las cuentas estarían en riesgo.**

Autenticación de dos factores

Con la autenticación de dos factores, el usuario puede crear un nivel de seguridad adicional. Un **sistema común de dos factores** es el envío de un código de confirmación a otro dispositivo. De esta manera, los datos confidenciales de la cuenta de usuario son seguros, incluso si un hacker ya ha capturado los datos de acceso para ellos.

Conciencia

Es importante estar al tanto de las tácticas y estafas de los ciberdelincuentes; esto ayudará a detectarlos más rápidamente o identificar tácticas similares. Además de la protección técnica, es esencial **tomar conciencia de las terribles estafas.**

La creatividad de los ciberdelincuentes es ilimitada: a menudo se dan cuenta de los acontecimientos actuales y usan temas cargados de emociones para dar credibilidad a sus mensajes. Los clientes del banco, en particular, son víctimas de estafas como esta. Los ciberdelincuentes enviaron correos electrónicos falsos en nombre de PayPal, usando el tema de GDPR, que entró en vigor en ese momento.

Existen **webs como el centro de asesoramiento al consumidor, donde se enumeran los métodos de phishing actuales.** Echar un vistazo a esta lista, puede revelar si has sido víctima de un correo fraudulento.

Medidas de emergencia

Si los ciberdelincuentes han logrado obtener los datos de acceso de un usuario a través de un correo electrónico de phishing, el **usuario aún puede protegerse a sí mismo.** Si aún es posible, el usuario debe iniciar sesión en la cuenta afectada lo antes posible para **cambiar la contraseña.** Además, debe verificar si ya se han realizado cambios en la cuenta o incluso se han realizado transacciones, como una transferencia bancaria. Si este es el caso, se recomienda **bloquear la cuenta afectada lo antes posible.**

Informar de ataques de phishing

Los correos electrónicos de suplantación de identidad (phishing) y los sitios web de suplantación de identidad (phishing) se pueden informar al remitente de quien se supone que se originó. **También es útil informar al** radar de phishing del centro de asesoramiento al consumidor. Los correos electrónicos falsos se enumeran allí y, por ello, otros usuarios pueden encontrarlos. Los empleados pueden informar de posibles ataques de phishing al responsable de seguridad de TI de la empresa, de modo que las empresas de seguridad de TI puedan reaccionar en consecuencia. Al usar un servicio de seguridad de correo electrónico, **se debe informar al proveedor de las anomalías que indican un ataque de phishing.**

CHECKLIST

- **Verificar remitente:** ¿Conozco al remitente? ¿Hay números o letras cifradas en la dirección del remitente? ¿Qué dirección IP se muestra en el encabezado?
- **Receptor:** Cuando uses diferentes cuentas de correo electrónico, asegúrate de usar la dirección correcta: ¿Me he registrado en PayPal usando mi cuenta de yahoo o Google Mail?
- **Diseño, ortografía y gramática:** ¿Se nota la cantidad de errores ortográficos y gramaticales? ¿Hay caracteres desconocidos en el correo electrónico? ¿El diseño generalmente causa una impresión de alta calidad?
- **Saludo:** ¿Se dirigieron a mí con mi nombre real?
- **Presión psicológica:** ¿El remitente amenaza con publicar grabaciones de video, acciones legales o similares? ¿El remitente solicita una acción rápida?
- **Verifica enlaces, archivos adjuntos y sitios web:** ¿Es la URL la dirección original del sitio web del presunto remitente? ¿Cuáles son los formatos de archivo de los archivos adjuntos? ¿El sitio web de phishing solicita datos que el operador debería conocer realmente?
- **Solicitud de datos confidenciales:** Si se le pide al destinatario que ingrese contraseñas o ¿Han solicitado los números PIN?
- **Medidas de seguridad:**
  - ¿Utilizo contraseñas diferentes y seguras para cada cuenta? ¿Utilizo la autenticación de dos factores? ¿Estoy familiarizado con las típicas estafas de phishing?
  - Medidas de emergencia: cambiar contraseñas, bloquear cuentas, informar de ataques de phishing a empresas y al centro de asesoramiento al consumidor

Básicamente, todos los indicadores y consejos mencionados anteriormente son importantes para **la detección y prevención de ataques de phishing** pero para estar protegido de manera fiable, **Hornetsecurity recomienda el uso de servicios de seguridad de correo electrónico** que previenen los ataques de phishing por adelantado.