Historia del Phishing

Universidad de las Ciencias Informáticas

Facultad 2

Maryla de la Caridad Jiménez Pérez [1*], Gabriela de la Caridad Puerto Acosta[2]

[1]2204, Facultad, Universidad de las Ciencias Informáticas, Carretera a San Antonio de los Baños, km 2 ½, Boyeros, La Habana, Cuba, maryla@estudiantes.uci.cu

[2] 2204, Facultad, Universidad de las Ciencias Informáticas, Carretera a San Antonio de los Baños, km 2 ½, Boyeros, La Habana, Cuba, cacosta@estudiantes.uci.cu

Mayo, 2024

RESUMEN

El phishing es una técnica de ingeniería social utilizada para engañar a los usuarios de Internet y obtener información confidencial. Los primeros intentos de phishing se remontan a la década de 1990, cuando los estafadores utilizaban diferentes tácticas para engañar a los usuarios de AOL y otros servicios de correo electrónico para que divulgaran sus contraseñas. Sin embargo, el término "phishing" no se acuñó hasta principios de la década de 2000, cuando los estafadores comenzaron a utilizar correos electrónicos y sitios web falsos para engañar a los usuarios.

A medida que la tecnología ha avanzado y los usuarios se han vuelto más conscientes de la seguridad en línea, los estafadores han evolucionado y adaptado sus técnicas de phishing para hacerlas más sofisticadas y efectivas. Las técnicas de phishing más comunes incluyen correos electrónicos fraudulentos, spear phishing, smishing, vishing y pharming.
En este trabajo se definirá el fenómeno actual del Phishing, un delito poco conocido, pero con gran impacto tanto económico como social. Además, se explicarán los tipos de phishing, la forma de combatirlo y las medidas necesarias que un usuario debe tomar para no ser una futura víctima y cuáles deben tomar las empresas para que no suplanten su identidad. En cuanto al ámbito internacional, se nombrarán los medios utilizados para evitar estos ataques y la forma en que los países colaboran entre sí para que todos estén actualizados e informados de las últimas novedades y evolución del mismo. .

Palabras claves: phishing, redes sociales, suplantación de identidad.

ABSTRACT

Phishing is a social engineering technique used to trick Internet users into obtaining confidential information. The first phishing attempts date back to the 1990s, when scammers used different tactics to trick users of AOL and other email services into giving up their passwords. However, the term "phishing" was not coined until the early 2000s, when scammers began using fake emails and websites to trick users.

As technology has advanced and users have become more aware of online security, scammers have evolved and adapted their phishing techniques to make them more sophisticated and effective. The most common phishing techniques include fraudulent emails, spear phishing, smishing, vishing, and pharming.

In this work, the current phenomenon of Phishing will be defined, a little-known crime, but with great economic and social impact. In addition, the types of phishing will be explained, how to combat it and the necessary measures that a user must take to avoid being a future victim and what measures companies must take so that their identity is not impersonated. Regarding the international level, the means used to prevent these attacks and the way in which countries collaborate with each other will be named so that everyone is updated and informed of the latest developments and evolution of the same.

Keywords: phishing, social networks, identity theft.

INTRODUCCIÓN

El phishing es una técnica de ingeniería social que se utiliza para engañar a los usuarios de Internet y obtener información confidencial, como contraseñas, números de tarjetas de crédito y datos financieros. Los primeros intentos de phishing se remontan a la década de 1990, cuando los estafadores comenzaron a engañar a los usuarios de AOL y otros servicios de correo electrónico para que divulgaran sus contraseñas. Sin embargo, el término "phishing" no se acuñó hasta principios de la década de 2000, cuando los estafadores comenzaron a utilizar correos electrónicos y sitios web falsos para engañar a los usuarios.

A medida que la tecnología ha avanzado y los usuarios se han vuelto más conscientes de la seguridad en línea, los estafadores han evolucionado y adaptado sus técnicas de phishing para hacerlas más sofisticadas y efectivas. En este artículo, se explorará la historia del phishing, desde sus orígenes hasta el día de hoy, y se examinarán las diferentes técnicas que se han utilizado a lo largo de los años.

Orígenes del phishing

Los primeros intentos de phishing se remontan a la década de 1990, cuando los estafadores utilizaban técnicas de ingeniería social para engañar a los usuarios de AOL y otros servicios de correo electrónico para que divulgaran sus contraseñas. En aquel entonces, los estafadores utilizaban diferentes tácticas para engañar a los usuarios, como hacerse pasar por representantes de servicio al cliente o enviar correos electrónicos de aspecto oficial que pedían a los usuarios que verificaran su información de cuenta.

En 1996, un grupo de estafadores rusos conocido como los "carders" comenzó a utilizar técnicas de phishing para obtener información de tarjetas de crédito de los usuarios de AOL. Utilizando un software especializado, los carders enviaban correos electrónicos a los usuarios de AOL que contenían un enlace a un sitio web falso que parecía ser el sitio web oficial de AOL. Una vez que los usuarios ingresaban su información de inicio de sesión en el sitio web falso, los carders podían acceder a sus cuentas de AOL y robar su información de tarjeta de crédito.

A medida que Internet se volvió más popular en la década de 2000, los estafadores comenzaron a utilizar técnicas de phishing más sofisticadas para engañar a los usuarios. En 2003, se informó sobre el primer ataque masivo de phishing, dirigido a los clientes de PayPal. Los estafadores enviaron correos electrónicos a los usuarios de PayPal que parecían ser del servicio de seguridad de PayPal y les pedían que verificaran su información de cuenta en un sitio web falso. Como resultado, muchos

usuarios divulgaron su información de inicio de sesión y los estafadores pudieron acceder a sus cuentas de PayPal.

DESARROLLO

¿QUÉ ES EL PHISHING?:

Se puede definir al phishing como el proceso por el cual una persona es contactada por email o por teléfono por alguien que simula ser una institución legítima para obtener datos privados, tales como datos bancarios, contraseñas, datos personales. Luego esta información obtenida de forma fraudulenta es utilizada para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad.

Actualmente la forma de phishing más utilizada es el envío masivo de correo electrónico con la finalidad de engañar a la víctima y que proporcione sus datos personales al "phisher". Aunque esta no es la única forma de phishing. En los últimos años esta actividad ha ido mejorando y cada vez es más difícil detectar un correo falso. Además, las técnicas han ido mejorando considerablemente y cada día hay más y mejores. Las más sofisticadas son el uso de sitios web falsos, instalación de troyanos, key-loggers, screen-loggers, envío de mensajes SMS, llamadas telefónicas etc...

Además del Phishing, hay más formas de estafas por internet, como el Pharming que es un ataque al servidor DNS4 y re direcciona el tráfico legítimo a una web falsificada. El Vishing es el ataque por el cual el usuario recibe un correo electrónico donde se le indica que llame a un número de teléfono. Al hacerlo se le pedirán datos personales. El Smishing es similar al anterior pero el método es por medio de SMS

Se pueden clasificar según el modus operandi, o sea la forma que utilizan para obtener esta información o una clasificación según los datos que buscan obtener. Por tanto, con esta última clasificación distinguimos por ejemplo el phishing bancario o el phishing de redes sociales. Actualmente se han contado más de 10.000 formas de phishing.

La definición más citada es la que proporciona el APWG y ha sufrido varias ampliaciones y modificaciones según la evolución misma del Phishing:

“Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Los ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social. Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación de crimeware en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos que captan las pulsaciones de teclado”.

En los últimos años la palabra phishing ha ido cobrando relevancia e importancia debido a las grandes pérdidas económicas que ha causado. Y también debido a que sus técnicas y su calidad ha mejorado notablemente y cada vez es más alto el número de personas que son víctimas de esta estafa. El phishing consiste en la suplantación de identidad de una empresa o entidad bancaria para que la víctima crea que la empresa legitima contacta con ella y necesita los datos personales de la misma. La víctima al creer que es un email/ llamada de la empresa o entidad de forma legítima proporciona esta información privada, sin darse cuenta que está siendo víctima de una estafa cometida por medios electrónicos.

Acuñación del término "phishing"

El término "phishing" se acuñó en 1996 en la comunidad de hackers de América del Norte. El término se derivó de la palabra "fishing" (pesca, en inglés), que se refiere a la técnica de lanzar una línea y esperar a que un pez muerda el anzuelo. El término se utilizó por primera vez para describir una técnica de hacking que implicaba el envío de correos electrónicos fraudulentos que parecían ser de una fuente confiable.

En 2004, el término "phishing" fue incluido en el Diccionario de Oxford, lo que demuestra la creciente importancia de la técnica de phishing en la sociedad. Desde entonces, el término se ha utilizado ampliamente en la industria de la seguridad cibernética y se ha convertido en un término común en la cultura popular.

Técnicas de phishing

A lo largo de los años, los estafadores han utilizado una amplia variedad de técnicas de phishing para engañar a los usuarios de Internet. Algunas de las técnicas más comunes incluyen:

- Correos electrónicos de phishing: los estafadores envían correos electrónicos fraudulentos que parecen ser de una fuente confiable, como un banco o un sitio web de compras en línea. Los correos electrónicos suelen contener un enlace a un sitio web falso que parece ser el sitio web oficial de la empresa.

- Spear phishing: una forma más sofisticada de phishing que implica el envío de correos electrónicos altamente personalizados a individuos específicos. Los correos electrónicos pueden incluir información personal del destinatario, como su nombre, dirección y número de teléfono, lo que hace que el correo electrónico parezca más legítimo.

- Smishing: una forma de phishing que utiliza mensajes de texto en lugar de correos electrónicos. Los estafadores envían mensajes de texto fraudulentos que parecen ser de una fuente confiable y contienen un enlace a un sitio web falso.

- Vishing: una forma de phishing que utiliza llamadas telefónicas en lugar de correos electrónicos. Los estafadores llaman a los usuarios y pretenden ser representantes de una empresa legítima, como un banco, y les piden que divulguen su información personal.

- Pharming: una forma de phishing que implica el redireccionamiento de los usuarios a un sitio web falso, incluso si escriben la dirección correcta en la barra de direcciones del navegador. Los estafadores utilizan técnicas de hacking para redirigir el tráfico web a un sitio web falso que parece ser el sitio web oficial de la empresa.

Prevención del phishing

Para evitar caer en una trampa de phishing, es importante que los usuarios de Internet tomen medidas para proteger su información personal y financiera. Algunas de las medidas que se pueden tomar incluyen:

- Tener cuidado al abrir correos electrónicos de remitentes desconocidos o sospechosos.

- No divulgar información personal o financiera en respuesta a correos electrónicos, mensajes de texto o llamadas telefónicas no solicitados.

- Verificar la URL del sitio web antes de ingresar información confidencial.

- Utilizar software de seguridad y antiphishing para protegerse contra ataques de phishing.

- Mantener actualizado el software del navegador y del sistema operativo para evitar vulnerabilidades de seguridad.

TIPOS DE PHISHING:

SEGÚN EL SERVICIO QUE ATAQUEN:

BANCOS Y CAJAS: Aquí el objetivo es robar el pin secreto, el número de tarjeta de crédito y datos análogos con el fin de lucrarse económicamente. Al poseer el atacante estos datos puede utilizarlos para realizar transferencias a otra cuenta, realizar compras y pagos por internet, retirar dinero de la cuenta. Consecuencia de esto es una gran pérdida económica para la víctima. Las excusas utilizadas son varias: a la posible víctima se le envía un correo con un enlace donde se le solicitan los datos porque su cuenta bancaria fue bloqueada por motivos de seguridad, o por un cambio de normativa en el banco, por ejemplo. Los bancos más conocidos que han sido falsificados son ING Direct, Bankia, Banco Popular... PASARELAS DE PAGO ONLINE: La intención es igual que cuando se habla de bancos, obtener los datos bancarios. Las excusas que utilizan los estafadores son varias, por ejemplo, que se produjo un cierre de sesión del usuario incorrecto o que se detectó una posible intrusión en sus sistemas de seguridad. Las empresas a las cuales afectan son Paypal, Mastercard...

REDES SOCIALES: Aquí lo que se pretende es claro: suplantar la identidad u obtener información sensible y privada del usuario de redes sociales. Las redes afectadas más comunes son Facebook, Twitter, Tuenti, Instagram... El método empleado aquí es comunicarle a la víctima que se le etiqueto en una foto, o que alguien le envía una solicitud de amistad, o por motivos de seguridad es necesario que envié sus claves. Este tipo de Phishing es cada vez más utilizado porque hoy en día las personas se comunican por este tipo de redes, el uso de las mismas va aumentando y cada vez es más común que sufran estos ataques. En la actualidad lo raro no es ser usuario de la red social, al contrario, es no serlo. Por tanto, el aumento del uso de las mismas hace que sea un blanco fácil para los Phishers.

PÁGINAS DE COMPRA/VENTA Y SUBASTAS: La pretensión del estafador en este tipo de phishing es obtener las cuentas de usuario de las víctimas y estafar económicamente al mismo. Las excusas típicas utilizadas para captar la atención del usuario son que se observan movimientos sospechosos, problemas con la cuenta de usuario.... Las empresas que sufren estos ataques son Amazon o EBay. Hay que tener en cuenta que actualmente las personas utilizan cada vez más este tipo de servicios para la compra venta. Antes no era un punto de atención de los phishers porque el uso de estas redes no estaba extendido. Hoy en día, el uso de las mismas es bastante extenso.

JUEGOS ONLINE: En este medio los motivos son varios: robar la identidad, robar los datos bancarios, los datos privados y suplantación de identidad. Los juegos online comunes suplantados por ejemplo es el World Warcraft. Las excusas son parecidas a las anteriores. Todas destinadas a engañar al usuario.

SOPORTE TÉCNICO Y DE AYUDA DE EMPRESAS Y SERVICIO: Un ejemplo muy común es el phishing a Apple. Aquí el objetivo es robar la cuenta al usuario, por ejemplo, el ID del AppStore para poder hacer compras con la identidad y cuenta bancaria de otra persona. Se suelen suplantar empresas como Outlook, Gmail... etc.

ALMACENAMIENTO EN LA NUBE: Las empresas que ofrecen este servicio de almacenamiento son Google Drive, Dropbox....Lo que se pretende conseguir son los datos privados, documentos, fotografías que el usuario almaceno en estas páginas web. Una vez obtenidos estos datos, el estafador puede cometer varios delitos relacionados.

SERVICIOS O EMPRESAS PÚBLICAS: Es un tipo de Phishing que simula ser, por ejemplo, la policía nacional, o la Agencia Tributaria y por esto su riesgo. El phisher intenta infectar el ordenador de la persona y así obtener los distintos datos para su beneficio. Una de las excusas utilizadas más comunes, es cuando intentan avisar al usuario de una posible multa y es necesario obtener sus datos.

SERVICIOS DE MENSAJERÍA: Esta estafa es menos común. Aquí se utilizan empresas proveedoras de correo y mensajería para efectuar el phishing y así conseguir información privada del

usuario. Por ejemplo, la víctima recibe un email de la empresa DHL informándole que ha recibido un paquete y le solicita sus datos.

FALSAS OFERTAS DE EMPLEO: Aquí hay diferentes tipos de oferta falsa que implican phishing para engañar al usuario y conseguir sus datos y a continuación usarlos con fines fraudulentos. Estas son: Trabajar desde casa haciendo tareas manuales: se piden sus datos y una cantidad de dinero para guardarle el puesto de trabajo. Oferta de trabajo, llama e infórmate: aquí se le pide a la víctima que llame a un determinado número de teléfono y aporte sus datos. ¡Empieza a trabajar! Solo tienes que aportar tus datos personales: muy fácil, la víctima ofrece fotografías de su documentación personal y ahí es cuando comenzarían a trabajar. Pero lo único que buscan es obtener información confidencial. Infórmate sobre un puesto de trabajo aquí: lo que hacen es poner un anuncio con un enlace ficticio. Cuando la víctima entra en ese enlace, se le instala malware o rellenan formularios con información susceptible. Transferencias bancarias: es el trabajo de mula o intermediario que utiliza el phishing bancario.

Hay varias medidas que los usuarios pueden tomar para protegerse de los ataques de phishing. Algunas de las medidas más efectivas incluyen:

1. Sé cuidadoso al abrir correos electrónicos: Si recibes un correo electrónico de una fuente desconocida o sospechosa, no lo abras ni hagas clic en ningún enlace que contenga. Si el correo electrónico parece ser de una empresa legítima, verifica la dirección de correo electrónico del remitente y comprueba si la gramática y la ortografía son correctas.

2. No reveles información personal o financiera: Nunca reveles información personal o financiera en respuesta a correos electrónicos, mensajes de texto o llamadas telefónicas no solicitados. Las empresas legítimas nunca pedirán información personal o financiera por correo electrónico o por teléfono.

3. Verifica la URL del sitio web: Antes de ingresar información personal o financiera en un sitio web, verifica la URL para asegurarte de que sea el sitio web oficial de la empresa. Si el sitio web parece sospechoso o no es el sitio web oficial, no ingrese información confidencial.

4. Utiliza software de seguridad y antiphishing: Utiliza software de seguridad y antiphishing para proteger tu computadora y tus dispositivos móviles contra ataques de phishing. El software de

seguridad puede detectar y bloquear sitios web fraudulentos y correos electrónicos sospechosos.

5. Mantén actualizado el software del navegador y del sistema operativo: Mantén actualizado el software del navegador y del sistema operativo para evitar vulnerabilidades de seguridad que los estafadores pueden explotar.

6. Usa autenticación de dos factores: Utiliza la autenticación de dos factores siempre que sea posible para proteger tus cuentas. Esto añade una capa adicional de seguridad y dificulta que los estafadores accedan a tus cuentas.

En resumen, la prevención del phishing es fundamental para proteger la información personal y financiera de los usuarios de Internet. Al seguir estas medidas, los usuarios pueden reducir significativamente el riesgo de sufrir un ataque de phishing y protegerse contra los estafadores en línea.

CONCLUSIONES

1. El phishing se remonta a la década de 1990, cuando los estafadores comenzaron a engañar a los usuarios de AOL y otros servicios de correo electrónico para que divulgaran sus contraseñas.

2. El término "phishing" se acuñó en la década de 2000, cuando los estafadores comenzaron a utilizar correos electrónicos y sitios web falsos para engañar a los usuarios.

3. Los estafadores han evolucionado y adaptado sus técnicas de phishing a lo largo de los años, utilizando diferentes tácticas para engañar a los usuarios y obtener información confidencial.

4. Las técnicas de phishing más comunes incluyen correos electrónicos fraudulentos, spear phishing, smishing, vishing y pharming.

5. El primer ataque masivo de phishing se informó en 2003, dirigido a los clientes de PayPal.

6. El phishing sigue siendo una amenaza significativa en la actualidad, ya que los estafadores continúan adaptando sus técnicas para engañar a los usuarios de Internet y obtener información confidencial.

7. La prevención del phishing es fundamental para proteger la información personal y financiera de los usuarios de Internet.

8. Algunas medidas de prevención del phishing incluyen tener cuidado al abrir correos electrónicos de remitentes desconocidos o sospechosos, no divulgar información personal o financiera en respuesta a correos electrónicos, mensajes de texto o llamadas telefónicas no solicitados, verificar la URL del sitio web antes de ingresar información confidencial, utilizar software de seguridad y antiphishing y mantener actualizado el software del navegador y del sistema operativo.

9. El phishing seguirá siendo una amenaza significativa en el futuro, ya que los estafadores continúan encontrando nuevas formas de llevar a cabo ataques de phishing.

10. Es importante que los usuarios de Internet estén al tanto de los riesgos del phishing y tomen medidas para proteger su información personal y financiera.

REFERENCIAS BIBLIOGRÁFICAS

1. Baker, S. (2015). A brief history of phishing. Network Security, 2015(7), 5-9. https://doi.org/10.1016/S1353-4858(15)30059-9

2. Johnson, M. (2005). Phishing attacks and countermeasures. Network Security, 2005(11), 5-8. https://doi.org/10.1016/S1353-4858(05)71101-6

3. Kaspersky. (2021). What is phishing? Definition and explanation. https://www.kaspersky.com/resource-center/definitions/what-is-phishing

4. Lewis, P. (2019). A brief history of phishing. Cybersecurity Magazine. https://www.cybersecurity-magazine.com/a-brief-history-of-phishing/

5. Microsoft. (2021). Protect yourself from phishing. https://www.microsoft.com/en-us/security/business/phishing

6. Stammberger, J. (2004). The history of phishing. Communications of the ACM, 47(9), 31-33. https://doi.org/10.1145/1015864.1015881