Dirección Nacional
de Ciberseguridad

Phishing

Una guía y un glosario para conocer sus modalidades y prevenirlas.

Argentina unida

Jefatura de Gabinete de Ministros
Argentina

Secretaría de Innovación Pública

Definición de phishing

La expresión phishing es utilizada para definir a un tipo de fraude que tiene por objetivo engañar a la persona usuaria para que revele algún tipo de información, generalmente financiera o personal, con el objetivo de suplantar su identidad digital y obtener algún beneficio. Se trata del ciberataque más común y más sencillo, y quien lo perpetra suele ser denominado “phisher”.

Algunas ideas sobre el origen del término

Si bien hay muchas teorías a la hora de rastrear el origen de la expresión, el consenso más difundido es que proviene de la palabra inglesa "fishing" que significa pesca, en relación al “anzuelo” que se le tiende a la persona usuaria para que “muerda” o caiga en la trampa.

Otra idea con mucho consenso, no contrapuesta sino complementaria, es que el término, o más precisamente su grafía, es un acrónimo de “password harvesting fishing”, que podría traducirse como “cosecha o pesca de contraseñas”. Sobre esta idea se piensa que es una explicación dada a posteriori, en virtud de que el fonema “ph” es utilizado habitualmente por hackers para sustituir a “f”, aunque también se dice que tiene que ver con la expresión “phony” que en inglés significa “falso”.

También se cree que esta grafía tiene que ver con los primeros hackers, quienes a través de los teléfonos de tierra podían realizar ataques, y se hacían llamar “phreaks”, nombre que deviene de la amalgama de las palabras “phone” (teléfono) y “freak”, que en inglés tiene variadas connotaciones, entre ellas “raro” o “loco”.

Perjuicios del phishing para la persona usuaria

Los daños causados por el phishing pueden ser muy variados, y van desde la pérdida de acceso a cuentas de correo electrónico, redes sociales, sitios de compraventa online hasta perjuicios y daños económicos derivados.

Si bien con el correr del tiempo las personas usuarias han ido adquiriendo recursos simbólicos y tecnológicos -muchas veces fruto de malas experiencias-, el robo de identidad que deviene del phishing sigue siendo un problema grave cuando no un gran dolor de cabeza. El daño depende en gran medida de la información que el phisher haya sido capaz de robar y de lo que pueda hacer con ella.

Debido a la gran variedad de objetivos y de modalidades de phishing, hoy día, es muy difícil establecer con precisión las pérdidas ocasionadas, pero sin lugar a dudas son cuantiosas. Veamos entonces diversos tipos de phishing organizados en función de su vector de propagación y de su objetivo para darnos una idea de los graves daños que ocasiona. Hay que tener en cuenta que un ataque de phishing puede entrar en varias de estas categorías a la vez.

Tipos de phishing según su vector de propagación

Ya que el phishing consiste básicamente en un engaño, es muy común el uso de ingeniería social para hacer que la persona usuaria muerda el anzuelo. Esta es la manera más difundida, pero no la única. Veamos entonces diversos tipos de phishing según cómo se propagan.

Phishing por correo electrónico

El phishing por correo electrónico es sin dudas la modalidad más difundida. Los mensajes de correo pueden contener enlaces, que dirigen a sitios webs maliciosos, o archivos adjuntos que incluyan un programa o código malicioso (malware). El phisher emite correos, que distribuye en forma masiva, haciéndose pasar por emisores de confianza para la persona usuaria. Generalmente, finge ser alguna entidad bancaria para solicitar información personal de la víctima.

Dentro de esta modalidad, además de los enlaces maliciosos o adjuntos infectados de malware, podemos encontrar lo que se conoce como “estafa nigeriana”. El curioso nombre proviene de un “hoax” en el que el phisher se hacía pasar por un príncipe nigeriano que decía necesitar una cuenta bancaria para transferir fondos de forma urgente y segura. Así, la víctima tentada por la obtención de beneficios brindaba datos bancarios al atacante. Este tipo de phishing ha tenido varias “historias”, algunas tan absurdas como la de un cosmonauta encerrado en una antigua estación espacial rusa durante más de dos décadas, y precisa nuestra ayuda.

Phishing por sitio web

En el phishing por sitio web, el engaño consiste en crear un sitio web que se haga pasar por el original con la intención de que la persona usuaria introduzca sus datos de inicio de sesión. De esta manera, el phisher se hace con la cuenta de la persona usuaria, pudiendo ser esta de correo, de una entidad financiera o de redes sociales. Los perjuicios dependerán de la cuenta a la que el hacker ha tenido acceso.

Vishing

El término vishing deviene de “voice phishing”. En este caso, el phisher intenta convencer a su víctima a través del teléfono, ya sea celular o de línea, para que revele información personal que pueda serle de algún provecho. En este tipo de ataque, el phisher afirma representar a una empresa pública o privada de la cual la persona usuaria es cliente y la amedrenta con algún tipo de problema prometiendo solucionarlo en el momento si se brinda información de cuenta o pagando algún tipo de cargo.

Smishing

Al igual que en el caso anterior, el término smishing se conforma por una inicial que hace referencia al vector de propagación, en este caso los SMS o servicios de mensajería. Así, la víctima recibe un mensaje de texto que le solicita que haga clic en un enlace o descargue una aplicación maliciosa. Una vez más, con esta modalidad, se intenta también sorprender a la víctima a través de algún inconveniente inventado para sustraer información valiosa.

Phishing por redes sociales

El phishing por redes sociales se da en el caso de phishers que acceden a cuentas de redes sociales y logran que la gente envíe enlaces maliciosos o spam a sus contactos, ya sea a través del servicio de mensajería o en el etiquetado de posteos públicos. También es frecuente el robo de datos personales mediante cuentas falsas, a través de las que los hackers logran engañar a sus víctimas.

Dentro del vector “redes sociales” encontramos la modalidad que se conoce como “Man-in-the-middle”. Se trata de una forma de phishing en la que el phisher se ubica entre la persona usuaria y la red social. La información enviada a la red social pasa a través del atacante, quien tiene la oportunidad de verla y hasta editarla.

También a través de redes sociales podemos encontrar lo que se conoce como “deceptive phishing” que no es otra cosa que una cuenta que suplanta la identidad de la víctima. De ahí la recomendación de prestar atención a la información que se comparte de manera online y a las configuraciones de privacidad.

Una vez creada la cuenta apócrifa, utilizando elementos que la víctima proporcionó de manera inocente, el phisher envía solicitudes de amistad con diversos tipos de anzuelos a los contactos de la persona usuaria.

Pharming

El nombre “pharming” viene de la combinación de los términos phishing y pharming, que podríamos traducir como cultivo. En este caso se suplanta la identidad de una web y se arbitran los medios para que la víctima acceda a ella pensando que se trata de un sitio legítimo. Una vez en esta página, la persona usuaria está a merced del robo de datos.

URL phishing

Incluso tomando la precaución de tipear la dirección de un sitio en la barra del navegador, se puede ser objeto de phishing. En esta modalidad, URL phishing, se intenta engañar a la víctima aprovechando errores de tipeo o de otro tipo. Así, los phishers crean sitios que se parecen a los legítimos y, una vez adentro, se muerde el anzuelo.

Uno de los derivados del URL phishing es el Search Engine Phishing. Este tipo de ataque consiste en la creación de un sitio falso indexado en motores de búsqueda legítimos. La víctima, encuentra el link en su buscador habitual, no sospecha y cae. La amenaza sigue presente, pero recientes versiones de navegadores brindan herramientas para reducir su incidencia.

Phishing desde la nube

En los últimos años, la capacidad de procesamiento de los diversos dispositivos electrónicos ha crecido con mayor velocidad que la de almacenamiento. Así, las personas usuarias se encontraron con capacidad de reproducir y editar archivos realmente pesados, pero con escasa capacidad de guardarlos. Esto dio paso a los servicios de almacenamiento online o denominados también en "la nube".

Como era de esperar, los ciberdelincuentes tomaron nota del asunto e inundaron con anzuelos las plataformas de almacenamiento e intercambio de archivos online. En esta modalidad, el phisher envía enlaces a contenidos almacenados. Como en otras modalidades, la piratería de contenidos digitales es un terreno riesgoso para la persona usuaria.

Addline phishing

Mediante la modalidad conocida como "addline phishing", el phisher logra acceder a un dispositivo de la víctima (generalmente móvil) tendiendo una red wifi gratuita como trampa. El ataque implica el acceso al dispositivo de la persona usuaria con el objeto de robar información de cuentas bancarias o de otro tipo. Este ataque también es conocido como "Evil Twin" o mellizo malvado, ya que las redes wifi maliciosas tienden a parecerse demasiado a las legítimas.

Tabnabbing

Tabnabbing es un ingenioso tipo de phishing que apunta directamente a la vulnerabilidad de la persona usuaria. Este tipo de ataque nace del saber que muchas personas usuarias navegan por Internet usando muchas pestañas o ventanas a la vez. Entonces, mientras la víctima tiene en primer plano una pestaña determinada, el sitio malicioso reemplaza a una de las webs que estaban en segundo plano. Si la persona no se percata, ingresará sus datos en el sitio web del atacante, que suele indicar que se ha perdido la conexión o que la sesión ha caducado.

Man in the Browser (MITB)

Se trata de la instalación de un troyano (malware) en el navegador de la persona usuaria, que le permite al phisher capturar y modificar la información ingresada. La forma más usual consiste en la instalación de extensiones maliciosas del navegador creyendo que se trata de aplicaciones legítimas. Una vez instalado el malware en el navegador, analiza el tráfico de datos a la espera de que se cargue una web considerada un objetivo.

Tipos de phishing según su objetivo: spear phishing, whaling y fraude del CEO

Spear phishing

Si hablamos de pesca, en este caso llamado “spear phishing” se trata de capturar a la víctima con un arpón, que es lo que significa “spear” en el idioma inglés. Consiste en un ataque pensado para una persona física o empresa en particular. La modalidad puede ser variada, pero lo que distingue a este tipo de ataque es su direccionalidad.

En consecuencia, el modo de contacto con la persona usuaria tenderá a incluir contenido personalizado, lo que lo hace más creíble que un texto genérico. El phisher se hace con información de su objetivo con el fin de ganarse la confianza a través de un ataque más elaborado. Esta modalidad de phishing está íntimamente relacionada con la que sigue.

Whaling

El whaling, que proviene del inglés “pesca de ballenas”, es una variante del spear phishing, pero dirigido a una persona o empresa considerada de influencia. Digamos que no es lo mismo hacerse con los datos personales o sesiones de una persona común y corriente, que hacerse con esa misma información de una persona considerada de mayor importancia. Podría decirse que el whaling es un tipo de spear phishing dirigido a “peces gordos”, como ejecutivos de alto rango o funcionarios de gobierno.

Fraude del CEO

En el ataque denominado “fraude del CEO”, los phishers se hacen pasar por un ejecutivo de alto rango, tanto del sector público como del privado, con el fin de obtener un pago o información de los empleados. Este ataque suele darse después de un whaling exitoso.

Un poco de historia

Se cree que la primera vez que el término “phishing” se utilizó fue en enero de 1996, en el grupo de noticias de hackers “alt.2600”. Su mención hacía referencia a la práctica utilizada por los phishers para

pescar cuentas de miembros de América OnLine (AOL). En su momento, se le atribuyó la invención del término a Khan Smith, un afamado hacker de la década de los '90.

Por aquel entonces, AOL era un proveedor de Internet bastante popular, y esto lo volvió objeto de numerosos ataques, y fue utilizado no sólo como coto de caza -o de pesca- sino también como medio de comunicación entre los hackers. Eventualmente, la empresa tomó medidas para evitar este tipo de ataques, pero el problema ya se encontraba ampliamente difundido, lo que obligó a la compañía a realizar advertencias a las personas usuarias afirmando que ningún personal de la compañía solicitará información de facturación o contraseñas con el fin de mejorar el servicio.

Como sabemos, ninguna medida es del todo efectiva a la hora de evitar los ataques y, en la década siguiente del siglo pasado, cuando internet explotó en términos de masividad, los phishers dirigieron sus ataques a clientes de servicios bancarios y financieros en general, terreno que constituía una auténtica novedad y al que las personas usuarias acudían sin una cultura digital bien conformada.

Ya en el siglo actual, el objetivo se mudó a la siguiente gran novedad: las redes sociales. A través de estas plataformas los hackers no sólo podían obtener información crediticia de sus víctimas sino también sus identidades digitales, con fines variados que van desde la extorsión hasta otros tipos de estafa.

A medida que lo digital fue permeando diversos aspectos de la vida cotidiana de las personas, se fueron abriendo nuevas posibilidades para los ciberdelincuentes, y las plataformas de compraventa online y los sitios de pago digital se convirtieron en un jugoso objetivo de los phishers.

Casos Resonantes

Si bien los ataques de phishing deben contarse a trillones, hay algunos casos resonantes que se destacan o por su impacto en materia de daños o por su habilidad y osadía. En nuestro país, en el último tiempo, se han registrado casos de phishing que tuvieron por objetivos a plataformas de contenido online y hasta a municipios y la banca pública.

A continuación, mencionamos algunos casos resonantes a nivel mundial con el fin de sensibilizar y concientizar sobre el tema.

Mundial de fútbol Rusia 2018

Si bien no se trata de un caso en particular, previo a su comienzo y durante el desarrollo de la Copa FIFA, hubo un pico de casos de phishing a nivel global. Aprovechando el entusiasmo que el evento generaba en los amantes del deporte, se encarnaba el anzuelo con entradas a los partidos del Mundial, con plazas hoteleras de última hora y a precios ventajosos y hasta con merchandising de las distintas selecciones. Pero, como sabemos, si la oferta es demasiado buena, difícilmente sea cierta.

Entre otras tantas estafas online, la más saliente fue la de un grupo de hackers que logró penetrar en la base de datos de Booking.com, y, desde allí, lanzó un smishing dirigido a personas usuarias de la plataforma a través de SMS y Whatsapp. Siendo contactada a través de un medio de comunicación tan personal, mucha gente cayó en la trampa.

Google y Facebook pescados

Google y Facebook, estos dos gigantes del mundo tecnológico, también mordieron el anzuelo y fueron pescados. En el año 2017, los departamentos de contabilidad de estas dos empresas transfirieron más de 100 millones de dólares a cuentas extranjeras controladas por un hacker. Como se dice habitualmente, una cadena es tan fuerte como lo es su eslabón más débil. El caso es útil para comprender la necesidad de formar a la corporación en materia de ciberseguridad y para pensar en las categorías antes planteadas, como whaling y spear phishing.

Target filtra datos de millones de personas usuarias

Target es una cadena de grandes almacenes de los Estados Unidos de América. En 2013, fue objeto de phishing y tuvo grandes problemas a partir de una filtración de datos que afectó a 110 millones de clientes. Si bien la empresa nunca reveló los detalles del ataque, se sabe que el inicio fue un correo electrónico de phishing enviado a uno de sus proveedores.

Conscientes del entusiasmo que despiertan las promociones del tipo “Black Friday”, los hackers accedieron a los lectores de tarjetas en los puntos de venta, y obtuvieron cerca de 11 GB de datos de tarjetas de crédito y débito de los clientes. Como consecuencia del ataque, la compañía tuvo que resarcir a las víctimas por un valor estimado de 18 millones y medio de dólares.

Pesca china de ballenas con arpones

En 2011, Gmail, el servicio de correo electrónico de Google, recibió un ataque originado en China y dirigido a funcionarios del gobierno de los Estados Unidos de América y Corea del Sur, a activistas por los derechos humanos, militares, periodistas y otros “peces gordos”. La finalidad de este ataque no era otra que robar usuarios y contraseñas para poder espiar conversaciones online. En este caso, los phishers no infiltraron los servidores de Google sino que lograron engañar a las personas usuarias para obtener sus datos.

Operación “Phish Phry”

Se conoce con el nombre “Phish Phry” a una operación que se inició en el año 2007 y que creció hasta convertirse en objeto de la investigación más grande del FBI en materia de ciberdelito. Se trató de una organización de phishing a gran escala que engañaba a sus víctimas para obtener números de cuenta, contraseñas y códigos PIN mediante correos electrónicos y sitios web falsificados.

Para cuando la investigación concluyó, los ciberdelincuentes habían logrado transferir aproximadamente un millón y medio de dólares a sus cuentas, y se llevaron procesadas a cien personas en Estados Unidos y Egipto.

Recomendaciones para evitar el phishing

Dado que el objetivo de este tipo de ciberataque es engañar a la persona usuaria, la primera recomendación general consiste en desconfiar o mantenerse alerta ante cualquier aspecto que pueda generar una sospecha. Luego, como en cualquier caso, contar con el software de protección adecuado y actualizado para cada equipo, de la misma forma que se debe hacer con el sistema operativo y el navegador web. Más allá de esto, que pareciera evidente, a continuación siguen algunas recomendaciones puntuales.

Siendo que muchas veces el “anzuelo” utilizado por el phisher es un link o enlace web, nunca es mala idea tipear directamente la dirección en el navegador. De esta manera, se evitará acceder a un sitio malicioso.

Es preciso siempre chequear la dirección del remitente del correo electrónico, aunque el mensaje del phisher sea muy cuidado en términos de prolijidad y de imitación de la imagen corporativa de la que se valga. Recordar que esa casilla de mail nunca será la de la institución que se pretende suplantar.

Nunca hacer click en ningún enlace de correo electrónico sin antes corroborar la veracidad del remitente con la empresa de la que aparenta provenir el correo. De la misma forma, no es aconsejable abrir ningún archivo adjunto, incluso, aunque provenga de una persona conocida.

Si a pesar de todo la duda persiste siempre, puede copiar el texto del correo electrónico recibido y pegarlo en un documento en blanco como “texto sin formato”. De esta manera, podrás ver URLs maliciosas u otros códigos ocultos que no son visibles en formato HTML.

Tampoco es recomendable brindar datos personales o financieros en sitios que no sean de confianza. Siempre es una buena práctica verificar que el sitio al que vamos a acceder comience su dirección con "https://" y que contenga el ícono de un candado cerrado.

Nunca brinde sus datos personales a terceros. Piense que las empresas del sector bancario o proveedoras de servicios públicos nunca solicitan este tipo de datos por medio de un mensaje de correo, SMS, llamada telefónica o a través de cualquier otro medio. Por más insólito que parezca, hay que prestar atención a los errores de ortografía y al uso de un lenguaje demasiado informal para sospechar, ya que las organizaciones serias tienen buena redacción y se expresan correctamente.

El riesgo de pasar por ser demasiado cauto y desconfiado no significa nada comparado con ser un objeto de phishing. En caso de recibir un correo de alguna persona conocida que contenga un texto genérico y un archivo adjunto de nombre sospechoso, no está de más comunicarse con esa persona para preguntarle si nos ha enviado ese mail.

Los cuidados deben extremarse si se está utilizando un smartphone. Esto tiene que ver con el

tamaño de las pantallas, con la mayor dificultad a la hora de apreciar detalles y también con los "métodos abreviados" que proponen las aplicaciones con el fin de simplificar la experiencia de la persona usuaria. Pero los smartphones y otros dispositivos móviles son más propensos a hacernos cometer errores, no sólo por sus dimensiones y sus pantallas táctiles.

Otra recomendación consiste en evitar las operaciones sensibles (transferencias de dinero, pagos de servicios, compras on line, llenado de planillas, etc) si se está utilizando wifi. Siempre una conexión terrestre o, incluso, una del servicio de telefonía móvil será más segura. Este tipo de cuidado no omite a los demás, se trata de establecer "capas" de protección que aumentan su eficacia cuando son utilizadas en conjunto.

Revisar los resúmenes de tarjeta de crédito o de movimientos de cuenta puede alertarnos sobre cualquier irregularidad en caso de que ya hayamos sido víctimas de phishing.

Piense en sus activos digitales con el mismo cuidado con el que se ocupa de su casa y utilice contraseñas fuertes y diversificadas, es decir, no use la misma para el correo, la banca personal y otros servicios. También es aconsejable cambiar sus contraseñas con cierta periodicidad. De esta manera, además, evitará uno de los phishings más difundidos: el presunto mail de proveedor de correo que insta a cambiar la contraseña.

No haga click en ventanas emergentes. Estas suelen aparecer en "sitios piratas". Sepa que mirar películas o transmisiones deportivas por Internet a través de sitios no oficiales es piratería. Si aún así usted decide consumir este tipo de contenidos de sitios no seguros, tenga en cuenta que navegará, literalmente, en un océano plagado de anzuelos. Esto implica que tampoco debe hacer clic en el botón que le asegura "Cerrar". Por lo tanto, lo mejor será buscar otras maneras de cerrar esa ventana, como por ejemplo a través del navegador.
.