El Phishing o suplantación de identidad, es un término informático atribuido al uso de ingeniería social para el intento del robo de información confidencial, como contraseñas, nombres de usuarios, información detallada de tarjetas de crédito, etc.

El Phisher es el cibercriminal que se hace pasar por una empresa o personal de una organización de confianza, mediante correo electrónico o llamadas telefónicas.

El término proviene de la palabra inglesa “fishing” (pesca), tomando como metáfora hacer que los usuarios “muerdan el anzuelo”.

Se dice que la primera mención del término pshishing se dio a conocer en enero de 1996, mediante el grupo de noticias de hackers alt.2600, aunque posiblemente ya haya aparecido en la edición impresa del boletín de noticias “hacker 2600 Magazine”. En ese entonces, los ciberdelincuentes pretendían “pescar” cuentas de AOL.

En la actualidad, es común que los intentos de phishing se efectúen a clientes de bancos y servicios de pago en línea. Esto mediante el envío de correos electrónicos fingiendo ser la institución.

Otros medios que han ganado popularidad como blancos de phishers son las redes sociales, en las que los piratas roban la información de los usuarios y fingen ser ellos en las redes.

A finales de 2006, un gusano informático logró robas páginas del sitio web MySpace, haciendo que los enlaces redireccionaran a una página web diseñada para el robo de información de ingreso de los usuarios.

Algunas técnicas de Phishing son la creación de páginas web falsas, donde se tenga que iniciar sesión. El phiser crea una página de algún banco por ejemplo, de nombre HSBC, cuyo dominio original es hsbc.com, con un nombre como hssbc.com o hsbc.net, con una copia idéntica del contenido de la página, para posteriormente enviar correos electrónicos utilizando direcciones parecidas a las oficiales solicitando a los usuarios que ingresen a la página a confirmar sus datos de banca.

Cuando el usuario ingresa a la página falsa y teclea sus datos, los delincuentes almacenan los datos.
Existen otros métodos como el uso de keyloggers, que almacenan la información del usuario y la envía por correo electrónico.

LAVADO DE DINERO

Otro caso actual del phishing, es el lavado de dinero, en el que empresas ficticias reclutan teletrabajadores por medio de correos electrónicos, chats u otros medios, ofreciéndoles trabajo desde casa, además de otros grandes beneficios.

Las personas que aceptan, se convierten en víctimas, sin saber que están incurriendo en un grave delito.
Cuando la víctima acepta el trabajo, debe rellenar un formulario de registro, en el que le solicitan su cuenta bancaria para realizar el pago por sus servicios. Las empresas ficticias, depositan el dinero producto de estafas bancarias por método de phishing. La víctima, una vez que acepta todo, se convierte en lo que se conoce como mulero.

Cuando la empresa realiza una estafa, le envía el dinero al supuesto empleado, el cual se queda con un porcentaje de entre el 10% y 20%, y el resto lo reenvía por medio de sistemas de envío a cuentas indicadas por la empresa.

Muchas veces, la víctima desconoce todo el proceso y cree estar realizando un trabajo legal, sin embargo, está incurriendo en un acto ilegal que podría causarle graves problemas legales luego de denuncias por parte de las entidades bancarias.

Ante la problemática y el gran aumento de casos de phishing, empresas y compañías de seguridad han creado métodos de difusión para evitar que los usuarios caigan.

Algunas empresas capacitan a sus empleados para evitar caer en trampas por correo electrónico.
También es recomendable el uso de programas anti-phishing, que detectan cuando una

página web o correo electrónico es fraudulento.

El Anti-Pshihing Working Group, cuya página es www.apwg.org, es una industria y asociación que aplica la ley contra las prácticas de phishing, y sugiere que las técnicas convencionales de phishing podrían ser obsoletas en un futuro, por medio de orientación sobre métodos de ingeniería social utilizados por los phishers.

El 26 de enero de 2004, la FTC (Federal Trade Commission) de Estados Unidos, llevó a juicio el primer caso contra un phisher sospechoso. Se trataba de un adolescente de California, que supuestamente creó y utilizó una página web con un diseño similar al de la página de América Online, con el que robaba números de tarjetas de crédito.

A finales de marzo de 2005, las autoridades arrestaron a un hombre estonio de 24 años de edad, utilizando una backdoor, luego de que las víctimas visitaron su sitio web falso, en el que tenía un keylogger que le permitía almacenar lo que los usuarios tecleaban.

Por otro lado, se llevó a cabo el arresto del phisher denominado Kingpin, Valdir Paulo de Almeida, quien era un líder de las más grandes redes de phishing que en dos años lograron robar entre 18 y 37 millones de dólares estadounidenses.