RECOMENDACIONES PARA EVITAR SER VICTIMA DEL "PHISHING"

ArCERT

COORDINACIÓN DE EMERGENCIAS EN REDES TELEINFORMÁTICAS DE ARGENTINA

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI)

versión 1.0 – Agosto 2006

Debido al crecimiento en la cantidad de incidentes de "phishing" reportados en los últimos meses, el grupo ArCERT le acerca las siguientes recomendaciones para facilitar su detección y mitigar sus efectos.

¿Qué es el "Phishing"?

"Phishing" es una forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo) a una o varias personas, intentando convencerlas para que revelen sus datos personales. Usualmente, esta información es luego utilizada para realizar acciones fraudulentas, como transferencias de fondos de su cuenta bancaria, compras con sus tarjetas de crédito u otras acciones delictivas que pueden efectuarse mediante la utilización de esos datos.

Actualmente el modo de difusión más utilizado por los atacantes para realizar un ataque de "phishing" es el correo electrónico. Estos correos suelen ser muy convincentes, y simulan haber sido enviados por una entidad conocida y confiable, con la cual la persona opera habitualmente, como por ejemplo un banco o una empresa que realice operaciones comerciales por Internet. En el mensaje se alegan diversos motivos, como problemas técnicos o la actualización o revisión de los datos de una cuenta, y a continuación se le solicita que ingrese a un sitio web para modificar o verificar sus datos personales: nombre completo, DNI, claves de acceso, etc.

Dicha página web es en realidad un sitio falsificado que simula ser el de la organización en cuestión. El diseño de estas páginas web suele ser muy similar, y a veces prácticamente idéntico, al de las páginas web reales de la organización cuya identidad se simula. Asimismo, estos sitios tienen direcciones web que pueden confundir a un usuario desprevenido por su parecido con las direcciones web auténticas. En la mayoría de los casos, el texto del enlace escrito en el correo electrónico es la dirección real del sitio web. Sin embargo, si el usuario hace clic en ese enlace, se lo redirige a una página web falsa, controlada por el atacante.

También se han detectado casos en los cuales el usuario recibe un mensaje SMS a su teléfono celular, un mensaje en un contestador automático o una llamada telefónica, en los cuales, mediante técnicas muy similares, se lo intenta convencer para que llame a un número telefónico indicado en el mensaje. Al llamar a dicho número, un sistema automatizado, haciéndose pasar por la organización, le solicitará sus datos personales, los que luego serán utilizados sin su autorización, con las previsibles consecuencias gravosas.

Medidas de prevención para evitar ser víctima del "phishing"

Las siguientes medidas buscan asistirlo para minimizar los efectos negativos de un ataque de "phishing" y de ser posible, impedirlo:

- **Si recibe un correo electrónico que le pide información personal o financiera, no responda. Si el mensaje lo invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo haga.** Las organizaciones que trabajan seriamente están al tanto de este tipo de fraudes y por consiguiente, no solicitan información por medio del correo electrónico. Tampoco lo contactan telefónicamente, ni mediante mensajes SMS o por fax. Si le preocupa el estado de la cuenta que posee en la organización que dice haber enviado el correo, o que lo ha contactado, comuníquese directamente utilizando un número telefónico conocido y provisto por la entidad u obtenido a través de medios confiables, como por ejemplo de su último resumen de cuenta. Alternativamente, puede ingresar en la página oficial de la organización, ingresando usted mismo la dirección de Internet correspondiente en el navegador.

- **No envíe información personal usando mensajes de correo electrónico.** El correo electrónico, si no se utilizan técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial. Para mayor información sobre recomendaciones para el uso del correo electrónico seguro, puede consultar en http://www.arcert.gov.ar/webs/tips/
- **No acceda desde lugares públicos.** En la medida de lo posible, evite ingresar al sitio web de una entidad financiera o de comercio electrónico desde un cyber-café, locutorio u otro lugar público. Las PCs instaladas en estos lugares podrían contener software o hardware malicioso destinado a capturar sus datos personales.
- **Verifique los indicadores de seguridad del sitio web en el cuál ingresará información personal.** Si es **indispensable** realizar un trámite o proveer información personal a una organización por medio de su sitio web, escriba la dirección web usted mismo en el navegador y busque los indicadores de seguridad del sitio. Al acceder al sitio web, usted deberá notar que la dirección web comienza con "https://", donde la "s" indica que la transmisión de información es "segura". Verifique también que en la parte inferior de su navegador aparezca un candado cerrado. Haciendo clic sobre ese candado, podrá comprobar la validez del certificado digital y obtener información sobre la identidad del sitio web al que está accediendo.
- **Mantenga actualizado el software de su PC:** Instale las actualizaciones de seguridad de su sistema operativo y de todas las aplicaciones que utiliza, especialmente las de su producto antivirus, su cliente web y de correo electrónico. La mayoría de los sistemas actuales permiten configurar estas actualizaciones en forma automática.
- **Revise sus resúmenes bancarios y de tarjeta de crédito tan pronto los reciba.** Si detecta cargos u operaciones no autorizadas, comuníquese de inmediato con la organización emisora. También contáctese con ella si se produce una demora inusual en la recepción del resumen.
- **No descargue ni abra archivos de fuentes no confiables.** Estos archivos pueden tener virus o software malicioso que podrían permitir a un atacante acceder a su computadora y por lo tanto, a toda la información que almacene o introduzca en ésta.

Recuerde - No conteste ningún mensaje que resulte sospechoso. Si un mensaje en su contestador le avisa sobre un evento adverso vinculado a su cuenta bancaria y le solicita que llame a un teléfono gratuito, no lo haga. Si recibe un correo electrónico que le pide lo mismo, no lo crea. Si del mismo modo le envían un SMS de bienvenida a un servicio que no ha contratado, bórrelo y olvídese. Las mencionadas prácticas no son sino diversas modalidades que persiguen el mismo fin: obtener sus datos personales para defraudarlo.

Finalmente - Permanezca siempre atento para evitar el acceso indebido a su información personal. Observamos que día a día aparecen nuevas estrategias de engaño. Su desconfianza y el cuidado con que analiza los sitios web en los que ingresa sus datos de identidad, son su mejor protección.

Si detecta o sospecha que ha sido víctima de un ataque de "phishing", reenvíenos el mensaje de correo electrónico y toda información que considere que puede ser de utilidad a: "**mailinfo@arcert.gov.ar**". Con esa información, ArCERT arbitrará todos los medios a su alcance para neutralizar el ataque y evitar que otras personas puedan verse afectadas.