

Por qué funciona el phishing

Varios miembros de la universidad de Harvard y Berkeley han publicado un informe con un sugerente título: "Por qué funciona el phishing". No es una pregunta, sino una rotunda afirmación. Mediante una prueba realizada a varios usuarios, han estudiado los diferentes factores que ayudan a que el phishing siga siendo una actividad rentable hoy en día.

Rachna Dhamija, J. D. Tygar, y Marti Hearst han publicado un interesante informe sobre el porqué del éxito del phishing. La prueba empírica, realizada sobre 22 estudiantes o personal de la universidad, ponía a prueba su capacidad de discernir entre la autenticidad de 20 páginas distintas. Varias reales, varias ataques típicos y otras copias realizadas expresamente y destinadas a engañarlos.

El informe es extenso y describe con detalle las situaciones (incluso anécdotas) que se dieron durante el estudio. De entre ellas, llaman la atención poderosamente algunas creencias y actitudes de los usuarios. Si bien 22 voluntarios no representa una cantidad como para extrapolar datos, me temo que refleja muy bien la actitud de miles de usuarios y, en cualquiera de los casos, explica el aumento de este tipo de ataques.

A grandes rasgos, las páginas de phishing engañaron al 90% de los participantes. Las alertas del navegador resultaron del todo ineficaces. El 23% de los participantes ni siquiera observaron las diferencias en la barra de direcciones (usaron Firefox para la prueba), la barra de estado o cualquier otro indicador de seguridad. De media, los participantes fallaron el 40% de las veces. El estudio concluye que no se puede establecer una estadística clara en correlación con los estudios, edad, sexo o experiencia previa para hablar de exposición ante ataques phishing.

Hasta aquí, los datos sorprenderán más o menos, pero no dejan de ser un reflejo de lo que puede estar ocurriendo ahí fuera. Hay que tener en cuenta que el estudio pretende conocer qué capacidad de distinción entre páginas reales y fraudulentas tienen los usuarios, no averiguar quiénes contestarían alegremente a cualquier email que cayera en su casilla de correo pidiendo datos sensibles (forma habitual de que los ataques de phishing capten víctimas)

Lo interesante del estudio se encuentra en las pequeñas anécdotas y "técnicas antiphishing", propias de los usuarios, que salieron a la luz. Varios de los participantes daban por sentado que el simple hecho de que la página tuviera un aspecto "profesional" garantizaba su legitimidad. Anuncios e imágenes animadas eran prueba, para ellos, de que se trataba realmente de la página del lugar que esperaban ver.

Uno de los usuarios pensaba que el hecho de que apareciese un candado en el navegador indicaba que la página no podía leer contraseñas o incrustar cookies. Las alertas en forma de ventanas emergentes fueron cerradas por la mitad de los usuarios sin ser leídas. El 23% usaban sólo el contenido de la página para evaluar su autenticidad, ningún elemento del navegador que no fuera la propia página mostrada les resultaba útil o comprensible.

Dos participantes sólo desconfiaban de una página si les pedía datos más allá del usuario y la contraseña. Uno de ellos incluso introdujo en una de las muestras su usuario y contraseña para verificar que era la página donde tenía su cuenta. Esta estrategia obedecía a la lógica de que si fuese un sitio fraudulento pediría datos bancarios, pues las contraseñas no son lo importante, sino los datos bancarios en sí.

También fueron curiosas las reacciones ante una réplica exacta de la página de Bank of the West, bajo el dominio "www.bankofthevest.com" (con dos "v" en vez de una "w"). Al ser una réplica exacta, el hecho de que apareciera un simpático oso (hubiese sido muy complicado de copiar, dijo algún participante) en el diseño y su "look" profesional (en realidad era una copia exacta del original), convencieron a la mayoría de que era legítima. Sólo la usuaria de mayor edad sin conocimientos mínimos de seguridad, detectó el error en el nombre de dominio.

Incluso uno de los usuarios, que hacía caso a todos los mínimos requerimientos de seguridad para comprobar si una página era legítima (excepto examinar los certificados) juzgó mal una de las 19 páginas.

Lo peor es que en general, en una escala de 1 a 5, estaban bastante seguros de sus decisiones en un valor de media de 3. No sólo demostraron no saber lo que hacían, sino además, afirmaban estar suficientemente seguros de lo que estaban haciendo.

El experimento viene a recordar una vez más dónde se encuentra el punto débil de la cadena de seguridad. El desconocimiento en general de qué es un sistema informático en red, qué es Internet o cómo funciona la seguridad, es la causa principal de que otros muchos puedan robar impunemente los datos sensibles de usuarios incautos. No se puede luchar contra un problema del que no se tiene conciencia, aunque el problema afecte de lleno a un medio que se usa todos los días. Aunque alertas, navegadores más seguros y sistemas operativos más controlados ayuden a mitigar el problema, es imposible defenderse de algo que ni siquiera se conoce... de hecho, siete participantes nunca habían oído la palabra "phishing" antes del experimento.

Opina sobre esta noticia: <http://www.hispasec.com/unaaldia/2782/comentar>

Más información:

Why Phishing Works

http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

Sergio de los Santos
ssantos@hispasec.com