VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Ingeniería social
- Detectar y detener ataques de ingeniería social
- Prevenir ataques futuros

Ingeniería social

Resumen

Una percepción errónea que la gente tiene sobre ciberataques es que sólo se requiere de herramientas y tecnologías avanzadas de hackeo para poder irrumpir en las computadoras, dispositivos móviles o cuentas de los usuarios. Eso no es cierto, así de simple. Los ciberatacantes han aprendido que una de las maneras más fáciles de robar tu información o de hackear tu computadora es simplemente usando las palabras para engañarte. En este boletín aprenderemos cómo funcionan los ataques enfocados a la persona (conocidos como ingeniería social) y qué puedes hacer para protegerte.

Editor Invitado

Alissa Torres es instructora certificada del SANS especializada en cómputo forense avanzado y en respuesta a incidentes. Su experiencia en la industria incluye colaborar como responsable directa en manejo de incidentes y trabajar para un equipo de seguridad interna como investigadora forense. Encuentra a Alissa en Twitter como **@sibertor**.

Ingeniería social

La ingeniería social es un tipo de ataque psicológico donde alguien, con engaños, te lleva a hacer lo que él desea. Ha existido desde hace miles de años, la idea de engañar o burlar a alguien no es nueva. De cualquier forma, los ciberatacantes han aprendido que utilizar esta técnica en Internet es realmente efectiva y que puede ser utilizada para dirigirse a millones de personas. La manera más simple de entender la ingeniería social es aprender de un ejemplo común que sucede en la vida real.

Supongamos que recibes una llamada de alguien que dice hablar de parte de una compañía de soporte a equipos de cómputo, tal vez de tu proveedor de servicios de Internet o del soporte técnico de Microsoft. Quien llama dice que ha notado que tu computadora se comporta de manera extraña, por ejemplo, haciendo escaneos en Internet o enviando correo basura, dice creer que tu equipo está infectado. Según esa persona, se le ha pedido investigar el asunto para ayudarte a mantener tu equipo seguro y utilizará una gama de términos técnicos que te llevarán a pasos confusos, todo con tal de convencerte de que tu computadora está infectada.

Es posible que te pida checar si tienes ciertos archivos en tu computadora y guiarte en cómo encontrarlos, cuando tú localices esos archivos, el atacante se asegurará de que creas que ese es un claro signo de que estás infectado, a pesar de que esos archivos no son otra cosa que documentos del sistema que encontrarías en cualquier computadora. Una vez que logre hacerte creer que tu equipo está infectado, te presionará para que vayas a un sitio web y adquieras su software de seguridad o para que le permitas acceso remoto a tu computadora,

Ingeniería social

de cualquier forma tendrás que pagar para que lo haga. Si le permites acceso a tu equipo, lejos de repararla, la infectará una vez estando ahí.

Toma en cuenta que los ataques de ingeniería social no se limitan a llamadas telefónicas, pueden suceder en prácticamente cualquier tecnología, incluyendo ataques de phishing por correo electrónico, mensajes de texto, publicaciones en Facebook o Twitter, chats en línea y muchos otros. La clave está en saber en qué poner atención.

Aprender cómo prevenir, detectar y detener ataques de ingeniería social es una de las formas más efectivas que tienes para protegerte.

Detectar y detener ataques de ingeniería social

La forma más simple de defenderte contra los ataques de ingeniería social es usar el sentido común. Si algo parece sospechoso o no da la impresión de estar bien, puede ser un ataque. Algunos indicadores comunes de ingeniería social incluyen:

- Alguien que imprime un gran sentido de urgencia. Si te sientes bajo la presión de tomar una decisión en ese mismo momento entonces debes sospechar.
- Alguien pidiendo información a la que no debería tener acceso o a la que supuestamente ya debería conocer.
- Algo demasiado bueno para ser verdad. Un ejemplo común es cuando te notifican que ganaste la lotería, incluso cuando jamás la has jugado.

Si sospechas que alguien está intentando hacerte víctima de un ataque de ingeniería social, corta toda comunicación con esa persona. Si es alguien que te está llamando por teléfono, cuelga. Si es por algún chat, termina la conexión. Si es un correo en el que no confías, bórralo. Si el ataque se relaciona con tu trabajo, asegúrate de reportarlo con el área de soporte o con el equipo de seguridad de la información lo más pronto posible.

Prevenir ataques futuros

Afortunadamente existen algunas precauciones que puedes tomar para prevenir exponerte a futuros ataques de ingeniería social.

- **Nunca compartas contraseñas**. Ninguna organización te contactará para pedirte contraseñas, si alguien la solicita, es un ataque.

Ingeniería social

- **No compartas demasiado**. Cuanto más sabe el atacante de ti, más fácil le será poder engañarte. Cuanto menos cosas hagas públicas (eso incluye pequeños detalles sobre ti como redes sociales, comentarios en páginas o en foros públicos, listas de correo, etc.) es menos probable que alguien te ataque.

- **Verifica los contactos**. En ocasiones tu banco, tu compañía de tarjetas de crédito, tu proveedor de telefonía o alguna otra organización o servicio podrían contactarte por razones legítimas. Si tienes dudas de la solicitud que te están haciendo, pregunta a la persona que te está contactando por su nombre y su teléfono. Después busca esos datos de la compañía en una fuente confiable, como el número en la parte de atrás de tu tarjeta, en tu estado de cuenta, o quizá directamente en el sitio web de la compañía (asegúrate de ingresar tú mismo la dirección). De esta forma, cuando tú llamas a la organización, sabes que realmente estás hablando con ellos. Aunque podría parecer molesto, podrás agregar un paso extra a proteger tu identidad personal y tu información.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Phishing por correo electrónico:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_sp.pdf
Redes sociales de manera segura:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201303_sp.pdf
Evitar estafas:	http://www.alertaenlinea.gov/topics/evite-estafas
Consejos de seguridad:	http://www.seguridad.unam.mx/usuario-casero/consejos/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Jazmín López

