Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Estafas en llamadas de soporte técnico

EDITOR INVITADO

Lenny Zeltser es el editor invitado para esta edición. Lenny se encarga de proteger las operaciones de TI de sus clientes en NCR Corp y enseña técnicas de combate contra malware en el SANS Institute. Puedes encontrarlo en Twitter como @lennyzeltser y consultar su blog de seguridad en blog.seltzser.com

RESUMEN

Detrás de muchos ciberataques, se encuentran los criminales que buscan engañarte para sacarte dinero, o para que les des información personal. Ejemplos comunes de esto son los correos fraudulentos llamados phishing, que fingen venir de una persona o compañía en la que confías, como alguno de tus amigos o tu banco. Aunque tales ataques siguen siendo una amenaza, los criminales ahora también llaman a sus víctimas potenciales por teléfono. En este boletín explicamos cómo operan estas estafas telefónicas, específicamente aquellas relacionadas a soporte técnico; y qué puedes hacer para protegerte.

LA ESTAFA

No existen estafas iguales, aunque usualmente incluyen muchos de los elementos que leerás a continuación: Recibes una llamada telefónica de una persona que dice ser de una compañía de soporte técnico asociada con Microsoft u otra empresa legítima. Al estar escaneando Internet, ellos dicen haber detectado que tu equipo se comporta de forma inusual y que creen que está infectada con un virus. Te explican que están investigando el caso por lo que te ofrecen revisar tu equipo. Los estafadores utilizan una variedad de términos técnicos con los que te hacen pasar por una serie de pasos confusos para hacerte creer que tu equipo está infectado y que, finalmente, adquieras el producto que están vendiendo.

Por ejemplo, podrían comenzar pidiéndote que descargues e instales un software de su sitio web, o que utilices servicios en línea que les darán acceso remoto a tu equipo para que puedan confirmar y corregir el problema. Estas herramientas usualmente son herramientas de acceso remoto legítimas como LogMeIn.com o ShowMyPC.com, así que no recibirás alertas de tu software antivirus. Contigo al teléfono, los maleantes te dirigirán a través de varios programas y configuraciones en tu computadora. La persona intentará convencerte de que él o ella está realizando acciones para investigar la infección que supuestamente aflige a tu computadora. Incluso, puede comenzar a deshabilitar servicios legítimos, que siempre están presentes en computadoras con Windows, indicando que dichos servicios son programas maliciosos. Al deshabilitar o incluso debilitar tu equipo, están intentado asustarte para que creas que efectivamente está infectado y que la única manera de corregir el problema es comprar

Estafas en llamadas de soporte técnico

su producto o pagar una costosa suma por su servicio de suscripción anual. Su meta es obtener control de tu computadora, quitarte tu dinero y potencialmente, obtener tu información personal.

Recuerda, cada cosa que te digan estas personas es una mentira, no caigas en sus engaños. La razón por la que los criminales utilizan el teléfono es que existe muy poca tecnología que podría protegerte de este tipo de ataques. Además, las llamadas telefónicas son una poderosa herramienta para que los criminales transmitan emociones y sentido de urgencia, aumentando las posibilidades de tener éxito en su estafa. Por lo tanto, la mejor protección contra estos ataques no es una solución tecnológica, eres tú mismo.

¿CÓMO PROTEGERSE?

Es posible que en ocasiones, las compañías legítimas que utilizas (como un banco) te llamen por teléfono para confirmar información de tu cuenta o para mantenerte al tanto de alguna compra. El reto es determinar cuándo estas llamadas son de compañías legítimas, y cuándo son engaños. Aquí hay algunos pasos clave para protegerte:

- Cuando alguien te pida información por teléfono, o te pida realizar alguna actividad, sé desconfiado y confirma su identidad antes que nada. Pregúntales en qué compañía trabajan. Si nunca has escuchado de su empresa antes, es probable que se trate de un engaño. Si es legítima y ya has escuchado de ella, diles que no es un buen momento para la llamada y solicítales su nombre y número de empleado, para poder regresarles la llamada. Luego visita el sitio web de la compañía o cualquier información que tengas en archivo, obtén el número telefónico y regresa la llamada.

Sospecha de cualquier persona que llame pidiendo acceso remoto a tu equipo o que te presione a comprar sus productos de seguridad informática, estas llamadas son probablemente un intento de estafa.

- Si la persona al teléfono intenta crear sensación de urgencia o ejercer presión para que actúes inmediatamente, no confíes en ellos, es muy probable que sea una estafa.

Estafas en Llamadas de Soporte Técnico

- No dependas únicamente del identificador de llamadas para autenticar a quien llama. Es fácil para los criminales engañar a este servicio, incluso crear identificaciones falsas, para que puedan fingir que llaman de una compañía legítima cuando en realidad no es así.
- Nunca entregues tu contraseña por teléfono. Ninguna organización legítima te pedirá alguna vez tu contraseña.
- Nunca des a una organización información que ya deberían poseer. Por ejemplo, si tu banco llama, la persona al teléfono debería tener ya tu número de cuenta.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! Siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando permiso antes de abrirlo.

Grabación en video de una estafa de soporte técnico (en inglés): http://preview.tinyurl.com/cbg9kku

Comentarios de Microsoft sobre estafas de soporte técnico: http://preview.tinyurl.com/7vqjmd8

Encuesta del ISC sobre estafas de soporte técnico (en inglés): https://isc.sans.edu/reportfakecall.html

Más información: http://preview.tinyurl.com/6rholuy

Reporta:
incidentes@seguridad.unam.mx
cert-mx@ssp.gob.mx

Tip del día en seguridad del Instituto SANS: http://preview.tinyurl.com/6s2wrkp

Consejos UNAM-CERT: http://preview.tinyurl.com/consejos-unamcert

Términos de seguridad en español: http://preview.tinyurl.com/6qpm9q4

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Sergio Becerril, Tonatihu Sánchez, Célica Martínez, Jazmín López