SANS SECURITY AWARENESS

OUCH!

Boletín mensual de seguridad para todos

Ataques telefónicos y engaños

Resumen

Cuando piensas en cibercriminales, probablemente piensas en una mente siniestra sentada detrás de una computadora lanzando ataques sofisticados en Internet. Mientras que muchos cibercriminales de la actualidad sí utilizan tecnologías como el correo electrónico o la mensajería instantánea, los chicos malos también usan el teléfono para engañar a sus víctimas. Existen dos grandes ventajas para utilizar un teléfono. Primero, a diferencia del correo electrónico, hay menos tecnologías de seguridad que monitorean llamadas telefónicas y que pueden detectar y detener un ataque. Segundo, es mucho más fácil para los actores maliciosos revelar emociones a través del teléfono, lo cual hace que sea más probable su éxito al engañar a las víctimas. Aprendamos cómo podemos detectar y detener este tipo de ataques.

¿Cómo funcionan los ataques telefónicos?

En primer lugar, debes comprender lo que buscan los atacantes. Usualmente están detrás de tu dinero, tu información o acceso a tu computadora, o de los tres. Su forma de lograrlo es engañándote para que hagas algo que ellos desean. Los actores maliciosos llaman a gente alrededor del mundo, creando situaciones que parecen urgentes. Quieren tomarte desprevenido al asustarte para que no pienses claramente y así orillarte a cometer un error. Algunos de los ejemplos más comunes incluyen:

El interlocutor pretende ser parte del servicio gubernamental de recaudación fiscal y te advierten que hay impuestos incumplidos de tu parte. Explican que si no pagas tus impuestos de inmediato podrías ir a prisión, y así te presionan para pagar con tu tarjeta de crédito por medio del teléfono. Esto es un engaño, puesto que los departamentos fiscales nunca llaman o escriben a las personas. Todas las notificaciones oficiales se envían por correo tradicional.

El interlocutor pretende llamar desde el servicio de soporte técnico de Microsoft y explican que tu computadora está infectada. Una vez que te han convencido, te presionan para que compres su software o para que les otorgues acceso remoto a tu computadora. Sin embargo, Microsoft nunca te llamaría a casa.

Recibes un mensaje de voz automatizado asegurando que tu cuenta bancaria ha sido cancelada, y que debes regresar la llamada a un número para reactivarla. Cuando llamas, contactas a un sistema automático que te solicita confirmar tu identidad y pregunta por todo tipo de información privada. Pero no se trata de tu banco, solo están registrando toda tu información para cometer robo de identidad.

Protégete a ti mismo

La mejor defensa contra los ataques telefónicos eres tú mismo. Mantén esto en mente.

Cada vez que alguien llama creando un sentido de urgencia exagerado y te presiona para que realices una acción, sospecha. Incluso si la llamada parece legítima al principio, pero después comienza a sentirse extraña, puedes detenerla y decir "no" en cualquier momento.

Si crees que una llamada telefónica es un ataque, simplemente cuelga. Si deseas confirmar si el número telefónico es legítimo, dirígete al sitio de la organización (como tu banco) y obtén el número de asistencia al consumidor para que puedas llamarlos directamente. De esta manera sabrás a ciencia cierta si estás hablando con la organización real.

Nunca confíes en los identificadores de llamadas, los cibercriminales a menudo falsifican el número para que parezcan provenir de una organización legítima o tengan el mismo código de área que tu número telefónico.

Nunca permitas que un interlocutor tome control temporal de tu computadora o que te engañe para descargar software. Así es como los actores maliciosos logran infectar tu computadora.

Si una llamada telefónica proviene de alguien que no conoces personalmente, deja que la llamada vaya al buzón de voz. De esta manera puedes revisar las llamadas desconocidas cuando quieras. Mejor aún, en muchos teléfonos puedes habilitar esta función por defecto con la función de "No molestar".

Los engaños y ataques vía telefónica están al alza. Tú eres la mejor defensa a tu disposición para detectar y detenerlas.

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

Editor Invitado

Jen Fox *ofrece servicios de concientización de seguridad, ingeniería social y evaluación de riesgo como consultora senior en All Covered. Puedes encontrarla en Twitter como* @J_Fox.

Recursos

Guía para proteger y usar de forma segura su móvil:
https://www.incibe.es/extfrontinteco/img/File/intecocert/Proteccion/usoseguromoviles.pdf

Robo de identidad y consecuencias sociales: https://www.seguridad.unam.mx/robo-de-identidad-y-consecuencias-sociales

Ingeniería social: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf