www.psicoadolescencia.com.ar

La técnica de ciberengaño que más crece

Las técnicas de los criminales para obtener información confidencial y otros riesgos para la seguridad y privacidad informática.

Una de las técnicas de engaño más habituales es el phishing.

El mayor riesgo para la seguridad informática no está en las máquinas ni en las conexiones, sino en los humanos. Más precisamente en su mente y su vulnerabilidad. Es que el ***phishing*** sigue siendo **formas de ciberataque. unas de las principales**

Se estima que hubo **más de 12,4 millones de víctimas de este tipo de engaño**, basado en ingeniería social, en apenas un año. Así lo afirma un estudio realizado por Google, la Universidad de California, Berkeley y el Instituto Internacional de Ciencias de la Computación.

Qué es el phishing

El término deriva del término en inglés "fishing" ("pescar") y hace alusión a la idea de que la víctima "muerda el anzuelo". La palabra phishing hace referencia a las técnicas de engaño que se usan para adquirir información confidencial (contraseñas, información bancaria o datos de tarjeta bancaria) de forma fraudulenta.

En estos casos, el cibercriminal se hace pasar por un entidad o empresa de confianza y envía un mensaje o correo eléctronico para pedirle al usuario que, por ejemplo, ingrese a un determinado sitio para actualizar sus datos o para verificar su identidad. De ese modo obtienen los datos confidenciales.

Ejemplo de engaños con mensaje de texto Phishing. Así se le pide a la usuaria que ingrese sus datos para acceder a su iCloud.

En otras ocasiones se tienta al usuario con promesas de falsos descuentos, promociones u otros beneficios inexistentes.

El smishing es otra variante de engaño que se basa en el envío de mensajes de textos para obtener información confidencial. El vishing sigue la misma lógica pero el medio empleado es un llamado telefónico.

¿Cómo protegerse de este tipo de engaño?

En principio **hay que correo, mensaje, chat o llamado que se obtenga solicitando directamente datos confidenciales o bien pidiendo que se ingrese a un dudar de cualquier sitio para ingresar datos personales o una contraseña.** En esos casos, lo mejor es contactarse directamente con la supuesta entidad desde donde se recibe el correo (el banco, o lo que fuese) y corroborar si enviaron o no el mail.

Por otra parte, es fundamental contar con más de un factor de autenticación en los correos o acceso a perfiles de redes sociales. Así, al cibercriminal no le bastará con obtener la contraseña para ingresar a las cuentas del usuario.

La verificación en dos pasos: ¿es suficiente?

El robo de credenciales es el truco más viejo y efectivo para los cibercriminales. El doble factor de autenticación suma una capa extra de seguridad pero este método tampoco es infalible, según se destaca en el último informe de Forcepoint donde se detallan las tendencias de crecimiento de ciberamenazas para el próximo año.

"Lo recomendado es contar con una autenticación multi factor: algo que sé (*password* o contraseña); algo que soy (factor biométrico) y algo que tengo (*token*). De esta manera se reduce el riesgo del uso de únicamente un factor que ahora sabemos que, por sí solo, representa un riesgo para nuestra autenticación", explicó Ramón Castillo, Ingeniero de Ventas de Forcepoint para México y América Central, en diálogo con Infobae.

Las fallas de la autenticación biométrica

¿Alcanza usar el rostro o una huella digital para validar la identidad de manera? No es suficiente. Al menos eso queda claro luego de varias muestra de vulnerabilidad.

En 2016, investigadores de la Universidad de Michigan hallaron una forma efectiva de reproducir las huellas digitales con una impresora estándar. Y en 2017, investigadores de la Escuela Tandon de Ingeniería en la Universidad de Nueva York demostraron que podían igualar las huellas dactilares de cualquier persona utilizando "huellas maestras" alteradas digitalmente.

El reconocimiento facial tampoco es del todo efectivo. Cuando el sistema está en el software basta con una fotografía para vulnerarlo y en el caso del sistema de Apple (Face ID) que incluye tomas con cámara infrarroja, también es posible engañarlo con técnicas más sofisticadas.

Los sistemas de autenticación biomética pueden ser vulnerados.

"El reconocimiento facial tiene serias vulnerabilidades, por eso creemos que los hackers van a robar los rostros del público en 2019. De hecho, ya ocurrió, aunque sólo en instancias de investigación. En 2016, los especialistas en seguridad y visión computacional de la Universidad de Carolina del Norte derrotaron los sistemas de reconocimiento facial utilizando fotos digitales disponibles públicamente de las redes sociales y los motores de búsqueda junto con tecnología de realidad virtual móvil", se destaca en el informe de Forcepoint.

Biometría del comportamiento: ¿de qué se trata?

La biometría del comportamiento recurre a los movimientos de la persona para validar su identidad. Se tiene en cuenta la manera en que desplaza el mouse, la forma de tipear e incluso la manera en que manipula el teléfono para reconocer al usuario. Al parecer es prácticamente imposible que un impostor pueda imitar esas acciones.

La combinación de este tipo de elementos biométricos con el doble factor de autenticación ofrece, al menos hasta el momento, mayor seguridad para el usuario.

Cuando se intercepta la comunicación

Los dispositivos conectados pueden ser atacados valiéndose de vulnerabilidades en el hardware y la infraestructura en la nube. Este tipo de ataques afecta a varios dispositivos conectados en la red y así resulta más efectivo para el atacante.

Los ataques M*an in the middle* (hombre en el medio) representan un riesgo para las conexiones. Así se llama a la técnica por la cual se introduce un intermediario en la comunicación entre el usuario y la fuente, que puede ser un correo o página. Esto se puede hacer, por ejemplo, empleando un router malicioso para que parezca legítimo o bien utilizando una vulnerabilidad para afectar la comunicación.

También se puede usar esta técnica para interceptar el navegador de la víctima (*Man in the browser*)."Se puede usar para robo de información con scams por ejemplo (clones de sitios originales con fines maliciosos); inclusive permite inyectar código malicioso para tomar control del equipo de la víctima", según se destaca en el sitio We Live Security de Eset.

Las técnicas de ingeniería social se usan, entre otras cosas, para obtener datos de tarjetas de crédito.

Qué medidas de precaución tomar

● En primera media, estar conscientes de los riesgos cibernéticos que hay y educar para que la población tome precauciones en general sobre este asunto.

● Desconfiar de los correos o mensajes que solicitan datos personales. Ser conscientes de que los sitios a los que se remiten pueden ser falsos

● Mantener el software actualizado y tener una solución de seguridad instalada

● Utilizar la autenticación multifactor, tal como se mencionó anteriormente

● Evitar conectarse a redes wifi públicas (en lo posible) porque la comunicación puede ser fácilmente interceptada.

● Usar VPN siempre o al menos al conectarse a una wifi pública. "Si nos preocupa nuestra privacidad y seguridad, sobre todo cuando se están utilizando redes públicas, definitivamente es una recomendación, ya que nuestros datos viajarán protegidos a los ojos de extraños husmeando las redes en busca de información que puedan explotar", concluyó Castillo.

Por Desirée Jaimovich
13 de noviembre de 2018
djaimovich@infobae.com

MÁS SOBRE ESTE TEMA:

Cuentas bancarias en la mira: 9 de cada 10 entidades financieras en América Latina fueron blanco de ciberataques en el último año

Cuál es la técnica de engaño que se usa para robar iPhones

Idearon un cable USB que permite hacer ciberataques a la distancia y buscan financiamiento colectivo para seguir con este proyecto