Delitos informáticos con Ingeniería Social y Phishing.

Instrucciones. El alumno deberá investigar los delitos informáticos reales y documentados en el mundo que hayan utilizado ingeniería social y de Phishing, del 2012 en adelante, el cual también será discutido en clase.

La ingeniería social y el Phishing han sido técnicas históricamente utilizadas por los delincuentes informáticos para realizar delitos a su conveniencia, obteniendo datos, dinero, etc., para su beneficio, o para fines filosóficos y/o políticos, de formas a veces tan simples que hasta las grandes compañías han sido trucadas para caer en este tipo de manipulación.

Uno de estos casos fue la estafa realizada a **Google** y **Facebook** a las que le fue estafado una suma que ronda los 100 millones de dólares estadounidenses, dejando en claro que ni siquiera las compañías de tecnología más grande del mundo se salvan de este tipo de ataques que han evolucionado a formas tan sofisticadas de fraude.

Este ataque fue realizado entre 2013 y 2015 por un hombre de Lituania llamado Evaldas Rimasauskas quien se haría pasar por ejecutivo de una empresa ficticia proveedora de hardware asociada con **Quanta**, previamente relacionada con Google y Facebook de esta forma fue que envió correos electrónicos con contratos fraudulentos para crear la falsa impresión de que habían sido enviados por empleados de la compañía y debido a su relación parecían genuinos, fue así como lograría convencer a ambas compañías de pagar 123 millones de dólares en total que repartió en cuentas en varios países del mundo, el gobierno de Lituania lo capturaría meses después y sería extraditado a Estados Unidos por sus crímenes en 2017, posteriormente en 2019 se declaró culpable, donde recibirá alrededor de 30 años en prisión, mientras que Google y Facebook lograron recuperar la mitad del dinero perdido.

A raíz de este tipo de ataques, y siendo este ataque a Google y Facebook uno con los que más se ha estafado dinero, los criminales han tomado conciencia de la enorme cantidad de dinero que pueden sacar utilizando este tipo de estrategias y para junio de 2016, el FBI reportó que en Estados Unidos se han registrado perdidas de 3 mil millones de dólares en compañías que caen en este tipo de fraudes donde fingen relaciones de negocio.

Otro ataque de **Ingeniería Social** reconocido fue el realizado al Departamento de Labor de los Estados Unidos en enero de 2022, diseñado para que los atacantes lograran robar las credenciales de Office 365 de las victimas trabajadoras del Departamento de Labor de manera muy convincente ya que, utilizaron dos métodos para hacerse pasar por correos electrónicos de dicho departamento,

comprando dominios de correo electrónico similares a los utilizados para pasar a través del filtro

de seguridad de emails de la organización, en estos correos se incluía un enlace que redirigía a un sitio fraudulento idéntico al utilizado por el departamento que registraba los datos de inicio de sesión de los empleados, problema que pudo haberse solucionado si la organización hubiera hecho mejor uso de sistemas de seguridad para correos electrónicos.

Referencias:

Cluley, G. (2019, 21 marzo). Google and Facebook scammed out of $123 million by man posing as hardware vendor. The State of Security. https://www.tripwire.com/state-of-security/featured/google-and-facebook-scammed-out-of-123-million-by-man-posing-as-hardware-vendor/

The Top 5 Phishing Scams of all Time. (2021, 15 noviembre). Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/

Rosenthal, M. (2022, 8 febrero). 15 Examples of Social Engineering: Real-World Attacks. Tessian. https://www.tessian.com/blog/examples-of-social-engineering-attacks/