La Amenaza del Phishing y sus Consecuencias

El cibercrimen es una industria de US$600 millones anuales que se proyecta en daños de US$6 trillones para el 2021 según datos de The Cybersecurity Hub. Una de las formas más comunes del este tipo de crimen es el phishing, una amenaza que finge inocuidad, pero representa el inicio del 91% de los ciberataques de acuerdo con datos de Digital Guardian.

El phishing es un método de ingeniería social utilizado para extraer información por medio del engaño y el uso de la tecnología para obtener acceso a aparatos, redes o servicios. Comúnmente finge elementos de confianza o autoridad, y generar credibilidad para enganchar a su víctima.
De acuerdo con la Universidad de Stanford, los criminales que utilizan métodos de phishing usualmente buscan claves, información financiera, robar identidades o dinero. Además, estiman que hay un 10% de probabilidades de que un mensaje de éstos sea exitoso ya que usualmente las personas caen por una ilusión de urgencia, deseo de complacer, ambición o avaricia, curiosidad, miedo o complacencia.

Esta amenaza no es nueva pues los primeros intentos conocidos enfocados en servicios financieros ocurrieron en el 2001 y la modalidad es conocida desde 1987. Tanto instituciones como individuos necesitan tomar conciencia de esta realidad y tratarlo como un riesgo, pues es una amenaza no solamente financiera, si no también reputacional e incluso legal.

Las personas individuales tienen propensión a ser víctimas de phishing al ser embaucados por medio de llamadas telefónicas o al hacer clic en enlaces engañosos que les redirigen a sitios web que han sido clonados, contienen información falsificada, o redirigen desde un sitio legítimo a uno fraudulento. De aquí resultan parte de las pérdidas monetarias por fraude de US$1.48 mil millones reportadas tan solo a la Comisión Federal de Comercio (FTC) de Estados Unidos en 2018 con un incremento de 38% sobre el año anterior.

Sin embargo, las instituciones y algunos individuos están expuestos al spearphishing, una modalidad enfocada a individuos o una compañía que aparenta provenir de una fuente oficial e incluye información específica para aumentar las posibilidades de éxito. De acuerdo con TechRepublic, una de las modalidades de spearphishing más comunes es el “fraude de CEO”, en donde

se solicita información o transferencias monetarias emulando mensajes legítimos del CEO de la institución. McAfee Labs provee datos que indican que el personal de las instituciones es dos veces más propenso a ser atacado que la gerencia y también dos veces más probable de ser engañado.

Tanto instituciones como individuos deben generar conciencia respecto a este riesgo para disminuir sus probabilidades de éxito. Algunas recomendaciones para las instituciones son:

1. Interesar e involucrar a los líderes de la institución.
2. Concientizar en seguridad a los empleados desde el inicio de la relación laboral.
3. Crear un plan formal de entrenamiento.
4. Realizar entrenamientos con escenarios realistas.
5. Resaltar la importancia de la seguridad en el entorno laboral y personal.
6. Evaluar resultados de periódicamente.
7. Comunicar resultados e información relevante.
8. Continuar entrenamientos actualizados.