



Managed secure IT | no matter what

PHISHING

Evitando ataques de ingeniería social y de phishing

www.mexis.net

Autor: Jorge Rubén Macías López
Gerente de Innovación Tecnológica Mexis



PHISHING

Evitando ataques de ingeniería social y de phishing

A principios de 2018, ISACA publicó los resultados anuales de su encuesta acerca del estado de la ciberseguridad en el mundo, y aunque la encuesta arroja algunas buenas noticias relacionadas con una mayor disponibilidad de especialistas que comienzan a reducir el déficit de talento orientado a la ciberseguridad, por otro lado confirmó un problema que genera dolores de cabeza en todas las organizaciones, el elevado nivel de riesgo que resulta del comportamiento humano, específicamente de los comportamientos de las personas que laboran en la empresa o que de manera indirecta tienen acceso a su información. Conforme a los resultados de la encuesta, la ingeniería social se ubica como el tercer vector de ataque más frecuente con el 28% -contra 29% observado en 2017- mientras que el Phishing se consolida como el número uno en este rubro, creciendo de 40 a 44%.

Si bien el Phishing es un vector de ataque que se basa en medios tecnológicos -generalmente un correo electrónico, aunque también suelen utilizarse memorias USB u otro tipo de dispositivos removibles para ataques focalizados, así como variantes que usan mensajes de voz o SMS la realidad es que su efectividad depende totalmente de la reacción que tenga la persona que es objetivo del ataque, ya sea abriendo un archivo adjunto o siguiendo un vínculo en el correo electrónico malicioso, insertando en su equipo de cómputo el dispositivo que contiene el ataque, o acatando cualquier otra instrucción que el atacante proporcione. Bajo esta perspectiva, se pueden sumar los porcentajes, resultando en un 72% de ataques que buscan explotar el exceso de confianza o el nivel de conocimiento inadecuado en términos de ciberseguridad que puede llegar a tener cualquier persona en una organización típica.

Estos riesgos se pueden intentar mitigar invirtiendo grandes cantidades de dinero en tecnologías diversas que buscarán anular las amenazas aun cuando la persona sea engañada; algunas de ellas pueden bloquear los puertos USB de los equipos de cómputo para que no activen dispositivos de almacenamiento pero permitan el uso de otro tipo de periféricos requeridos para la actividad cotidiana, otras aplicarán complejos mecanismos de vieja o nueva generación para detectar los correos de Phishing y evitar que lleguen al usuario, y seguramente habrá quienes cuenten con tecnologías de antimalware diversas que protejan la ejecución de procesos no reconocidos, resguarden la navegación de los usuarios e impidan la descarga de archivos dañinos.



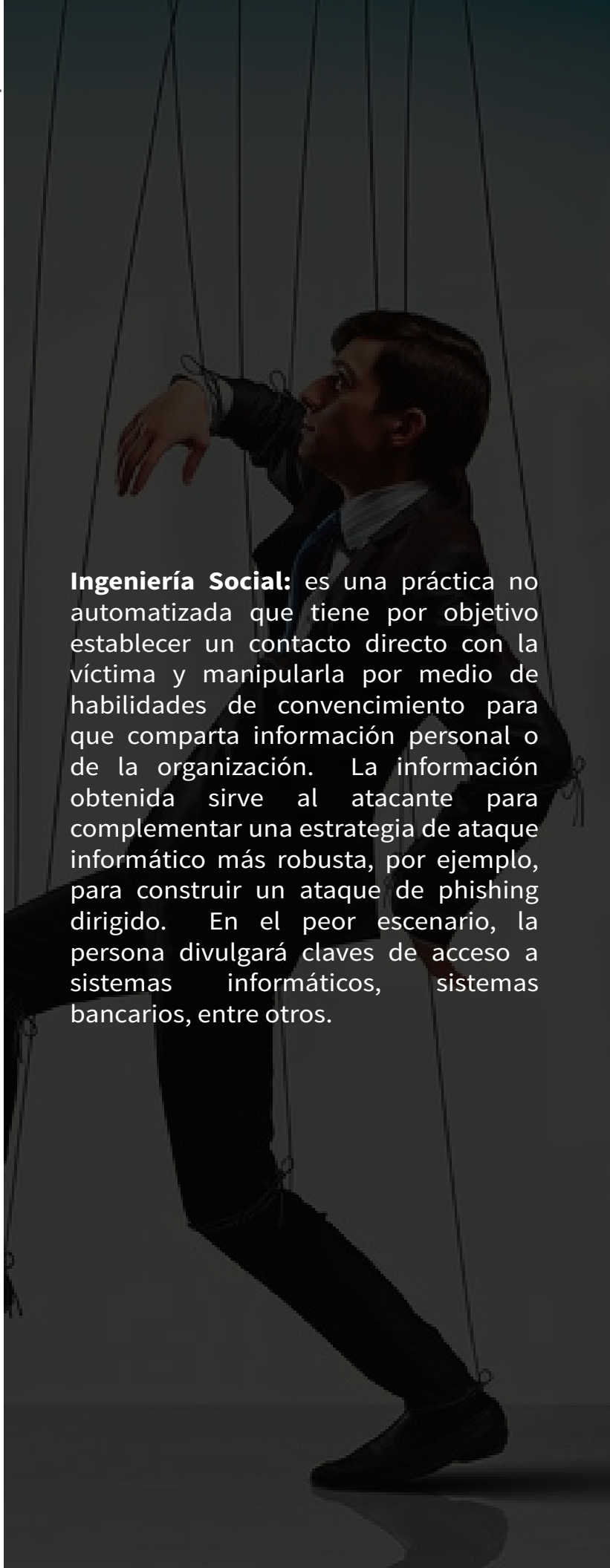
PASSWORD

* * * * *

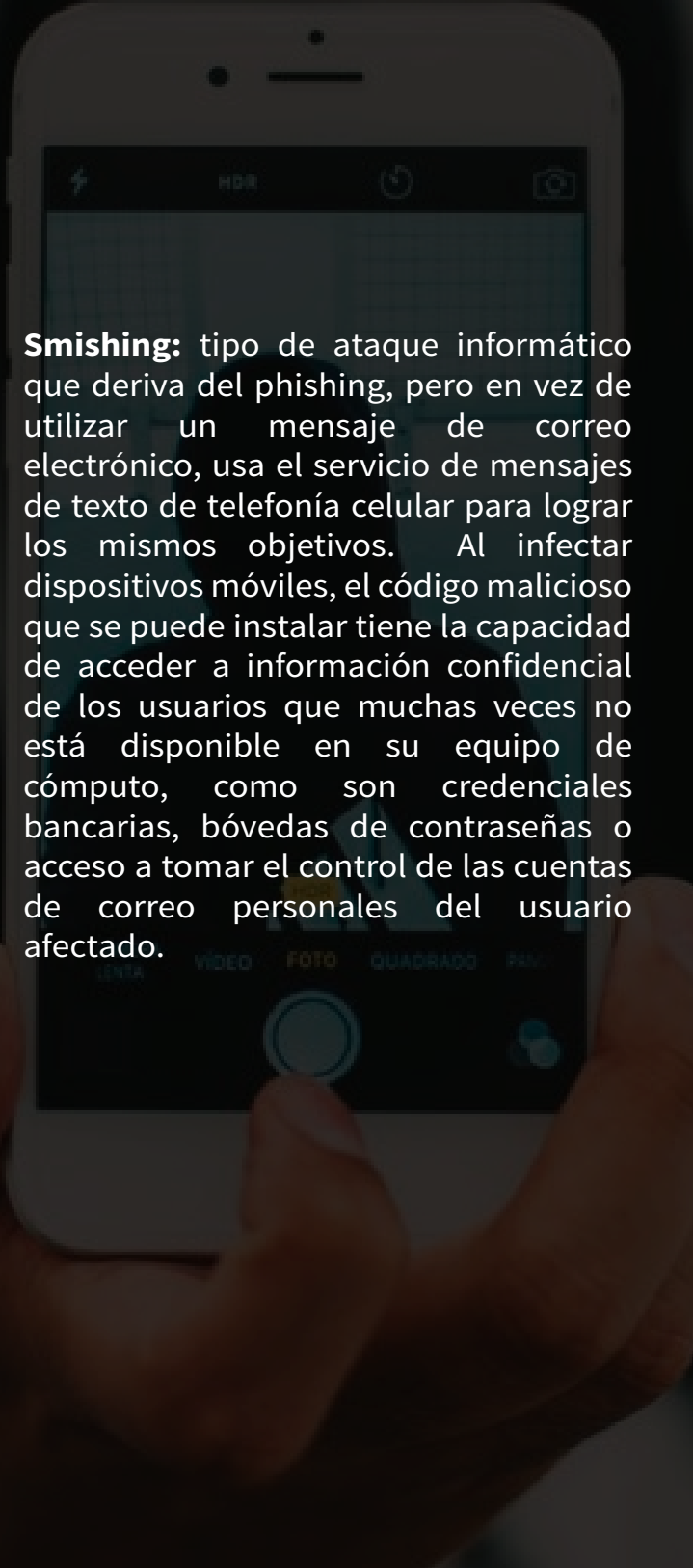
Phishing: ataque informático basado en la suplantación de la identidad de una persona u organización legítima, busca aprovecharse de la confianza de la víctima para inducirlo a seguir instrucciones que lo llevan a sufrir un robo de información como puede ser su contraseña de acceso a algún sistema o servicio, o a ver su equipo de cómputo o dispositivo móvil infectado con un programa malicioso que puede causar aún mayor daño a la persona u organización.

Sin embargo, toda tecnología llega a un punto en el cual pierde su efectividad. El usuario de negocio que necesita urgentemente insertar esa memoria USB en su computadora, con la advertencia de perder un negocio de gran valor para la empresa si no se le permite; existe también el denominado usuario VIP a quien es impensable ponerle restricciones a aquello que puede o no hacer con su equipo de cómputo. Por un lado, la propensión de las tecnologías de seguridad a generar bloqueos en falso y por otro lado, la inercia de las personas que buscan mantener sus métodos ya probados para realizar actividades cotidianas, son ambas fuentes muchas veces de cantidades inmanejables de excepciones en los sistemas de seguridad. Porque, después de todo, si ya se le otorgó a ese usuario el permiso de usar un dispositivo USB en este momento, ¿Para qué quitárselo si después lo volverá a pedir?

Bajo este panorama, la herramienta más efectiva que tienen las organizaciones para dar tratamiento a estos riesgos asociados a la acción humana es lograr modificar los comportamientos de las personas hacia aquellos considerados como seguros, comportamientos que deben darse por convencimiento, mismo que debe nacer del aprendizaje y entendimiento de las amenazas, la manera de detectarlas y las acciones a tomar ante ellas. De aquí la importancia de que las empresas cuenten con programas adecuados de entrenamiento -para los aspectos técnicos que les permitan detectar una amenaza- y concientización -para convencerlos de la importancia de aplicar ese conocimiento técnico adquirido. Programas de entrenamiento adecuados. Tenerlos resulta más complicado de lo que parece.



Ingeniería Social: es una práctica no automatizada que tiene por objetivo establecer un contacto directo con la víctima y manipularla por medio de habilidades de convencimiento para que comparta información personal o de la organización. La información obtenida sirve al atacante para complementar una estrategia de ataque informático más robusta, por ejemplo, para construir un ataque de phishing dirigido. En el peor escenario, la persona divulgará claves de acceso a sistemas informáticos, sistemas bancarios, entre otros.



Smishing: tipo de ataque informático que deriva del phishing, pero en vez de utilizar un mensaje de correo electrónico, usa el servicio de mensajes de texto de telefonía celular para lograr los mismos objetivos. Al infectar dispositivos móviles, el código malicioso que se puede instalar tiene la capacidad de acceder a información confidencial de los usuarios que muchas veces no está disponible en su equipo de cómputo, como son credenciales bancarias, bóvedas de contraseñas o acceso a tomar el control de las cuentas de correo personales del usuario afectado.

¿Qué se requiere para que un programa de entrenamiento y concientización resulte adecuado? Joseph Opacki hace un planteamiento muy acertado en ese sentido en su publicación de 2017 en el Journal de ISACA, “Construyendo una Cultura de Seguridad: ¿Por qué la concientización en seguridad no funciona y qué hacer en su lugar?”. Básicamente, se requiere un programa que parezca todo menos el típico programa de concientización en seguridad. Esto es, las empresas pueden olvidar la idea de llevar a todo su personal en pequeños o grandes grupos una vez al año a escuchar recomendaciones genéricas de seguridad durante dos horas y cumplir así con un lineamiento de seguridad interno o de regulación externa.

Se necesita un entrenamiento que cumpla con las mismas características que el entrenamiento especializado que toda persona recibe para su función laboral específica. Partiendo de evaluar la situación inicial de conocimiento de la persona y los comportamientos que resultan de éste, identificar las condiciones a las cuales está expuesto conforme a sus funciones específicas, poner a su disposición el conocimiento que resulta relevante con base en los dos puntos anteriores, proveerle los escenarios para aplicar el conocimiento adquirido, evaluar el avance logrado en cuanto a sus comportamientos y comenzar de nuevo. Esto es, no todas las personas deben recibir el mismo entrenamiento, primero porque sus conocimientos iniciales son distintos, segundo porque su exposición a las amenazas de seguridad puede no ser la misma y tercero porque cada persona responderá de manera distinta ante cada una de las herramientas de aprendizaje.

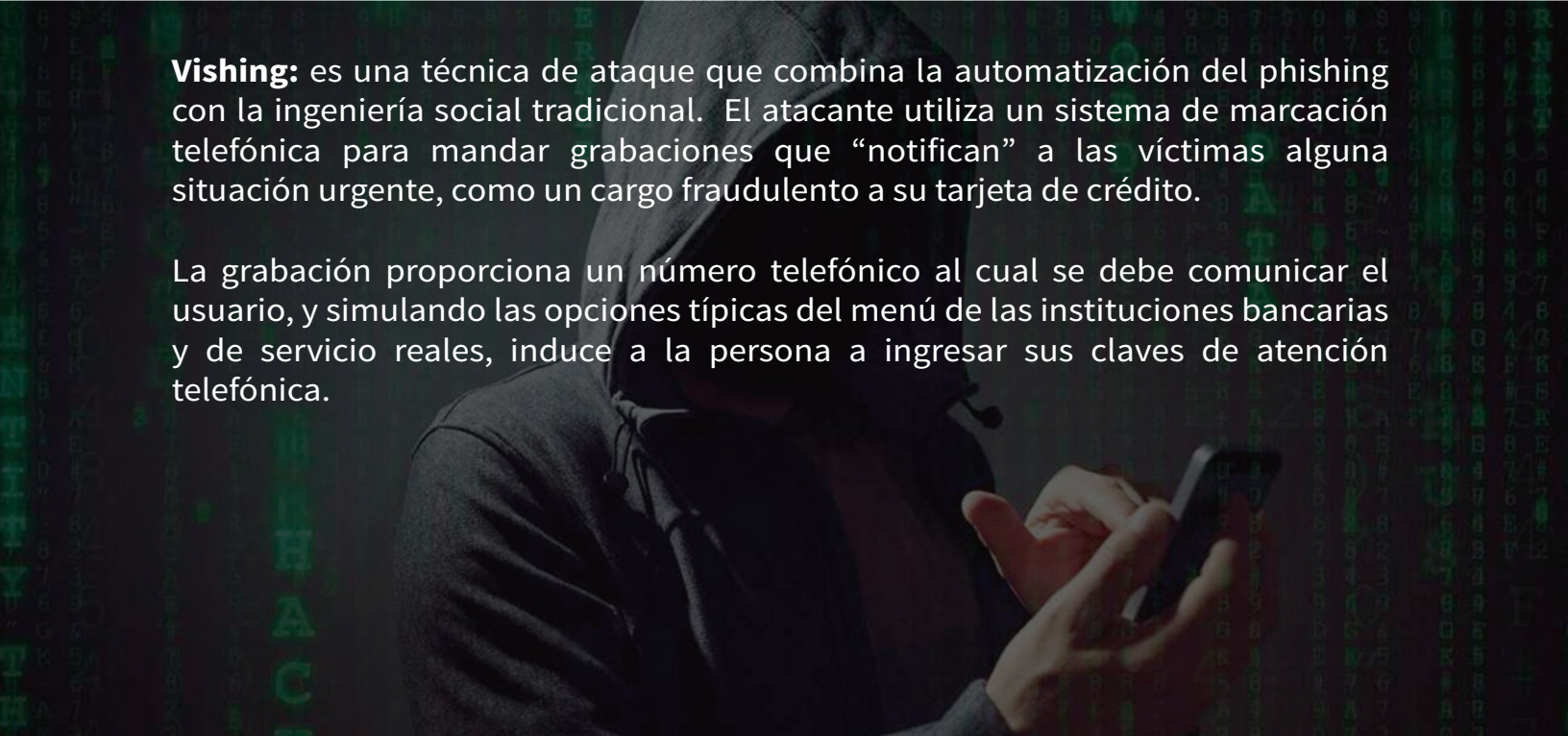
Una de las herramientas más útiles que permiten evaluar el nivel de conocimiento de cada persona, así como observar sus comportamientos ante diversos escenarios de riesgo, es la simulación. Conforme a los vectores de ataque antes mencionados, podemos diferenciar entre dos casos, la simulación de phishing y el hackeo ético de ingeniería social.

En el primer caso, se seleccionan grupos de personas con un perfil de exposición a amenazas común, se construye un correo cuya estructura es equivalente a la de un mensaje de phishing real, se les envía y se identifica quienes de ellos tienen un comportamiento adecuado -eliminan el correo y lo reportan a su área de soporte de TI, por ejemplo- o inadecuado -siguen las instrucciones del correo, ya sea para visitar una página web, ingresar sus credenciales de acceso, descargar y ejecutar un archivo o cualquier otro escenario que se haya simulado.

Mientras que el segundo caso es una tarea más demandante ya que la ingeniería social se debe llevar a cabo de manera individual, una persona objetivo a la vez. Se puede usar una llamada telefónica, o una interacción en persona en una circunstancia inesperada. En cualquier caso, el objetivo es inducir a que la persona revele información de la organización que pueda permitir a un atacante avanzar en su objetivo de causar un daño a la misma. El tipo de información que se puede obtener va desde nombres de personas en puestos clave, descripción de mecanismos de seguridad utilizados, horarios en los cuales se lleva a cabo algún proceso -como un cambio de turno, cuando existe un grado mayor de distracción que puede explotarse-, hasta elementos más puntuales como contraseñas o incluso convencer a la persona de entregar su tarjeta de acceso a las instalaciones.

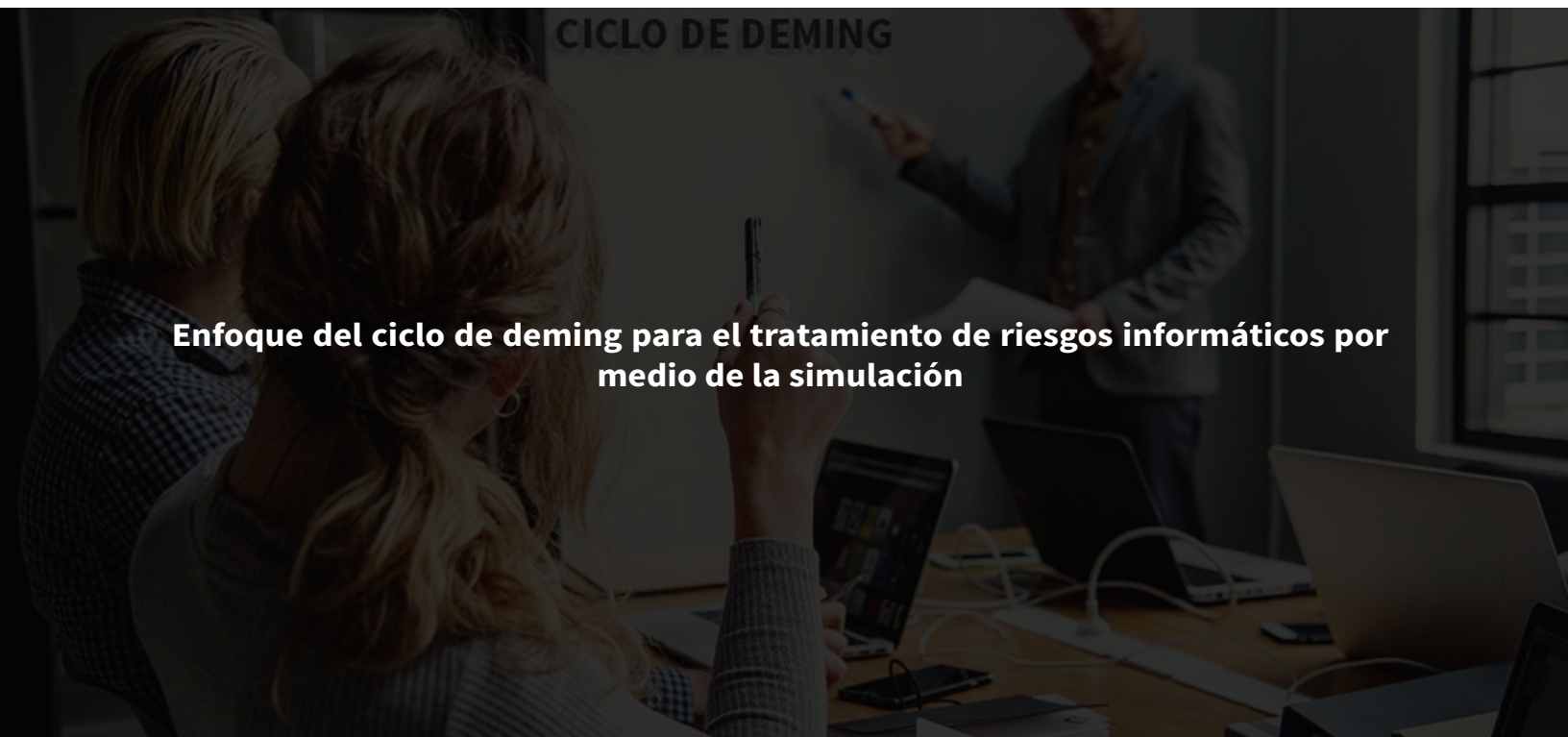
Por su naturaleza masiva, la simulación de Phishing puede usarse continuamente en toda la población, usando campañas dirigidas a segmentos específicos; mientras que la ingeniería social puede reservarse para personas que ocupan posiciones estratégicas en la organización, ya sea por tener un puesto alto en el organigrama, por tener acceso a información sensible, o por trabajar de manera cercana con los anteriores -asistentes o colaboradores directos. También se puede aplicar la ingeniería social ética a aquellas personas cuyos resultados en las simulaciones de phishing determinen un mayor nivel de riesgo.

Las herramientas de simulación mencionadas servirán para registrar los comportamientos de las personas ante los escenarios de amenaza, el siguiente paso es proveerles el entrenamiento adecuado según estos comportamientos. Aquellas personas que no fueron engañadas e incluso notificaron la actividad sospechosa a las instancias adecuadas en la empresa, claramente no requerirán mayor entrenamiento, sino al contrario, pueden recibir reconocimiento por su aportación a la cultura de seguridad. En el otro extremo se encuentran quienes de manera constante logran ser engañados por las simulaciones, y en consecuencia deben recibir entrenamiento por métodos diversos como lecturas, seminarios por internet, cursos interactivos, clases grupales y hasta sesiones de trabajo individuales con un especialista del equipo de seguridad.



Vishing: es una técnica de ataque que combina la automatización del phishing con la ingeniería social tradicional. El atacante utiliza un sistema de marcación telefónica para mandar grabaciones que “notifican” a las víctimas alguna situación urgente, como un cargo fraudulento a su tarjeta de crédito.

La grabación proporciona un número telefónico al cual se debe comunicar el usuario, y simulando las opciones típicas del menú de las instituciones bancarias y de servicio reales, induce a la persona a ingresar sus claves de atención telefónica.



Enfoque del ciclo de deming para el tratamiento de riesgos informáticos por medio de la simulación

Para que estas herramientas generen los beneficios esperados, es importante que los resultados que se van obteniendo al utilizarlas, se ingresen en modelos de evaluación de riesgos, en los cuales se pueda observar la variación de éstos en función de las acciones ejercidas, conforme se realizan simulaciones, las personas van completando sus tareas asignadas de entrenamiento y se observan los cambios de comportamiento, el nivel de riesgo debe ir disminuyendo tanto para los segmentos específicos de personal, como en general. Por otro lado, si las personas no cumplen con sus tareas de entrenamiento o no se observan cambios positivos de comportamiento, el riesgo debería incluso aumentar.

El modelo planteado no es algo nuevo en su mecánico, sino que se trata de implementar un programa que se base en la aplicación del ciclo de mejora continua de deming, conocido como PDCA por sus siglas en inglés (Plan-Do-Check-Act).

Si el trabajo se realiza de forma adecuada, los ciclos de mejora pueden resultar en alcanzar eventualmente un nivel de riesgo residual que ya no pueda ser disminuido, posiblemente porque hacerlo signifique ya un costo financiero o en otros recursos que no se pueda justificar.

Llegar a este punto dependerá de muchas circunstancias, como son la tasa de rotación de personal en la organización -a mayor rotación, mayor necesidad de continuar el ciclo de mejora-, la exposición que la empresa tenga a las amenazas informáticas -que tan probable sea que existan ataques dirigidos en su contra, o que solamente reciba ataques genéricos-, que existan cambios significativos en el entorno tecnológico de la organización - nuevos sistemas de información, cambios en las herramientas de colaboración, implementación de nuevos procesos - o si se requiere la alineación a nuevos marcos regulatorios, estándares o buenas prácticas.

En este caso, lo recomendable es ejecutar algunos ejercicios de simulación periódicos, para monitorear que los comportamientos siguen estando alineados con las prácticas de seguridad de la información requeridas.

Asumiendo que la organización ha llegado al convencimiento de adoptar estas prácticas para dar tratamiento a los riesgos derivados de ataques de phishing e ingeniería social, ¿Cuáles son las alternativas que existen para hacerlo?

Específicamente para el caso de phishing existe siempre la opción de adquirir una herramienta, configurarla y comenzar a ejecutar campañas de simulación. Surgen algunas preguntas ¿Cuál elegir? ¿Por qué? ¿Quién la va a configurar? La oferta tecnológica es muy diversa, aunque con modelos de licenciamiento generalmente rígidos. Las tecnologías reconocidas como “Top” por los analistas de la industria manejan esquemas de licenciamiento perpetuo con usuarios nombrados que pueden representar inversiones cuantiosas. Y eso sin considerar todo el trabajo experto que se requiere, primero para definir cómo se utilizará la herramienta y segundo para ejecutar el ciclo de mejora aprovechándola.

Planear: entender la situación actual y plantear un objetivo de mejora. Para fines prácticos se puede establecer como “lograr una reducción en el nivel de riesgo presente en la organización y asociado a la posible pérdida de información como resultado de ataques de ingeniería social y phishing”. Se debe complementar el estatuto con datos específicos del contexto de la organización, por ejemplo, el historial de este tipo de ataques que la hayan afectado directamente, que sucedieran en su sector, que tuvieran impacto en su cadena de suministro o incluso que sean de impacto global como fue la crisis por ataques de Ransomware en 2017. Conforme al objetivo, se establece un plan de trabajo para realizar campañas de simulación, preferentemente dando prioridad a las áreas, funciones y personas de mayor impacto en la organización con respecto a su acceso a información confidencial o sensible.

Hacer: se lleva a cabo la ejecución de las campañas de simulación, incluyendo sus componentes de entrenamiento y concientización. En esta etapa es necesario que en la organización se perciban el apoyo y la participación de los altos ejecutivos, así como de los líderes informales reconocidos.

Evaluar: se recopila la información de ejecución de la campaña, con sus resultados - personas que fueron víctimas de los ejercicios de simulación, que atendieron sus actividades de entrenamiento, quienes no lo hicieron, quienes contactaron a sus jefes o al área de soporte de TI o de seguridad para reportar las actividades sospechosas, etc- y se ingresan al modelo de evaluación de riesgo, observando de qué manera cambia el mapa de riesgos global, por área o por función.

Actuar: con base en los resultados obtenidos, se debe planear el siguiente ciclo de trabajo. Cada ciclo subsecuente puede ser enfocado en segmentos más específicos de la población, aquellos que siguen representando un nivel de riesgo significativo. Mientras que, para quienes demostraron los comportamientos óptimos se pueden utilizar algunos mensajes de reforzamiento, o incluso se les puede “reclutar” para tener una función de mentores en temas de seguridad informática.

La realidad es que la tecnología es el factor menos importante en este caso. De la misma manera que el objetivo es reducir el riesgo que se deriva del elemento humano de las organizaciones, es también el elemento humano el que resulta clave para la implementación de un programa exitoso. Aspectos clave como el perfilamiento de los grupos de audiencia para dirigir los ejercicios de simulación, la creación de escenarios de simulación que realmente pongan a prueba los criterios para tomar decisiones y actuar de las personas, la generación de contenido de entrenamiento y concientización adecuado para los distintos segmentos de audiencia y la toma de decisiones con base en los resultados observados, no son sujetos para la automatización tecnológica.

Es entonces que adquiere valor y relevancia optar por un servicio consultivo que acompañe a la organización en cada etapa de sus ciclos de mejora.

Uno de los principios que se cuidan es no distraer a la organización de las actividades inherentes a su negocio y dejar que el proveedor de servicio se haga cargo de todas las tareas especializadas que se requieren para gestionar un programa exitoso, planteado con su alcance correcto. No se trata de implementar un “programa de simulación” o “programa de entrenamiento”, sino que se debe contemplar como un programa de gestión de riesgos informáticos asociados al comportamiento humano, mismo que debe estar alineado con el plan maestro de seguridad existente en la organización.

Un servicio consultivo integral debe considerar la generación del modelo de evaluación de riesgos, su actualización continua, el perfilamiento de los grupos de usuarios, el diseño y la ejecución de las simulaciones de phishing y los eventos de hackeo ético de ingeniería social. También debe apoyar a la organización en el desarrollo de los contenidos de entrenamiento y concientización y en la interpretación de los resultados de las distintas acciones. Todo esto, dentro del contexto de la evaluación de riesgos y gestión de la seguridad de la información global de la organización.

En Mexis contamos con el conocimiento experto apoyado en la tecnología, combinación que nos permite ofrecer un servicio modular que puede configurarse a la medida de cada uno de nuestros clientes. Evaluamos la exposición del cliente ante las amenazas de ingeniería social y phishing, analizamos el historial de eventos de seguridad que han afectado a la organización, proponemos, diseñamos, construimos y ejecutamos campañas de simulación que generan información de gran valor para la evaluación de riesgos y la toma de decisiones. Trabajamos con el cliente para implementar un programa de entrenamiento y concientización tan específico como su situación presente lo requiera.

ISACA. (2018). *State of Cybersecurity*.

Opacki, J. (2017 Volumen 4). Building a Security Culture: Why Security Awareness Does Not Work and What to Do Instead. ISACA Journal.

Síguenos en nuestras redes sociales:



MexisMX



Servicios
Administrados
Mexis, S.A. de C.V.



Mexis TI



Servicios
Administrados
Mexis, S.A. de C.V.