Lección 1—Los malos actores

Cada día, a cada hora, personas de todas las edades, en todo el mundo, están en riesgo por consecuencia de amenazas informáticas.

¿Sabes a quién te enfrentas?

Mientras estás viendo este video, encuentro diferentes maneras de engañar a las personas para que me digan sus números de cuenta y contraseñas de forma directa.

A esto yo le llamo PHISHING.

Y así es cómo funciona:

Primero, configuro un servidor web con una página de inicio de sesión que se ve idéntica a la que quiero acceder.

Luego, redirigiré su navegador a la página de inicio de sesión real dónde podrán iniciar sesión y pensar que todo está bien.

Después envío un correo electrónico especialmente diseñado que parezca que fue enviado por el sistema real e incluirá un enlace útil.

Sin embargo, ese enlace no los lleva al sistema real, los lleva a mi servidor web especial que se hace pasar por el sistema real.

Para cuando ingresen al sistema real, tengo sus credenciales y puedo iniciar sesión como ellos. Y la mejor parte… la mayoría de la gente nunca lo sabrá.

Y esto apenas comienza ...

¿Quiénes somos?

Sencillo, somos un grupo motivado por la indignación política, social o moral, que representamos cosas con las que no estamos colectivamente de acuerdo.

Soy el que envía solicitudes de red falsas a nuestras víctimas para atacar lo que se conoce como un Distributed Denial of Service mientras obtenemos millones de computadoras en todo el mundo.

¿Cómo conseguimos todas esas computadoras?

Fácil: creando un botnet.

Un servidor de comando y control accesible en Internet que a través de un malware instalado en algunas computadoras confiadas, esperará pacientemente las instrucciones del servidor de comando y control.

Pero un método común es colocar un instalador de software como un archivo adjunto al correo electrónico no deseado. Digamos... ¿Un error bancario a tu favor?

Cuando abren el archivo adjunto para obtener más información y darse cuenta de que no es real, ya instalamos nuestro software de botnet en su computadora y ... La mejor parte ... no tienen ni idea.

Cada día, a cada hora, personas de todas las edades, en todo el mundo, están en riesgo por consecuencia de amenazas cibernéticas.

¿Nuestra ideología?

Intimidar y sembrar el terror en los corazones de nuestros enemigos, causando trastornos, caos y daños.

¿Sabes quiénes somos?

... Sí, somos ciberterroristas, un grupo que no suele estar bien financiado, pero con un gran ingenio para atacar a nuestros enemigos de alto perfil ...

Capaz de interrumpir los servicios de Internet con ataques DDoS, infiltrarnos en los sistemas para robar datos personales y exponer datos confidenciales de personas que queremos que resulten afectadas. También amenazamos con corromper la información crítica, con la esperanza de destruir industrias enteras.

Pero ... ¿Cómo podemos lograr todo esto con pocos recursos?

Fácil, a través de Spear Phishing.

Una técnica simple en la que enviamos correos electrónicos solo a personas específicas a las que queremos dirigirnos. Una vez que infectamos la computadora que usan, sabemos que podemos llegar a la información más importante, que al final es lo que realmente queremos ...

¿Nuestra motivación?

Lo que mueve al mundo ... ¡EL DINERO!

¿Qué hacemos?

Aunque nuestra presencia es puramente en línea, utilizamos malware ya existentes para apuntar a terminales de tarjetas de crédito en puntos de venta.

Sí, somos cibercriminales ... Y esto es de lo que somos capaces ...

Entramos a una red y robamos los datos de las tarjetas de crédito, esta información la podemos vender a un gran número de compradores o incluso usarlas nosotros mismos. Una vez que estamos dentro de esa red también podemos obtener la información personal de otros clientes.

Luego, instalamos un ransomware. Este nos permite extorsionar directamente a los propietarios de las computadoras infectadas, reteniendo esos datos a cambio de una recompensa. Por lo general, significa infectar una computadora con un software que cifrará el disco duro y mostrará un mensaje exigiendo el pago de cierta cantidad de bitcoins a cambio de la clave cifrada para recuperar los datos.

Y la mejor parte…

Cuantas más computadoras se infecten, más dinero ganaremos.

Nuestra misión es usar el espionaje, la extorsión y la humillación, a través del uso de armas cibernéticas para interrumpir, dañar o destruir infraestructura crítica.

Somos ciber soldados… un grupo bien financiado que actúa bajo el interés nacional y militar del gobierno de nuestro país y que cuenta con los recursos para, no solo utilizar cualquier tipo de amenaza que exista, sino también para desarrollar nuevos ciberataques por nuestra cuenta.

Siéntate y observa lo que somos capaces de hacer ...

Nuestro método más conocido es aprovechar las vulnerabilidades en los sistemas operativos y aplicaciones comunes. A esto podemos llamarlo ataques de "día cero", porque representa el primer momento en que se notifica sobre la falla y no se ha creado una medida para solucionarlo.

Con suerte, en ese momento, somos los únicos que conocemos sobre esa vulnerabilidad. Cuando llegue el momento de lanzar una amenaza que se aproveche de una vulnerabilidad, lo más probable es que no pase mucho tiempo hasta que alguien descubra cómo neutralizarla. Entonces, el proveedor de software seguramente emitirá un código o parche de inmediato.

Por eso, una vez que utilizamos una de las amenazas, estas tienen una vida útil muy corta antes de que ya no se puedan volver a utilizar.

Como dije antes... es por eso que guardamos el secreto.

Lección 2—Perspectivas sobre la seguridad de los datos

Hola, soy Chloe. Bienvenidos a la capacitación en seguridad informática: Clase sobre seguridad de los datos. Hablaremos de su papel como usuario de internet y de cómo las ciberamenazas afectan su experiencia, ya sea en casa, en el trabajo o en un viaje.

La seguridad de la información, también conocida por el acrónimo inglés InfoSec, es importante para personas de cualquier edad. Es un deporte de equipo y todos participamos. A medida que la tecnología evoluciona a paso firme en la era digital, tenemos la responsabilidad compartida de hacer que el ciberespacio sea un entorno más seguro para nosotros y las generaciones futuras.

Si bien hay muchas capacitaciones y contenidos educativos sobre seguridad para organizaciones, aquí queremos brindar consejos para que los individuos naveguen seguros en internet. Si usted está conectado, es vulnerable; y evitar los ciberataques cada vez más complejos requiere vigilancia permanente. Nos gusta la idea de transformarnos en un firewall humano. Es sentido común. Si es consciente de la seguridad, podrá aventajar a los atacantes. Al conocer las medidas a su alcance como usuario particular, podrá reducir los riesgos cuando esté en línea. ¡Comencemos!

Para proteger los datos, la seguridad y la privacidad van de la mano. La privacidad se refiere a políticas empresariales que fijan pautas para la gestión de datos, como su recopilación, conservación y eliminación. La ciberseguridad consta de métodos para proteger redes, dispositivos y datos frente a accesos no autorizados y para asegurar la confidencialidad, integridad y disponibilidad de esa información. La seguridad de la información rige tanto a nivel cibernético como físico.

Aquí le mostramos algunos términos que debe tener en cuenta para entender mejor algunos riesgos:

- Las vulnerabilidades son fallas de software, firmware o hardware que un atacante puede aprovechar para realizar acciones no autorizadas en un sistema. Los atacantes se valen de estos errores para infectar computadoras con malware o realizar otras acciones maliciosas.
- Un atacante es alguien que aprovecha las vulnerabilidades del software y los sistemas informáticos para beneficio propio; sus acciones suelen ir en contra de los fines para los que se creó el sistema. Las amenazas van del mero daño al robo o adulteración de información.
- La superficie de ataque es cualquier parte de un entorno que está expuesta y que un atacante puede usar para acceder a sectores protegidos o extraer algo valioso de ellos. Tras el primer acceso a una red, el intruso utiliza las rutas de comunicación habilitadas entre los dispositivos de la red para obtener más acceso. Por eso, los profesionales de la ciberseguridad buscan identificar todas las superficies de ataque, reducir su magnitud y disminuir el riesgo de ataques.
- Un malware es un archivo o programa no deseado que puede dañar una computadora o poner en riesgo los datos almacenados en ella. Algunos ejemplos de la clasificación de códigos maliciosos son los virus, gusanos, botnets, troyanos, los ataques distribuidos de denegación de servicios o DDoS y ransomware. Los archivos de datos maliciosos son no ejecutables y pueden ser archivos de Microsoft Word, Adobe PDF, ZIP o de imagen que aprovechan los puntos débiles del programa con el que se abren. Los atacantes suelen usar este tipo de archivos para instalar un malware en el sistema de la víctima y los distribuyen por correo electrónico, redes sociales y sitios web inseguros.
- La ingeniería social es una técnica muy lucrativa que engaña a los usuarios porque piensan que lo que ven es auténtico. El objetivo de un ingeniero social es ganar su confianza y luego aprovechar la relación para que usted divulgue información confidencial, suya o de otra entidad, y que le otorgue acceso a una red. Estos agentes prefieren el camino más fácil. ¿Por qué usar una costosa amenaza de día cero si la ingeniería social funciona? Ellos hackean la mente de determinados individuos, quienes rara vez se dan cuenta del engaño, y utilizan inteligencia e interacciones públicas para crear perfiles de víctimas. Estos fraudes atraen a la víctima porque parecen confiables y activan disparadores emocionales, como la curiosidad, la urgencia o la intimidación.

Hoy en día, parece que todo se basa en internet: correos electrónicos, teléfonos inteligentes, videojuegos, redes sociales, aplicaciones, compras en línea, equipamiento médico e historias clínicas. Y la lista sigue. La desventaja es que las ciberamenazas presentan un grave riesgo tanto para la empresa como para los datos personales. Por ejemplo, un malware puede eliminar por completo un sistema, mientras que un atacante podría ingresar en él y adulterar los archivos, utilizar una computadora para atacar a otros o robar información de tarjetas de crédito y hacer compras no autorizadas. No existen garantías que lo protejan de todo esto, incluso si toma las máximas precauciones. Sin embargo, ahora mismo puede adoptar medidas para reducir las probabilidades. En primer lugar, hay que reconocer los riesgos cibernéticos potenciales.

Así como la tecnología continúa avanzando y haciendo nuestra vida más fácil y conectada, los ciberdelincuentes utilizan técnicas sofisticadas que ponen en peligro los hábitos tecnológicos y de navegación en línea. Los atacantes aprovechan el contenido de las redes sociales, incluidos los planes para las vacaciones, porque este tipo de actividades requiere que usted brinde información confidencial en línea. Tenga siempre presente que la información de carácter confidencial y privado requiere protección constante. Por ejemplo, la información personal incluye datos que pueden identificarlo, como su nombre completo, fecha de nacimiento, datos biométricos, número de pasaporte, documento de identidad, tarjetas de crédito o teléfono y direcciones de correo electrónico o la dirección de su casa. También debe proteger los datos confidenciales de la empresa. Si usted comparte información confidencial en la red, los ciberdelincuentes pueden aprovechar esta gran oportunidad para cometer fraudes con tarjetas de crédito, robar su identidad o poner en riesgo el acceso a los recursos confidenciales de la empresa. En pocas palabras, la información vale oro. Por eso, es imperativo seguir las leyes de privacidad y protección de los datos en el lugar de trabajo.

Para cada sector de la empresa, se deben documentar los niveles de riesgo aceptables en relación con la ciberseguridad y la privacidad. Es necesario adoptar tanto las prácticas de seguridad reconocidas por la industria como las garantías adecuadas para proteger la información personal y los datos, sistemas, actividades y recursos de una organización. El objetivo es crear una fuerza de trabajo orientada a la seguridad.

El ciberdelito es una amenaza global que no conoce fronteras. En consecuencia, distintas reglamentaciones y gobiernos, como es el caso del Reglamento General de Protección de Datos (GDPR) en Europa y en otros países, priorizan la seguridad de la información mediante nuevas leyes y estándares normativos. Recuerde que usted es responsable de proteger su información. ¡El error humano es la causa de casi todas las filtraciones de datos! Sea cauteloso con las solicitudes sospechosas, los desconocidos que intenten contactarlo o la información no solicitada que le llegue a través de cualquier medio. Si tiene alguna duda, consulte con el sector encargado de la privacidad de la empresa. Su función es la de ayudarlo a manejar estos riesgos y recomendarle medidas de ciberseguridad.

Repasemos por qué los atacantes son tan efectivos. Los ataques maliciosos van en constante aumento. Según algunos estudios, el 91 % de los ciberincidentes que ocurren dentro de una organización se originan en un error humano, tal como hacer clic en un correo de suplantación de identidad o spear phishing sin darse cuenta. Se estima que el uso indebido de los privilegios de acceso está relacionado con un 80 % de las filtraciones de datos. En un mundo en el que los ciberenemigos corren con una gran ventaja, la seguridad de los datos es primordial.

En temas de ciberseguridad, el conocimiento es poder; por eso, al tomar medidas que están a su alcance, puede evitar las trampas más comunes. ¡Garantice la ciberseguridad!

Gracias por su tiempo, y no olvide responder las preguntas a continuación.

Lección 3—Perspectivas de las contraseñas

Hola, soy Steve. Bienvenidos a la serie sobre “capacitacion en seguridad informática” - Clase de capacitación sobre Contraseñas. Hablemos de su rol en la protección de los datos, usando contraseñas únicas y fuertes.

Primero, si mantiene sus contraseñas escritas en un papel cerca de su escritorio, deténgase. Deséchelas HOY, y no coloque ese papel en la basura. ¡Destrúyalo! Además, mantener las credenciales predeterminadas en cualquier dispositivo es el peor tipo de contraseña, porque hace que sea mucho más fácil para los atacantes: los hackers tienen bases de datos de credenciales comunes, especialmente, para sistemas específicos que están conectados a Internet; por ejemplo, aquí hay una lista de las contraseñas más usadas y realmente muy malas. ¡No las utilice!

- 123456789
- 12345678
- 1234567
- 123456
- 12345
- 123123
- 111111
- 666666
- 654321
- Qwerty
- qwerty123
- Abc123
- Aa123456
- !@#$%^&*
- Passw0rd
- password1
- admin
- charlie
- Donald
- football
- iloveyou
- monkey
- Password
- Princess
- sunshine
- welcome
- zzxxccvvbb

Recuerde, la mejor contraseña es una frase segura con una combinación única de letras mayúsculas y minúsculas aleatorias, números variados y caracteres especiales, que son imposible de olvidar y difícil de adivinar, incluso para alguien que conoce detalles personales de su vida. No facilite a los Hackers comprometer sus cuentas mediante el uso de una contraseña débil. En resumen, sus contraseñas son como su cepillo de dientes: desea elegir una buena, que sea única para cada cuenta, nunca compartirla, cambiar todas las contraseñas predeterminadas y reemplazarlas dos veces al año. Siempre cambie las contraseñas que se generan por defecto y mantenga contraseñas diferentes para cada cuenta. De esa manera, si un atacante irrumpe en un sistema, solo tendrá la contraseña para ese sistema. Todas sus otras cuentas seguirán siendo inaccesibles para ellos. Ahora, sé lo que va a decir: no puedo recordar todas estas contraseñas, y eso es comprensible. Afortunadamente, hay administradores de contraseñas que crearán y guardarán contraseñas seguras para usted, y luego le permitirán accesarlas de forma segura cuando las necesite. Pregunte, investigue y encuentre uno que funcione para usted y asegúrese de que su contraseña maestra sea segura. Si está instalando una aplicación en un dispositivo móvil, recuerde descargarlo de las tiendas de aplicaciones oficiales. Adicionalmente, solo una sugerencia, tenga cuidado de dónde el administrador de contraseñas almacena sus contraseñas, si está en la nube o en cualquier almacenamiento fuera del dispositivo, entonces cualquier ataque a ese almacenamiento posiblemente les dará a los intrusos todas sus contraseñas.

Esto nos lleva a la autenticación multifactor o MFA, donde el sistema requiere al menos dos elementos separados para permitir el acceso. En la mayoría de los casos, esto consiste en combinar algo que usted sabe, con algo que usted tiene, como un token físico, que muestra un número que cambia rápidamente. Para utilizarlo, debe mirar el monitor e ingresar el número que se indica, acompañado de su contraseña. El token está sincronizado con el sistema que deseas acceder, si en algún momento su contraseña se ve bajo riesgo, un atacante no podrá acceder sin tener el token físico, ya que éste cambia constantemente. Incluso si lograran ver el código de su token, ya no será válido.

Otra opción es un token de software, que a menudo toma la forma de una aplicación cargada en un teléfono inteligente. La forma en que funcionan es la misma que la de un token físico, pero usted usa su teléfono inteligente para obtener el código. Alternativamente, algunos sistemas simplemente emiten un código único para permitirle el acceso y se le transmite de manera segura y configurada previamente. La recomendación aquí es que, si un proveedor tiene una opción para la autenticación de dos factores, generalmente será más seguro que solo la contraseña.

La verdad es que, no importa cuán fuerte sea su contraseña, la posibilidad de un ataque siempre está latente. Todo lo que se necesita es que, solo una de sus cuentas sea violada y su información importante puede ser accesible para los ciber criminales. En resumen: priorice continuamente la protección de sus cuentas que contengan información personal o de más alto valor, y sus accesos remotos, habilitando las funciones de autenticación multifactor. De esa forma, se asegura que el único usuario con acceso a su email, banca en línea, redes sociales o cualquier otro sistema que requiera contraseña sea usted.

Ahora hablaremos de un tema que todos conocen pero que se no piensa con frecuencia. Respaldos. Espero que sepa, para proteger sus datos o información, debe respaldarla regularmente. No lo olvide, para defenderse de los ataques contra los datos es crucial también proteger los respaldos con contraseñas. Si algo ocurre, como, un secuestro de sus datos, disponer de respaldos recientes lo ayudará a restaurarlos sin necesidad de preocuparse o pagar un rescate. No recomendaremos ninguna solución en particular para hacer sus respaldos, solo asegúrese de que la solución que elija le permita restaurar sus datos desde un momento específico, y que además le permita integrar seguridad cifrada como una protección extra. De igual forma, esté atento en qué lugar están guardados sus respaldos. Algunos ataques también pueden cifrar el almacenamiento de respaldos cuando permanecen físicamente conectados a la computadora.

Aunque este no es particularmente un tema de seguridad, también es un buen momento para pensar en respaldar sus documentos y carpetas importantes, como sus fotografías.

En materia de ciber seguridad, el conocimiento es poder. Implementando este tipo de recomendaciones antes mencionadas podemos evitar las trampas más comunes. ¡Asegúrese de estar ciber seguro!

Gracias por su tiempo y por favor recuerde tomar el examen después de esta lección.

Lección 4—Perspectivas sobre amenazas en internet

Hola, mi nombre es Chloe. Bienvenidos a la clase sobre amenazas en internet. Hablaremos de su papel como usuario de internet y de cómo las ciberamenazas afectan su experiencia, ya sea en casa, en el trabajo o en un viaje, y de los intereses que hay en juego.

Con el tiempo, la tecnología ha explotado con ceros y unos digitales que rigen casi todos los aspectos de la vida. Las tecnologías emergentes, como la inteligencia artificial (IA), el aprendizaje automático, el 5G o la computación cuántica, y las que están en evolución, como la nube, los vehículos autónomos y los dispositivos conectados a la internet de las cosas (IoT), son blancos cuya seguridad debe resguardarse. En efecto, cada segundo, más de cien nuevos dispositivos de IoT se conectan a la red. Como las ciberamenazas no paran de crecer, debemos ser cada vez más conscientes de la seguridad. La ciberseguridad es una responsabilidad compartida. Todos tenemos que contribuir para que la internet sea segura.

Lo primero es estar alerta. Los delincuentes utilizan la ingeniería social para poner en riesgo los sistemas tan solo porque funciona. Por eso, hay que conocer la infinidad de fraudes que esta permite. Los ingenieros sociales o agentes de amenaza intentan influir en el comportamiento, y el error humano es la causa de casi todas las filtraciones de datos. El objetivo de un ingeniero social es ganar su confianza y luego aprovechar la relación para que usted divulgue información confidencial, suya o de otra entidad, y que le otorgue acceso a una red.

A continuación, algunos métodos de ingeniería social que exploraremos:

- Juice Jacking: puestos de carga inseguros que instalan malware cuando se conecta un dispositivo en áreas comunes, como aeropuertos, estaciones o salas de conferencias
- Phishing: correos electrónicos dañinos que parecen confiables e invitan a un grupo puntual a realizar una acción, y solo requieren una víctima para cumplir su objetivo
- Ransomware: malware que impide el acceso a sistemas informáticos y exige una suma de dinero para recuperar los datos. El correo electrónico es el vector de ataque más común porque se vale de solo un clic para burlar los controles
- Spear phishing, whaling, fraude del CEO y ataques por email de tipo BEC: mensaje fraudulento y dañino a personas o cargos específicos, en general con motivos financieros

Existen muchos otros métodos de ingeniería social de los cuales podrás leer más adelante en este curso.

Los anzuelos existen. Pero si usted se convierte en un firewall humano, le dificultará las cosas al atacante. Use el sentido común y esté alerta cuando algo se ve mínimamente sospechoso.

Ahora hablaremos de la seguridad de los móviles. La mayoría de nosotros llevamos dispositivos móviles durante el día. Los revisamos con frecuencia y los mantenemos cerca incluso mientras dormimos, ya que permiten acceder a la información en todo momento y desde cualquier lugar. Hoy concentran más de la mitad del tráfico en internet, y ya casi no se diferencian de una computadora. Como estos dispositivos pueden contener una gran cantidad de información confidencial, son blancos muy atractivos y brindan jugosas oportunidades a delincuentes que buscan lucrar con ellos. Hay aplicaciones móviles cuyos datos son tentadores, como los de bancos, redes sociales, correos electrónicos, calendarios, contactos, comercio electrónico o GPS, y presentan un sinfín de vulnerabilidades. Estas se encuentran, por ejemplo, en las capas tecnológicas del móvil, como el SMS o MMS, el Bluetooth o la sincronización con computadoras, y son vectores potenciales de ataques que aumentan la capacidad de daño de los agentes maliciosos.

La ciberdelincuencia dirigida a dispositivos móviles tiene efectos nefastos, como el robo de datos clave, el rastreo de usuarios o el bloqueo de acceso al propio dispositivo. Su dispositivo también puede utilizarse como medio para otros ataques más lucrativos a sistemas empresariales, redes sociales o plataformas en la nube.

Para mitigar las amenazas que representan estas vulnerabilidades, proteja su red Wi-Fi. El término «Wi-Fi» proviene del inglés wireless fidelity (fidelidad inalámbrica), y el router inalámbrico es la puerta principal por la que los ciberdelincuentes acceden a los dispositivos conectados en el hogar. Siempre proteja los dispositivos digitales. Antes de conectarse a una red pública inalámbrica, como en aviones, aeropuertos, hoteles o cafés, verifique con el personal el nombre de la red y la forma de acceso para asegurarse de que la red es auténtica.

Las redes públicas son siempre un riesgo para la seguridad. Para protegerse de las amenazas del juice jacking, piense bien antes de conectarse a un puesto de carga supuestamente confiable en hoteles, aeropuertos o estaciones. Es mejor adquirir un cargador portátil. Los puestos gratuitos pueden contener malware que infectará el dispositivo y permitirá que los atacantes accedan a sus datos. Si un dispositivo conectado a su red queda expuesto, alguien podría espiarlo, incluso en su propio hogar o en una red Wi-Fi cifrada.

Todos queremos hacer lo correcto. Por eso, veamos los siguientes buenos hábitos para conexiones móviles:

- Evite conectarse a redes Wi-Fi desconocidas
- Utilice las Autenticaciones Multi-Factor (MFA)
- Respalde sus datos
- Evite abrir archivos, hacer clic en links, o llamar a números desde mensajes no solicitados
- Cambie las credenciales predeterminadas de sus equipos
- Borre toda la información de sus equipos anteriores antes de deshacerse de ellos
- Deshabilite las opciones que no esté utilizando, como Bluetooth o WI-FI
- Encripte toda los datos importantes y los caminos de comunicación
- Habilite el bloqueo de pantalla, y utilice contraseñas fuertes
- Siga las políticas sobre el manejo de datos de su empresa
- Mantenga sus softwares y sistemas operativos actualizados
- Nunca deje sus equipos abiertos y desatendidos
- Apague su equipo o active el modo avión antes de guardarlo
- Active el Bluetooth en modo incógnito
- Apague las conexiones automáticas cuando no esté utilizando su equipo.

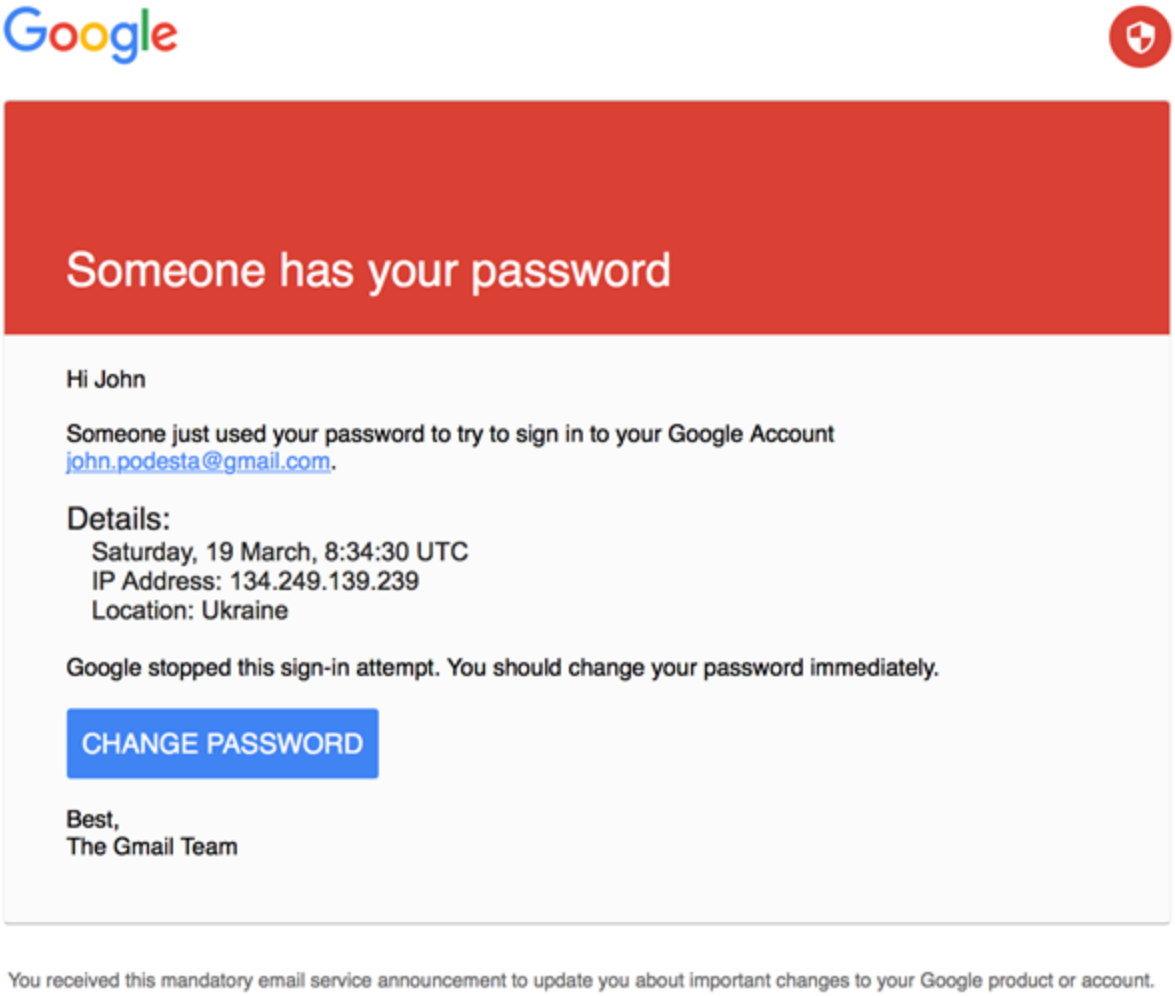
Ahora hablaremos de los correos electrónicos. Pasamos buena parte del día en la bandeja de entrada. De hecho, se envían 300.000 millones de mensajes por día en todo el mundo. El correo electrónico es el principal vector de infecciones con toda clase de malware, incluido el ransomware. Una forma común de transmisión de malware son los adjuntos. Si recibe un correo que contiene un adjunto y proviene de un remitente desconocido, probablemente no debería abrir el archivo.

Retrocedamos y veamos en primer lugar cómo recibe estos correos. Se trate de spam tradicional o de phishing, alguien tiene su dirección de correo electrónico, y ha circulado entre remitentes de correo no deseado. Si bien es difícil mantener la dirección en absoluto secreto, hay formas de que aparente tener menos valor para quienes envían spam. Una de las más efectivas consiste en configurar la cuenta de manera que no se muestren imágenes descargadas. En este tipo de mensajes, el solo hecho de descargar una imagen avisa al remitente que hay alguien que los abre. Esto hace que su cuenta sea un blanco de mayor valor. La mayoría de los clientes de correo que tienen esta función le permitirá descargar imágenes de mensajes auténticos. Así se verán en el formato correcto y serán

fáciles de leer. El spam no suele requerir ninguna acción, y para evitar recibir más mensajes del mismo remitente basta con marcarlo como correo basura y bloquear el remitente.

Veamos ahora las técnicas de phishing, spear phishing, whaling, fraude del CEO y BEC. Los ciberdelincuentes diseñan correos que parecen auténticos e invitan a realizar una acción, como hacer clic en un enlace o abrir un adjunto. A primera vista, los mensajes aparentan ser de una institución financiera, un sitio de comercio electrónico, un organismo gubernamental u otro servicio o empresa auténticos. Por este medio, los atacantes, recopilan información personal, privilegiada o financiera, y pueden infectar computadoras con malware y virus. Los hackers suelen usar técnicas de redireccionamiento de dominios. Simulan ser un remitente que usted conoce e intentan que les proporcione información confidencial, como credenciales de acceso, números de cuenta o de tarjetas de crédito y transferencias de dinero. Como estos correos parecen provenir de fuentes confiables, puede ser muy difícil darse cuenta de que no son auténticos.

Los ciberdelincuentes utilizan estos medios para realizar ataques porque siguen siendo efectivos. Son atractivos y verosímiles porque se asemejan a solicitudes verdaderas. Para lograr su objetivo, deben engañar a los usuarios. Para protegerse, desconfíe de cualquier mensaje que le solicite realizar una acción, sin importar qué tan oficial se vea. Tómese un tiempo y busque indicios que permitan descubrir si es auténtico o no. Por ejemplo, ¿este anzuelo le parece sospechoso? Hay un caso tristemente célebre de una persona famosa que recibió un correo urgente en el que se le solicitaba cambiar la contraseña y… él hizo clic en el enlace de este correo:



Entonces, si hay algo que deben recordar de este video es lo siguiente: ¡coloque el cursor sobre el enlace antes de hacer clic! Si se toma la molestia de colocar el cursor sobre un enlace, verá hacia dónde lo llevará realmente. Es un indicio clave para determinar si el correo es genuino.

Por ejemplo, si recibe un correo que aparenta ser del banco y le informa que hay un problema con su cuenta y que para solucionarlo debe acceder a un sitio web mediante un enlace, no haga clic en él. En cambio, abra un navegador actualizado y escriba manualmente la dirección del sitio (URL) para ver de qué se trata.

Si recibe un correo en el que le solicitan una transferencia de dinero, por ejemplo, el pago de una factura, aun si lo envía un conocido, lo recomendable es que se comunique por otro medio de confianza para verificar que el mensaje sea auténtico antes de tomar una decisión. Además, preste especial atención a la dirección del remitente. Aunque un mensaje diga que proviene de alguien que usted conoce o en quien confía, no significa que se trata de esa persona.

Los ataques de phishing se envían a muchos destinatarios, mientras que los de spear phishing, whaling, fraude del CEO, BEC e incluso vishing están dirigidos a individuos o cargos específicos. Según estudios, estos ataques tienen una efectividad del 91 %. Si un atacante desea penetrar en una organización concreta, puede hacerlo por medio un correo diseñado para tal fin o de una llamada particular que parecen provenir de una fuente interna o de un proveedor externo que trabaja con la organización y es de confianza. Muchas veces, estas comunicaciones fraudulentas se asemejan a mensajes directos de un superior o un alto ejecutivo. Si tiene dudas, incluso cuando los detalles parezcan correctos, no responda.

Coloque el cursor sobre el enlace para ver el destino real y verifique que no haya errores ortográficos o gramaticales. Para estar a salvo, nunca transfiera dinero ni revele información confidencial ni dé permisos de acceso especiales sin antes corroborar con otra fuente de confianza.

Los ingenieros sociales son expertos en hacerse pasar por fuentes auténticas, manipular la mente humana para provocar una respuesta emocional y convencerlo de que incumpla los protocolos comunes de seguridad. ¡No se deje engañar!

En temas de ciberseguridad, el conocimiento es poder; por eso, al tomar medidas que están a su alcance, puede evitar las trampas más comunes. ¡Garantice la ciberseguridad!

Gracias por su tiempo, y no olvide responder las preguntas a continuación.

Lección 5—Perspectivas sobre amenazas internas

Hola, soy Steve. Bienvenidos a la clase sobre amenazas internas. Hablaremos de su papel como persona con acceso a información privilegiada de la empresa y los intereses que hay en juego, y veremos que el sentido común es crucial para prevenir un incidente de seguridad.

Las amenazas para la seguridad están en todos lados y vienen de todo el mundo, las 24 horas, los 7 días de la semana, los 365 días del año. Además, el error humano es la causa principal de casi toda filtración de datos.

Para simplificar, los siguientes consejos prácticos lo ayudarán a mejorar la resiliencia de su entorno virtual y a ser consciente de la seguridad física de su lugar de trabajo.

Siempre siga la política de la empresa y las pautas de manejo de datos. Si tiene alguna duda sobre una política, consulte. No hay preguntas tontas.

Resguarde toda información confidencial e importante en un dispositivo cifrado con una contraseña segura.

Preste atención a su alrededor y a quienes se acercan a su escritorio y actúan de manera sospechosa. Podrían buscar información confidencial o espiarlo cuando ingresa las contraseñas.

No escriba las contraseñas en notas adhesivas ni las deje en su escritorio, computadora o teclado.

No deje en su escritorio información protegida o confidencial y guarde bajo llave toda información privada cuando se retire de su puesto de trabajo por un período prolongado o al final de la jornada.

Bloquee la pantalla de su computadora o teléfono celular al retirarse para evitar que terceros revisen o manipulen la información confidencial que hay en ellos.

Informe de inmediato al personal de seguridad sobre puertas, ventanas o cerraduras dañadas.

Denuncie toda actividad sospechosa en los accesos del edificio o alrededores, zonas de carga o estacionamiento, garajes y proximidades, y siempre cierre su vehículo con llave.

Denuncie cualquier paquete sospechoso y no lo abra ni lo toque.

Triture y destruya todo documento que contenga información importante para usted o la organización en lugar de arrojarlo a la basura.

Los dispositivos con información protegida o confidencial, como computadoras de escritorio o portátiles, DVD, CD-ROM o memorias USB, se deben tratar como confidenciales. Nunca los comparta con personas no autorizadas, incluidos los miembros de su familia.

Use su credencial para entrar al lugar de trabajo y no permita que nadie ingrese detrás de usted. Solicite a los extraños que se identifiquen y que expliquen el motivo de la visita a su lugar de trabajo.

Ahora hablaremos de las amenazas internas. La mayoría de las personas que trabajan en una empresa son empleados fieles y trabajadores que realizan tareas muy importantes. Al final del día, se van a sus casas con su familia, amigos o mascotas. Es más, se podría pensar que las ciberamenazas provienen de un delincuente anónimo y lejano que está detrás de la pantalla de una computadora, y que la ciberseguridad en el trabajo solo apunta a amenazas externas. Por desgracia, una amenaza interna puede ser dañina para la organización, sus datos y la reputación de su marca. Los empleados actuales y antiguos tienen conocimientos valiosos sobre la empresa y son capaces de cometer delitos que pueden ocasionar un daño irreparable a la organización.

Vamos a las definiciones. Una persona con acceso a información privilegiada tiene acceso a recursos de la empresa, tales como información importante, empleados, equipamiento, instalaciones, redes y sistemas. Una amenaza interna

es el riesgo de que una persona con acceso a información privilegiada use este acceso autorizado para dañar la organización, voluntaria o involuntariamente.

En general, se trata de alguien con buenas intenciones que pone en riesgo a la empresa por accidente, por ejemplo, al abrir un correo electrónico de suplantación de identidad (phishing); o por negligencia, como cuando un usuario con privilegios no sigue la política de la empresa para trabajar más rápido y termina poniendo en riesgo la seguridad, aun sin saberlo. Otras veces, las amenazas internas son maliciosas y surgen de la organización, que es el blanco de un ataque intencional. Son acciones deliberadas, como la vulneración malintencionada, el robo, la destrucción de datos o la puesta en peligro de los recursos informáticos. Según estudios, podrían ser llevadas a cabo por empleados actuales o exempleados, contratistas, directivos o cualquiera que tenga o haya tenido permiso de acceso al edificio, las redes, los sistemas o información confidencial de la empresa.

Las amenazas internas son los vectores de ataque más difíciles de enfrentar porque los usuarios de confianza que deben tener acceso legítimo a datos importantes, redes y recursos son los mismos que podrían dañarlos.

Las personas son el centro de toda amenaza interna. Por eso, poner siempre el foco en ellas es esencial. La vida pasa, y todos nos enfrentamos con retos y obstáculos inesperados en el camino. Los errores son parte de la naturaleza humana. Lo importante es aprender de ellos y no ser negligentes. De nuevo, según algunos estudios, estos actos dañinos no suelen ser impulsivos. Algo sucede para que un empleado de confianza se convierta en un empleado malintencionado. Para mitigar este riesgo, corrobore que todos los recursos esenciales estén identificados y protegidos.

La mayoría de las amenazas internas son sin intención, de ahí la importancia de concientizar. Hay que estar alerta. Si ve u oye algo que considera preocupante, no se quede callado. Por ejemplo: ¿A quién vio? ¿Qué vio? ¿Cuándo lo vio? ¿Dónde ocurrió? ¿Por qué es sospechoso? No importa qué tan insignificante parezca: puede ser una puerta de seguridad entreabierta, un documento confidencial en la impresora o la pieza de un equipo que funciona raro. Denuncie toda actividad sospechosa a su superior jerárquico y al equipo de seguridad de la información de la empresa.

En temas de ciberseguridad, el conocimiento es poder; por eso, al tomar medidas que están a su alcance, puede evitar las trampas más comunes. ¡Garantice la ciberseguridad!

Gracias por su tiempo, y no olvide responder las preguntas a continuación.