DEPARTAMENTO DE OPERACIONES – CAPACITACIÓN DE CIBERSEGURIDAD– JUNIO 2021

Cuando informas, nos hacemos más fuertes – COVID-19 PAB

Un mensaje importante de tu equipo de seguridad con respecto a los delitos cibernéticos y COVID-19

Seguramente has escuchado la vieja frase que dice “ver algo, decir algo”. Buen consejo, ¿verdad? Pero ¿cómo lo haces? Ahí es donde entra el botón de alerta de suplantación de identidad (busque el icono de "gancho" en la barra de herramientas del correo electrónico de su cliente).

En este momento, los ciberdelincuentes se están aprovechando de todo el miedo, la interrupción y la confusión que rodean a COVID-19 y una de las formas más importantes en que lo están haciendo es enviando correos electrónicos de phishing. Es posible que ya sepas que debes evitar estos textos y mensajes cuando los veas. Pero ahora más que nunca es muy importante que informe sobre estas amenazas a través de la PAB.

(Utiliza la PAB para informar sospechas de intentos de suplantación de identidad)

Si tienes alguna pregunta sobre la legitimidad de un correo electrónico, infórmalo. Incluso si es solo un presentimiento, usa la PAB. Hacerlo nos da la oportunidad de investigar, defender a la organización y mantener alejados a los malos.

Cuando informas, nos fortalecemos. Recuerda: ***MANTEN LA CALMA Y NO HAGAS CLIC***

Bienvenido a la Capacitación en concientización sobre ciberseguridad de KnowBe4 para Texas

¿Recuerda haber recibido un correo electrónico o un mensaje de texto que pareció sospechoso? Preste atención a esas sospechas porque el ciberdelito es un gran negocio y una creciente preocupación mundial.

El Proyecto de Ley 3834 (86R) de la Cámara de Representantes de Texas se creó para exigir que los empleados de los gobiernos estatales y locales, así como los empleados contratados, reciban capacitación obligatoria en materia de ciberseguridad para ayudar a proteger mejor a Texas contra estas crecientes amenazas.

Este curso se centra en los hábitos y procedimientos de seguridad de la información que protegen los recursos de información y enseñan las mejores prácticas para detectar, evaluar, informar y abordar las amenazas a la seguridad de la información.

Al final de este curso tú:

- Comprenderás los principios de la seguridad de la información.
- Tendrás conciencia de las amenazas a la seguridad de la información.
- Conocerás las prácticas recomendadas para proteger la información.
- Serás capaz de identificar, responder y notificar apropiadamente las amenazas a la seguridad de la información y las actividades sospechosas.

El contenido de este curso incluye partes de los siguientes módulos de capacitación KnowBe4 que han sido seleccionados para cumplir con estos requisitos estatales: (1) *Definición y manejo de información sensible, (2) 2020 Tu función: la seguridad en Internet y tú.*

La información confidencial se considera valiosa porque es información personal o que está sujeta a derechos de propiedad, que no debería estar disponible al público porque en las manos equivocadas puede causar daños graves a una persona u organización.

Sigamos adelante y exploremos cinco tipos de información confidencial.

1. ***La información personal***, o PI, se define como "información que se puede utilizar o distinguir o rastrear la identidad de un individuo, ya sea sola o combinada con otra información personal o de identificación". Algún PI por sí solo no es necesariamente arriesgado de tener ahí fuera. Por ejemplo, tu nombre, la ciudad en la que vives y el tipo de automóvil que conduces están todos disponibles públicamente.

Otros tipos de PI son sensibles y no deberían estar disponibles públicamente. Ejemplos de estos elementos incluyen:

- Licencia de conducir u otro número de identificación emitido por el gobierno
- Número de identificación nacional (por ejemplo, SSN en los EE. UU.)
- Número de pasaporte
- Historial médico
- Número de tarjeta de crédito (o débito) y fecha de vencimiento
- Información bancaria y financiera
- Información sobre sueldos o salarios

Además, cierta información no es identificable por sí misma, pero puede llegar a ser identificable cuando se agrega a otra parte de PI. Por ejemplo: Origen racial o étnico, Afiliación política / opiniones, Creencias religiosas o filosóficas, Afiliación sindical, Datos genéticos o biométricos, Rastreador portátil de datos de salud y actividad física, Datos relacionados con hábitos u orientación sexuales.

Algunos otros términos que puede escuchar usados indistintamente para este tipo de datos son: Información de identificación personal (PII), Información de identidad personal (PII), Datos personales (PD).

2. ***Información de salud protegida***, o (PHI), es la información registrada sobre la salud, el historial de atención médica, los registros del proveedor o el pago de la atención médica de una persona. Algunos ejemplos incluyen:

- Registros médicos
- Número de beneficiario del plan de salud
- Información privada sobre el paciente, incluida la fecha de nacimiento.
- Número de identificación nacional (NIN)
- Número de seguro social (SSN)
- Identificadores biométricos, incluido el ADN, así como huellas dactilares y de voz
- Imágenes fotográficas de rostro completo y otras imágenes identificables

3. ***Los comerciantes y las entidades que almacenan, procesan o transmiten información de tarjetas de pago*** (PCI) deben proteger cierta información de acuerdo con las regulaciones definidas por un consejo de seguridad de toda la industria.

Los datos protegidos de la tarjeta de pago incluyen: Nombre del titular de la tarjeta, Número de tarjeta, Fecha de caducidad, Número de verificación de tarjeta, Número de identificación personal (PIN), Datos de la banda magnética en la parte posterior de la tarjeta, Datos del chip en el frente de la tarjeta.

Los estándares PCI se aplican a nivel mundial y el incumplimiento de ellos puede resultar en multas y mayores costos de transacción para su organización.

4. ***La información no clasificada controlada***, o CUI, es un tipo de información sensible especialmente relacionada con el gobierno de los EE. UU. CUI está definido por las regulaciones del Departamento de Defensa (DoD) y se aplica a cualquier socio estatal, local, tribal, del sector privado y extranjero que utilice información del DoD.

El primer paso para comprender qué hace que algo sea CUI es reconocer la diferencia entre información clasificada y no clasificada controlada.

La información clasificada es cualquier información que el gobierno de los EE. UU. Determina que puede dañar la seguridad nacional si llega a las manos equivocadas. Por ejemplo, los códigos de lanzamiento nuclear serían información clasificada.

La información no clasificada controlada (CUI) es un paso debajo de la información clasificada.

Esta información no representa un riesgo para la seguridad nacional, pero su divulgación podría ser perjudicial para las personas u organizaciones, por lo que debe protegerse. Ejemplos incluyen: Información personal, Información financiera, Información de seguridad de Informática, Registros judiciales y policiales, Patentes y documentos técnicos.

En términos generales, la información de propiedad privada es información que una organización desea mantener en privado y lejos del público en general. Los ejemplos incluyen, pero no se limitan a:

• Información organizativa no pública, incluidos métodos y procesos de producción, así como secretos comerciales

• Contraseñas, ID de usuario e información de red interna

• Planes estratégicos o decisiones de la junta

• Datos financieros confidenciales

• Información que podría dañar a la organización, un compañero de trabajo o un cliente si se divulgara

Este tipo de información generalmente se controla mediante el uso de acuerdos de confidencialidad o acuerdos de no divulgación (NDA). Las acciones legales son posibles por incumplimiento de esos contratos.

En un mundo donde la información es abundante, debemos tener cuidado con la forma en que manejamos la información personal y sensible. Incluso un poco de información puede ser de gran ayuda. Por ejemplo:

Un pirata informático tiene el nombre, el apellido y el número de seguro social de alguien. Utilizando motores de búsqueda en línea y redes sociales, encuentra una dirección, fecha de nacimiento y otra información identificable. Luego, el pirata informático combina toda la información para comenzar a abrir tarjetas de crédito con el nombre de la persona y las envía a una ubicación diferente.

Quizás el pirata informático haya adquirido un nombre, una dirección de correo electrónico y sepa en qué empresa trabaja el individuo. ¡Usan esa información para realizar un ataque y robar las credenciales de inicio de sesión de la víctima!

Ahora tienen acceso a la red de las organizaciones y a toda tu información privada.

Recuerda, los ciberdelincuentes solo necesitan un poco, para causar mucho daño.

5. ***Información sensible o confidencial***. Trabajar con información sensible significa proteger esa información más allá de lo que exige la ley. El simple hecho de solicitar acceso a la información confidencial de alguien conlleva el entendimiento, y la obligación, de que harás todo lo posible para mantener la privacidad de la información privada.

Sin esta confianza, tus clientes, consultores y compañeros de trabajo no estarían dispuestos a compartir su información. A su vez, el funcionamiento y la reputación de la organización se verán afectados.

De hecho, cuando hablamos de información de compañeros de trabajo, eso incluye tu propia información. Por lo tanto, practica el tratamiento de la información de todos con el mismo grado de cuidado que esperaría que usen con su información.

Algunos trabajos requieren que los empleados manejen o compartan información confidencial, otros no. Pero a veces, es posible que tengas acceso a información privada, como los datos personales de un solicitante o aplicante (como la información de salario actual o el número de identificación nacional / número de seguro social) revelados en una solicitud de empleo.

Una buena regla general es que, si no necesitas manejar información confidencial, no lo hagas y avisa a tu gerente si tienes acceso a ella innecesariamente.

Ahora que hemos analizado algunas de las mejores prácticas para el manejo de información confidencial, repasemos qué hacer si tienes que compartir información confidencial con otras personas.

Antes de compartir cualquier información confidencial, ya sea con el personal de la organización o con terceros, ***asegúrate de detenerte, mirar y pensar primero.***

Esto puede ayudar a garantizar que la información confidencial se mantenga privada. Aquí está cómo:

Primero, ***tómate un momento*** para considerar lo que estás a punto de hacer.

A continuación, ***mira la información*** que estás a punto de compartir. ¿Contiene algún tipo de información personal o sensible? Recuerda, compartir esta información de manera incorrecta puede ser ilegal, causar problemas de seguridad y dañar la reputación de tu organización.

Finalmente, considera: ¿en qué se supone que debo ***pensar*** antes de compartir información confidencial? Cuando estés pensando en compartir información confidencial, pregúntate: ¿Estoy autorizado a compartir esta información? ¿Está autorizada la otra parte a recibirlo? ¿Estoy seguro de que son quienes dicen ser? ¿Tenemos acuerdos adecuados de confidencialidad / no divulgación (NDA), contratos y / u otras protecciones legales vigentes? ¿He tomado todas las medidas posibles para mantener segura esta información?

Y lo más importante, asegúrate de preguntarte: "¿Debería compartir esto?" en lugar de "¿Puedo compartir esto?" En caso de duda, comunícate con tu supervisor o equipo de seguridad y pregunta.

Dediquemos unos minutos a explorar por qué es importante que estés familiarizado con la información confidencial y las mejores prácticas para proteger esa información.

Como empleado, TU eres un objetivo. Los piratas informáticos quieren engañarte para que los ayudes a dañar tu organización. Es más, caer en un ataque de estos ciberdelincuentes puede dañarte personalmente. Todo lo que necesita es que cometas un error, como hacer clic en un enlace que luego expone el nombre, el número de licencia de conducir, la fecha de nacimiento y el número de cuenta bancaria de cada empleado contratado por tu organización en la última década. Tu organización necesitaría gastar importantes recursos financieros para remediar este único error, y tus compañeros de trabajo pasarían meses, tal vez incluso años, luchando contra el robo de identidad personal. La seguridad de tu organización tiene algo que ver contigo. A medida que continúe la capacitación, presta atención a las amenazas comunes que tú y tu organización enfrentan a diario. Aprende el papel que desempeñas en la protección de tu organización y de ti mismo, descubriendo las cosas que debes y no debes hacer cuando el pirata informático se dirige a ti. Comencemos por explorar algunas estrategias comunes que a los malos les gusta usar.

ESTRATEGIA 1 - LA INGENIERÍA SOCIAL es el arte de manipular, influir o engañarte para que realices alguna acción que no es lo mejor para ti ni para tu organización. El objetivo de los ingenieros sociales es obtener tu confianza y luego explotar esa relación para convencerte de que divulgues información confidencial sobre ti o tu organización o para darles acceso a su red.

ESTRATEGIA 2 - MALWARE significa “software malicioso” o “programa maligno”, un término general para todo el software que está siendo utilizado por los ciberdelincuentes para espiar y robar tu información. Una vez que tu computadora se infecta, algunas aplicaciones maliciosas pueden registrar todas sus pulsaciones de teclado, incluido tu nombre de usuario y contraseña. Algunas aplicaciones se apoderan de tu computadora e incluso pueden permitir que el pirata informático encienda su cámara web y te espíe o escuche tus conversaciones.

Un tipo de malware que aparece mucho en las noticias se llama Ransomware. Este tipo de programa maligno puede extenderse a todos los dispositivos y archivos a través de una red y niega el acceso hasta que se paga un rescate. El Ransomware codifica los datos en archivos de computadora y los hace ilegibles. El pirata informático hace esto para obligar

a la organización a pagar un rescate. Una vez pagado, la organización recibirá una "clave" que desbloquea los archivos de la computadora y los devuelve al estado original.

ESTRATEGIA 3 - DESINFORMACIÓN es información falsa creada y distribuida con la intención específica de manipular. Aunque esta estrategia no es nueva, se ha vuelto más común debido al alcance de las redes sociales y la facilidad con la que se puede difundir información a través de estas redes. Tú y tu organización pueden sufrir daños económicos o de reputación como resultado de una campaña de desinformación exitosa.

Un ejemplo de esto fue cuando una serie de tweets y anuncios de Starbucks se volvieron virales. Una promoción del "Día de los Soñadores" ofrecía bebidas gratis y descuentos para inmigrantes indocumentados. Esta campaña no fue una promoción real y fue creada por un grupo de personas anónimas que querían dañar la reputación de la organización.

Una de las mejores formas de luchar contra la propagación de la desinformación es verificar la veracidad de la información. Detente y verifica los hechos antes de actuar o compartir información.

ESTRATEGIA 4 - PRETEXTING (fingir) crea un escenario ficticio donde el mal actor finge ser otra persona para ganarse tu confianza y obtener información tuya. Puede suceder en persona, en una llamada telefónica, por mensaje de texto o correo electrónico.

Por ejemplo, recibes una llamada de alguien que te dice que es de tecnología y trabaja con Sam, que es alguien que conoces. Dicen que necesitan tu nombre de usuario y contraseña para verificar una actualización del sistema. Los escenarios de pretextos pueden ser muy convincentes, y este tipo de ataques van en aumento. Es importante que nunca brindes información por teléfono, en persona o en línea, a menos que hayas confirmado la identidad de la persona que la solicita.

Los métodos utilizados por los ciberdelincuentes para piratear tu dispositivo e irrumpir en la red de tu organización se conocen como el *panorama de amenazas*. El panorama de amenazas actual es extenso y se hace más grande cada día.

Independientemente del dispositivo que estés utilizando en la oficina o que trabajes de forma remota, los piratas informáticos podrían estar intentando utilizar uno de los siguientes tipos de ataques en tu contra. Saber cuáles son, te ayuda a asegurarte de que no dejes entrar a los delincuentes. A medida que aprendes más, recibirás breves comprobaciones de conocimientos en el camino.

ATAQUE 1 - PHISHING es el ataque digital más común. El phishing es el proceso en el que los delincuentes intentan engañarte para que proporciones información confidencial o realices una acción potencialmente peligrosa, como hacer clic en un enlace o descargar un archivo adjunto infectado. Lo hacen utilizando correos electrónicos disfrazados de contactos u organizaciones en las que confías, para que reacciones sin pensar primero.

Por ejemplo, recibes un correo electrónico que parece provenir de su departamento de tecnología y te informa que hay un problema con tu cuenta de correo electrónico y que necesitas restablecer tu contraseña. Se te pide que hagas clic en el enlace del correo electrónico. El enlace te lleva a una página de restablecimiento de contraseña con un campo de contraseña, que es lo que busca el pirata informático. Una vez que tenga tu contraseña, podrá acceder a tu cuenta. Lo usará para acceder a tu computadora y acceder a la red de tu organización.

ATAQUE 2 - SPEAR PHISHING es un pequeño y enfocado ataque por correo electrónico a una persona u organización en particular. El objetivo es penetrar las defensas de su organización. En este ataque, los delincuentes invierten tiempo en investigar un objetivo específico utilizando las redes sociales y otras fuentes abiertas de información. Armados con esta información, te envían un mensaje personalizado diseñado para engañarte para que tomes una acción que pondrá en riesgo a tu organización. Los ataques de Spear phishing pueden ser convincentes, pero al igual que en cualquier ataque de phishing, debes realizar una acción para que sea eficaz.

Una forma muy común de Spear phishing se dirige a la alta dirección, normalmente a las personas que interactúan con el director ejecutivo de su organización. Un pirata informático se hace pasar por tu director ejecutivo y te envía un correo

electrónico con instrucciones para hacer algo que podría dañar a la organización. Esta táctica se llama fraude de CEO y está ganando popularidad. ¡Incluso puede suceder por teléfono con un mensaje de voz falso!

ATAQUE 3 - SMISHING significa “phishing del servicio de mensajes cortos (SMS)” o phishing que se produce a través de mensajes de texto. Por ejemplo, envían un mensaje de texto pidiéndote que llames a un número o hagas clic en un enlace. El mensaje puede parecer que proviene de tu banco e incluso puede contener la mayor parte o la totalidad de tu número de cuenta, datos que suelen obtener los piratas informáticos de forma ilegal. Incluso si el mensaje que estás leyendo contiene tu contraseña o tu número de cuenta, aún puede ser fraudulento.

Algunos ciberataques no comienzan con un correo electrónico y pueden tener éxito sin solicitarte que tomes una acción específica a sabiendas.

ATAQUE 1 - SITIOS WEB. Cualquier sitio web es potencialmente peligroso, pero algunos son más peligrosos que otros: sitios de juegos de azar y sexualmente explícitos y aquellos que ofrecen descargas gratuitas, por nombrar algunos. Pero los sitios respetables y con mucho tráfico también pueden infectarse con publicidad maliciosa y ni siquiera es necesario hacer clic en el anuncio para que su computadora se vea comprometida. Este programa maligno puede infectar su estación de trabajo con solo acceder a una página web. A esto se le llama descarga directa. Consulta con tu departamento de tecnología o la política de seguridad de tu organización sobre cómo evitar este tipo de ataque. Nunca te conectes a una red Wi-Fi pública a menos que estés utilizando una VPN o una red privada virtual. Esta tecnología crea una conexión a Internet segura que protege tu actividad en línea de los malos. Se consciente de tu entorno y utiliza siempre una VPN cuando te conectes a una red Wi-Fi pública.

ATAQUE 2 - COMPARTIR MEDIOS SOCIALES. Una de las mayores amenazas de las redes sociales es la abundancia de información compartida que los ingenieros sociales pueden utilizar para engañarte a ti o a tu compañero de trabajo. Los planes de viaje son un ejemplo obvio de información que nunca debes compartir en línea. Anunciar que no estarás en casa nunca es una buena idea. Pero hay piezas de información menos obvias que pueden ponerte a ti y a su organización en riesgo. Cualquier tipo de información sensible es como oro para los piratas informáticos. Piensa en ello desde la perspectiva de un ingeniero social. ¿La información que estás a punto de publicar será útil para estafarte a ti o a tu compañero de trabajo? Asegúrate de comprender la política de tu organización con respecto a compartir información en las redes sociales.

ATAQUE 3 - PERFILES FALSOS. Otro truco eficaz que utilizan los delincuentes es crear un perfil con un montón de conexiones reales o falsas que parecen muy convincentes. Por ejemplo, el perfil podría parecer un cazatalentos que quiere hablar contigo sobre un cambio de carrera, un posible interés romántico o alguien en tu industria que quiere que hables en una próxima conferencia. Pero los perfiles falsos son una tendencia creciente en las redes sociales y están diseñados para engañarte. Por lo tanto, observa de cerca las solicitudes que recibas. Algunos aspectos comunes de un perfil falso incluyen fotos de perfil con calidad de modelo o similares a celebridades, un perfil incompleto o genérico, mala ortografía y/o gramática, o un historial de trabajo sospechoso. Los perfiles falsos a menudo te guiarán por un tiempo y luego le enviarán un enlace para hacer clic en el mensaje que parece tener sentido en el contexto de la conversación. Pero este enlace conduce a un sitio que puede infectar tu dispositivo con programa maligno. Ahora el pirata informático puede comenzar a entrar en la red de tu organización.

Los ciberataques también se pueden poner en marcha en persona o con una simple llamada telefónica.

Un ataque de ingeniería social en persona es cuando el pirata informático ingresa a tu ubicación e intenta "piratear humanos".

ATAQUE 1 - TAILGATING. (Ir a rebufo o muy pegadito a ti). Aquí es donde el pirata explora un área como la sección externa de tu empresa y luego se une a tu grupo, participando en la conversación del grupo. Cuando tu grupo regresa al trabajo, te sigue como cualquier otro empleado y luego encuentra una estación de trabajo que puede piratear e infiltrarse en la red de tu empresa.

ATAQUE 2 - Un ATAQUE FÍSICO de gran eficacia se basa enteramente en la curiosidad humana. Los piratas informáticos suelen utilizar unidades de memoria portátil para enviar programa maligno que infectará su dispositivo. Los atacantes dejan una unidad de memoria portátil que dice "Nómina" donde se puede encontrar fácilmente, como en el estacionamiento de su oficina, el vestíbulo de su edificio o un baño. O podrían enviarle un sobre por correo postal con una unidad memoria portátil en su interior que parece provenir de un cliente o un proveedor. Una vez que alguien se vuelve lo suficientemente curioso como para conectar esa unidad memoria portátil a su computadora, esa computadora es "propiedad" de los malos y la red de la organización puede verse comprometida.

ATAQUE 3 - VISHING. Otro nombre para la ingeniería social basada en el uso de líneas de teléfono convencional es phishing de voz o "Vishing". Al igual que el phishing, el Vishing es cuando el pirata informático te llama y trata de engañarte para que le entregues información confidencial. Por ejemplo, un pirata informático te llama con un mensaje pregrabado que se supone que proviene de un representante de atención al cliente de tu banco. Dice que hay un problema con tu cuenta y te pide que llames a un número falso de atención al cliente para aclarar las cosas. El representante de soporte es parte de la estafa. Ella te pedirá información de identificación personal (PII) como la información de tu tarjeta de crédito, PIN u otros detalles confidenciales. Una vez que tenga esta información, podrá acceder a tu cuenta y robar tu identidad y dinero.

No hay forma de evitarlo: Tú eres la última línea de defensa de tu organización. Comprender tu papel en la protección de la información confidencial de tu organización es un primer paso fundamental para tomar decisiones informadas y ayudar a tu organización a gestionar el problema continuo de las amenazas de ciberseguridad. Recuerda, solo se necesita un error para exponer toda la información sensible valiosa de la que eres responsable. Por eso es extremadamente importante detenerse siempre, mirar y pensar antes de realizar cualquier tipo de acción, incluido hacer clic en un enlace, abrir cualquier cosa que recibas o compartir información confidencial.

Y recuerda, si algo parece sospechoso, tómate el tiempo para verificar que se trata de una solicitud legítima con tu supervisor, el equipo de seguridad o alguien responsable de la seguridad de la información en tu organización antes de actuar.

¡Gracias por completar la capacitación!