TU TELÉFONO PODRÍA EXPONERTE A TODO TIPO DE PROBLEMAS.

SUPERAR CIBERAMENAZAS

Aprende a cuidar bien tus datos.

BONUS: ¡Descubre una nueva y emocionante carrera en ciberseguridad!

NATIONAL CRYPTOLOGIC FOUNDATION

El número de incidentes cibernéticos que afectan a empresas e individuos en los Estados Unidos aumenta cada día.

Cada vez que usas tu smartphone, tableta o computadora, compartes tus datos personales. ¿Sabes cómo protegertus datos? Tal vez hayas oído a tus padres, abuelos u otros adultos hablar de ciberataques en las noticias. ¿Qué significa eso? ¿Cómo podría afectar a tu familia? ¿Cómo podría afectarte a ti?

En un mundo cada vez más digital, debes aprender sobre la ciberseguridad y cómo cuidar los datos para protegerte a ti mismo, tus dispositivos y tus cuentas en línea creando contraseñas seguras y evitando abrir mensajes de personas que no conoces.

La National Cryptologic Foundation (NCF) es un experto destacado en educación cibernética K-12 y te anima a leer esta revista de ciberseguridad con tus profesores y padres. Este recurso te ayudará a aprender cómo mantenerte seguro frente a las ciberamenazas mientras te anima a aprender sobre temas de ciberseguridad y STEM (ciencia, tecnología, ingeniería y matemáticas).

En las páginas siguientes, aprenderás la importancia de cuidar tus datos. Los distritos escolares, hospitales, organizaciones de atención médica y empresas públicas, entre otros, no tienen el personal ni las habilidades para defenderse y la necesidad de profesionales de ciberseguridad crece diariamente. Queremos que esta revista despierte TU interés en la ciberseguridad para desarrollar habilidades en la escuela secundaria y preparatoria que puedan llevarte a elegir la ciberseguridad como tu profesión. ¡Es una industria en crecimiento! Visita **cyberseek.org** para ver los trabajos cibernéticos disponibles hoy y las que se esperan en el futuro, en tu estado.

La NCF es uno de un grupo de organizaciones que están desarrollando conjuntamente recursos para estudiantes y educadores K-12 a los que se puede acceder sin coste sin cargo. Por favor, visita nuestro sitio web **cryptologicfoundation.org** para acceder a estos recursos.

Extendemos nuestra gratitud a nuestro socio de desarrollo Start Engineering y a Gula Tech Adventures por financiar este proyecto crítico de cuidado de datos.

Atentamente,

Laura C. Nelson
National Cryptologic Foundation
Presidenta y Directora Ejecutiva

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21061
443-795-4498 ◆ booklet@cryptologicfoundation.org ◆ www.cryptologicfoundation.org

QUÉ HAY ADENTRO

SUPERAR CIBERAMENAZAS ➜ PÁGINA 3

Tu teléfono tiene un día ocupado

6:45 AM: Justo al lado de tu oído, algo hace clic y suena cuando se apaga la alarma de tu teléfono. Tu aplicación Sleep Cycle presume saber exactamente cuándo despertarte, pero siempre es demasiado temprano.

7:20 AM: Durante el desayuno, revisas las nuevas historias de Instagram de Nike y de algunos amigos; das *like* a un par de ellas, comentas en varias, compartes otras.

12:45 PM: Durante el almuerzo, ese chico Greg está jugando Words with Friends en línea con quién sabe quién y pidiendo ayuda a todos en la mesa. Ugh. Tu teléfono vibra con un mensaje de texto de un amigo del campamento del verano pasado sobre un nuevo juego divertido llamado Space Noodle con un enlace para descargarlo. Rápidamente, haces clic para descargar el juego también.

3:15 PM: Llega un mensaje de texto del director sobre las fotos escolares que se tomarán al día siguiente. Vaya rollo. Ahora a tu mamá realmente le importará qué ropa te pones.

PHOTOS BY ISTOCKPHOTO.COM UNLESS OTHERWISE INDICATED

6:45 PM: Después de la cena, te pones los auriculares, para escuchar una nueva playlist de Spotify que tu hermana compartió mientras buscas en Amazon nuevos cordones para las zapatillas que compraste allí la semana pasada.

7:50 PM: Te cuelas un poco en Netflix antes de las 8 en punto, cuando se apagan los teléfonos, justo cuando llega un mensaje de texto con una actualización del juego que descargaste en el almuerzo. Extraño, pero justo a tiempo, así que haces clic en el enlace y observas cómo se descarga el archivo antes de que se apague el dispositivo hasta el día siguiente.

Después de un día como este, tu teléfono ha aprendido sobre tus **hábitos de sueño**, **preferencias de ropa**, **sentido del humor**, **gustos musicales**, **hábitos de juego** y **sentido de la moda en calzado.** Y eso es solo el comienzo. Cada vez que interactúas con una empresa o una aplicación en línea, entregas aún más información.

Las empresas tienen un apetito voraz para la información. En un estudio para determinar cuales aplicaciones recopilan más datos, todas las empresas mencionadas anteriormente estaban en el top 25. Además de elementos obvios como tu **correo electrónico**, **nombre** y **número de teléfono**, estas aplicaciones también recopilan cosas como **edad, género**, **ubicación geográfica** y **dirección de casa**. Incluso aprenden sobre tus *hobbies*, cuenta bancaria y cualquier mascota que tengas. Ah, y a menudo las empresas recopilan gran parte de la misma información sobre todos con quienes te conectas a través de una aplicación: tu familia, amigos, contactos en línea, etc.

APLICACIONES QUE MÁS TE RASTREAN

GRAN IDEA 1:
La seguridad de los datos

Los datos están en todas partes. Están a nuestro alrededor todo el tiempo. Mantenerlos seguros, privados y correctos es un desafío crucial tanto para individuos como para organizaciones. Un aspecto de la seguridad de datos es mantener el control sobre el acceso físico a los dispositivos que almacenan datos. Otro aspecto implica el acceso virtual y todas las cosas que necesitamos hacer para mantener los datos digitales seguros de los delincuentes.

Piensa en todas las máquinas que recopilan y almacenan datos.

- ¿Cuántas puedes nombrar?
- ¿Dónde almacenan datos las personas en tu escuela?
- ¿Qué tipos de restricciones existen en tu escuela para mantener a las personas fuera de los espacios donde se almacenan datos?

Para acceder a tus datos almacenados en sistemas informáticos, generalmente tienes que pasar por dos "puertas": **autenticación** y **autorización**.

La autenticación es demostrar que tú eres tú. Generalmente implica algo que

- solo tú sabes, como una **contraseña**,
- solo tú tienes, como una **llave**, o
- solo tú eres—por ejemplo, tu **huella digital** o tu **retina**.

La autorización es lo que tienes permitido ver o hacer con los datos una vez que has demostrado que eres tú.

Los mejores sistemas de seguridad de datos combinan controles **físicos** y **virtuales** en múltiples capas o secuencias de medidas de seguridad. Si una capa falla en un ciberataque, las siguientes capas deberían estar listas para evitar un acceso adicional a los datos almacenados.

Piensa en dónde colocas tu teléfono por la noche, cuando está fuera de tu posesión física. ¿Qué tipos de capas de seguridad físicas y virtuales hay para protegerlo? ¿Puedes imaginar cómo cada una de estas capas podría fallar? ¿Qué podrías hacer para mejorar el perfil de la seguridad general de tu teléfono?

Tu negocio es un gran negocio

Se ha convertido en un gran negocio — no, en un negocio enorme — recopilar, analizar y luego vender información. En 2018, las empresas gastaron casi $20 mil millones en datos recopilados de nuestras actividades en línea. Con los datos en mano, no les resulta difícil conectar todos los puntos y conocernos a fondo.

Las empresas modelan nuestros comportamientos y preferencias para entender y predecir qué compramos, qué nos importa, qué sentimos y qué hacemos en el mundo real. Facebook, por ejemplo, reveló en 2017 que podía determinar cuándo los adolescentes en Australia y Nueva Zelanda se sentían "inseguros" o "sin valor" — resultados que la empresa luego compartió con los anunciantes.

La mayor parte del tiempo, las empresas utilizan los datos en línea para fines comerciales comprensibles: mejorar sus servicios y productos, aprender más sobre lo que todos queremos de ellos y desarrollar nuevas estrategias de marketing y publicidad. Los anuncios de cordones de zapatos que aparecen en tus búsquedas de Google, por ejemplo, son el resultado de los rastros que dejas en línea buscando nuevas opciones para los cordones de las zapatillas que acabas de comprar. Puede que nos sintamos un poco inquietos por lo bien que nuestras tecnologías personales parecen conocernos, pero los efectos a veces pueden ser útiles.

Lo que nos lleva al cibercrimen

Pero. Todos esos fragmentos y piezas de nuestro "yo" digital que se mueven en línea también presentan un **riesgo**. Las personas con malas intenciones pueden usar nuestros datos en línea de manera incorrecta y han hecho del **cibercrimen un gran negocio**. Los daños atribuidos al cibercrimen cuestan miles de millones de dólares cada año. Las brechas de datos exponen cientos de millones de cuentas en línea a una posible explotación criminal. Cada individuo u organización en línea puede verse afectado. Más de 1,000 escuelas han sufrido ataques cibernéticos en los últimos años, con daños que van desde la pérdida de dinero hasta datos filtrados y operaciones interrumpidas.

Mantener los datos en línea seguros de los malos actores es la principal preocupación de las personas que trabajan en la ciberseguridad. Intentan construir redes más seguras, teléfonos y computadoras más seguros, programas de seguridad más robustos y sistemas de gestión de datos que resistan la intrusión o el ataque.

La ciberseguridad es una industria en **rápido crecimiento**, con oportunidades emocionantes y grandes recompensas para las personas con las habilidades, intereses y determinación necesarios para tener éxito. En este libro, identificarás habilidades e intereses propios que podrían hacerte un buen candidato para trabajar en este campo.

CÓMO LAS ESCUELAS SON HACKEADAS

Uno de los peores ataques de datos afectó a más de 13,000 escuelas K-12 en 2019. El FBI descubrió que los piratas informáticos habían obtenido acceso a la información personal de muchos millones de estudiantes a través de los registros de Pearson, una empresa de servicios de examenes a nivel nacional. Los datos incluían los nombres de los estudiantes, correos electrónicos y fechas de nacimiento. La mayoría de las brechas de datos conocidas de K-12 ocurren debido a prácticas de seguridad laxas por parte de empresas u organizaciones que trabajan con escuelas, no por las escuelas mismas. Pero los riesgos de los datos de los estudiantes permanecen, y el problema solo empeora. Todos los recientes aumentos en el aprendizaje en línea y a distancia, debido a la COVID y otros factores, amplifican la dependencia de las escuelas K-12 en estas empresas externas para materiales, tecnología y servicios de aprendizaje. Estos intercambios crecientes expandirán las "superficies de ataque", o vulnerabilidades a amenazas cibernéticas, de los cuales las escuelas K-12 tendrán que aprender cómo protegerse.

A los criminales cibernéticos les encantan tus datos. He aquí el por qué.

A los malos en línea no les importan tanto los niños en sí mismos sino que les encantan sus datos. Eso se debe a que, por lo general, los niños no tienen un historial financiero adjunto a sus datos. Con un conjunto completo de datos de personas reales y sin historial financiero adjunto, los delincuentes pueden hacer todo tipo de cosas fraudulentas para pedir dinero prestado y gastarlo, todo en nombre de niños reales. La parte mala es que cuando estos niños crezcan y soliciten tarjetas de crédito, préstamos estudiantiles u otras formas de crédito y deuda, descubrirán que sus identidades ya están vinculadas a comportamientos financieros irresponsables o incluso ilegales, incluso si no tuvieron nada que ver con ellos en primer lugar.

Otra forma de pensar en la ciberseguridad

El trabajo más importante, sin embargo, es uno en el que todos participamos: cuidar mejor de nuestros datos desde el principio. Esto significa entender lo que compartimos sobre nosotros mismos con las empresas en línea y pensar detenidamente sobre lo que nos hace sentir cómodos.

Significa tanto **exigir que las empresas cuiden de nuestros datos** de la manera que deseamos como ser capaces de recuperar los datos que hemos compartido si demuestran no ser confiables. También necesitamos practicar una **seguridad en línea adecuada**: construir y mantener contraseñas fuertes, estar alertas a las estafas que nos llegan y compartir nuestra información personal solo con entidades conocidas y de confianza.

La ciberseguridad, junto con este plantamiento de responsabilidad individual por los datos, forman una idea más grande que llamamos **"cuidado de datos"**. Este término describe una empresa integral con muchas partes y piezas diferentes, todas dirigidas a asegurar que los datos en línea se usen de maneras apropiadas y seguras. El cuidado de los datos abarca actividades que van desde nuestros **comportamientos en línea individuales** hasta medidas técnicas de ciberseguridad, pasando por la esfera más amplia de **reglas**, **comportamientos**, **normas** y **procedimientos** que determinan cómo sociedad gestionamos los datos digitales y las experiencias en línea asociadas a ellos.

Probablemente entiendes que el cuidado de la salud implica mucho más que los médicos recetando medicamentos y arreglando huesos rotos. De hecho, tu cuidado de la salud comienza contigo: la comida que comes, las horas que duermes, el cuidado que le das a tu cuerpo. Y esa oficina del doctor funciona gracias a las enfermeras, asistentes y personal de oficina que son tan buenos en sus trabajos. Más allá de la oficina del doctor, las compañías de seguros gestionan los pagos para los proveedores de atención médica; todo tipo de empresas desarrollan medicamentos, fabrican equipos médicos y proporcionan servicios médicos; los investigadores investigan las causas y curas de enfermedades; los gobiernos establecen reglas sobre lo que todas estas personas deben y no deben hacer; y mucho más.

SE NECESITA AYUDA

Trabajos en la ciberseguridad para cubrir en 2024:

¡ 3.5 million!

PHOTO BY JOPWELL FROM PEXELS

Cool!

¿Qué se necesita para tener éxito en las carreras de ciberseguridad?

Podrías pensar que saber todo sobre computadoras, software y redes es lo que se necesita para tener éxito en la ciberseguridad. Para algunos trabajos, ese es definitivamente el caso. Pero para muchos más trabajos, se necesitan otros tipos de habilidades e intereses. Los líderes de alto nivel en ciberseguridad están de acuerdo en que la imaginación, la resolución de problemas, el trabajo en equipo, un compromiso con mantener a las personas seguras en línea y un deseo de aprender son más importantes que las habilidades técnicas. Las personas con estas habilidades pueden hacer enormes contribuciones para mantener a raya a los malos en línea y hacer que el internet sea más seguro para todos nosotros.

Tus datos llegarán a lugares en línea que nunca imaginarías

Cuidar de tus datos comienza CONTIGO y con lo que decides compartir en línea sobre quién eres, a dónde vas y lo que haces.

Algo para todos

El cuidado de los datos es sorprendentemente complejo y de gran alcance. Involucra a personas con una **amplia gama de habilidades**, **intereses** y **capacidades** que realizan muchos tipos de trabajos diferentes relacionados con la generación, recopilación, análisis, uso y protección de los volúmenes casi inimaginables de datos que se mueven y brillan a través de los dispositivos y las redes digitales. Y al igual que el cuidado de la salud, el cuidado de los datos comienza contigo. **Tus comportamientos y decisiones ahora pueden ayudar a mantener tus datos más seguros en línea**. En esta revista, aprenderás cómo lo que elijas hacer ahora puede ayudarte a comenzar camino hacia una carrera en este mundo.

La ciberseguridad puede ser técnica y centrada en la informática, y las habilidades en estas áreas son vitales para las protecciones digitales en línea. Pero para construir y mantener un entorno seguro para los datos en línea, también necesitamos personas que puedan hacer cosas además de escribir código, construir redes y desarrollar sistemas de seguridad. Necesitamos **solucionadores de problemas imaginativos**, **comunicadores creativos,** formuladores de políticas perspicaces, maestros conocedores, líderes empresariales reflexivos y, quizás lo más importante, ciudadanos informados.

En la Parte 2 de esta revista, aprenderás algunas cosas que puedes hacer ahora para protegerte a ti mismo y tus datos en línea. Y también aprenderás algunas cosas sobre ti mismo y tus intereses que podrían hacerte un buen candidato para trabajar en un campo relacionado con los datos. **Aunque no creas que una carrera de este tipoes sea para ti, podrías sorprenderte. ¡Sigue leyendo para descubrirlo!**

PARTE 1 CONCLUSIONES

➜ **Cada vez que interactúas con una empresa o una aplicación en línea, generas datos.**

➜ **Las empresas crean modelos de nuestros comportamientos y preferencias para entender y predecir qué compramos, qué nos importa, qué sentimos y qué hacemos en el mundo real.**

➜ **Los ciberdelincuentes roban datos para venderlos o para pedir un rescate por ellos de grandes sumas de dinero.**

➜ **Los daños atribuidos al cibercrimen ascienden a miles de millones de dólares cada año.**

➜ **Para estar seguro en línea, necesitas crear contraseñas fuertes y estar alerta ante las estafas.**

➜ **Mantener los datos en línea seguros de los malos actores es la principal preocupación de las personas que trabajan en ciberseguridad.**

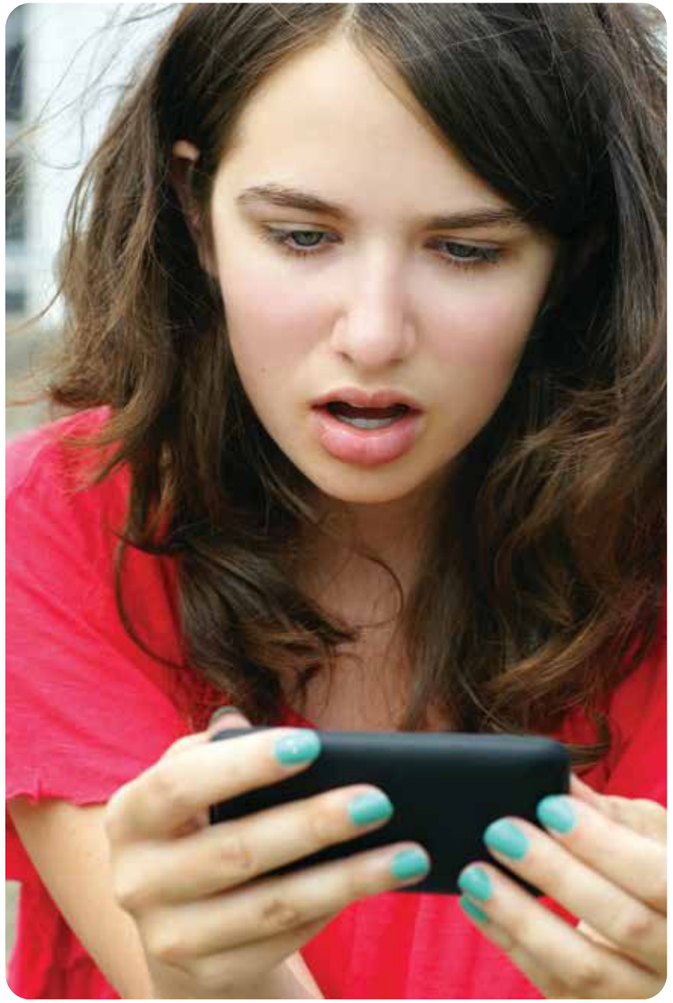
➜ **El campo de la ciberseguridad está lleno de empleos y necesita solucionadores de problemas con imaginación.**

El siguiente, terrible, muy mal día

6:45 AM: El mismo sonido de clic y pitido te despierta cuando la alarma de tu teléfono interrumpe el sueño profundo que estabas disfrutando. Algunos días comienzan peor que otros. Bueno...esperate y verás.

7:07 AM: Después de cepillarte los dientes, recoges tu teléfono y ves que la pantalla tiene más notificaciones de lo habitual. Muchísimas más. Está llena de notificaciones de mensajes de texto, de arriba a abajo.

7:09 AM: Has leído los primeros 14 mensajes. Todos dicen lo mismo: **"¡Somos el Equipo de Asalto Space Noodle 1! Hemos encriptado tu teléfono y todos los archivos están bloqueados. Perdedor. Envía $18 con tarjeta de crédito a este enlace o nunca volverás a abrir ninguna aplicación del teléfono: http://tiny.url.com/41s00pNe33"**



MIRAGE3/123RF

7:14 AM: En el siguiente lote de mensajes, un montón de tus amigos se están quejando de haber recibido un mensaje de texto tuyo recomendando un juego llamado Space Noodle. Y luego de recibir un mensaje raro sobre que sus teléfonos estaban bloqueados por un rescate. ¡¿Qué demonios...?!

7:17 AM: ¡Papá! ¡Mamá!

7:18 AM: Con la ayuda de tus padres, deslizas hacia la izquierda para eliminar todos los mensajes de texto sin abrirlos, haces un reinicio de tu teléfono y lo pruebas para ver qué pasa. ¡Uf! Todo funciona. ¿Solo una broma? ¿O tal vez un error? Lo que sea. Rápidamente eliminas la aplicación Space Noodle y empiezas a enviar mensajes de texto a tus amigos, diciendo lo siento, lo siento, lo siento, y les cuentas cómo pueden verificar si sus teléfonos están a salvo.

¿Cómo sucedió todo esto? Pasa la página para averiguarlo.

TÉRMINOS CLAVES DE LA SEGURIDAD CIBERNÉTICA

Malware: Abreviatura de "software malicioso", el malware es un software diseñado por criminales cibernéticos para acceder y dañar las computadoras o redes de otras personas. Generalmente se propaga a través de correos electrónicos o mensajes de texto que animan a las personas a hacer clic en enlaces o abrir archivos adjuntos que pueden servir para infectar los dispositivos de las personas.

Virus: Software escrito para dañar el rendimiento de los dispositivos, robar o alterar datos almacenados, o interferir con las funciones normales de una máquina o red.

Gusano: Software dañino que se replica y se propaga por sí solo entre computadoras conectadas a través de una red. Cuanto más se propagan en una red, más rápido pueden replicarse y causar problemas, desde ralentizar las redes hasta dañar archivos y sistemas operativos.

Spyware: Software de seguimiento que recopila datos capturando pulsaciones de teclas, hábitos de navegación u otros datos y comportamientos del usuario. Toda esta información es visible para el hacker que ha instalado el spyware en la computadora de otra persona.

Ransomware: Software que encripta datos en el dispositivo de alguien hasta que la persona acepte pagar una cantidad de dinero para recuperar el acceso a los archivos.

Phishing: Correos electrónicos aparentemente legítimos o inocentes que te piden responder con datos personales o hacer clic en un enlace; una vez que caes en la trampa, el hacker obtiene acceso a tu identidad en línea o incluso a tu dispositivo y hace cosas malas. Consulta la página 17 para obtener más información sobre el phishing.

El problema con la confianza

¿Qué salió mal con tu teléfono para que tuvieras un comienzo de día tan horrible? Bueno, primero, nada salió mal con tu teléfono. **Algo salió mal con *cómo* usaste tu teléfono**—específicamente, cómo confiaste en lo que recibiste.

Ese mensaje de texto con un enlace para descargar Space Noodle no provino realmente de tu amigo del campamento de verano. Provino de los hackers (quizás rusos, quizás chinos, o tal vez alguien que fingía ser ruso o chino) que infectaron el teléfono de tu amigo con malware.

El malware luego obtuvo acceso a todos los contactos de tu amigo y generó el mensaje extorsivo. Cuando hiciste clic en el enlace de Space Noodle dentro del mensaje de texto, descargaste ese mismo malware en tu teléfono, *¡y voilá!* Mensajes de texto amenazantes fueron enviados a todos tus amigos que también hicieron clic y descargaron la aplicación.

Confiaste en el mensaje de texto porque parecía provenir de alguien que ya conoces y en quien te confías en la vida real. Pero recibir una recomendación sobre un nuevo juego divertido de tu amigo en persona es diferente a recibir una recomendación por mensaje de texto. Como dicen, en internet, nadie sabe que en realidad eres un perro. Con solo un poco de disimulo en linea, **la gente puede aparentar casi cualquier cosa que quiera ser**.

Entonces, ¿cómo sabemos en quién y en qué confiar en línea? Todos aportamos mucha confianza a las cosas que hacemos en línea. Compramos zapatillas, libros, acciones y bonos, pagamos facturas, publicamos fotos e historias de nuestras vidas reales, todo con la confianza de que estos intercambios son seguros. Y sin embargo, al mismo tiempo, **necesitamos practicar una cautela inquebrantable en todo momento** por miedo a responder a una solicitud fraudulenta de datos de alguien en quien no deberíamos confiar. Construir y mantener la confianza entre personas, cara a cara, es bastante difícil. Y como especie, llevamos miles de años haciéndolo. Lograr la confianza entre una persona y una máquina, a través del internet, es aún más desafiante. Y apenas estamos empezando a descubrir cómo hacerlo.

Cómo detectar un intento de phishing

Reconocer un correo electrónico falso cuando lo ves es complicado. Los mejores se ven realmente convincentes, como muchos otros correos electrónicos en tu bandeja de entrada. Los hackers de phishing cuentan con que las personas no presten mucha atención a los correos electrónicos y simplemente hagan clic o respondan sin mirar detenidamente lo que están haciendo. Pero siempre hay algunas características reveladoras:

¡Son demasiado buenos para ser verdad! **El dinero a cambio de nada simplemente no sucede, ni en la vida real ni en el correo electronico.**

¡Actúa ahora! **Si te están presionando para que hagas algo, probablemente te estén engañando.**

Hiperenlaces extraños. **Pasa el cursor sobre un enlace y mira la URL en la parte inferior de la página. Si es extraña, aléjate.**

Archivos adjuntos inesperados. **Si no esperas un archivo adjunto, no lo abras. Regla facil. Siempre puedes responder para confirmar algo con el remitente.**

Remitente desconocido**. Si no conoces a la persona que te envía algo, no lo abras. Otra regla facil.**

Para practicar reconocer correos electrónicos de phishing, busca por internet y elige tres o cuatro de las opciones de cuestionarios rápidos y divertidos que aparecen.

GRAN IDEA 2:
Establecer la confianza

La confianza radica en el corazón de un sistema robusto y confiable de cuidado de datos. Para confiar en un sistema de datos en línea, necesitamos tener fe en tres cosas: la confidencialidad, la integridad y la disponibilidad de nuestros datos. Todos los sistemas en línea confiables deberían estar diseñados para que:

1. **Los datos sean confidenciales, accesibles solo para nosotros y personas autorizadas en la organización que posee nuestros datos.**
2. **Los datos tengan integridad; es decir, que sean correctos, auténticos y confiables, correspondiendo a la realidad fuera de línea tal como la conocemos y esperamos que sea.**
3. **Los datos estén disponibles, y que podamos acceder a ellos y utilizarlos cuando y donde los necesitemos.**

Diseñar un sistema de cuidado de datos que cumple con estos tres objetivos y que sea fácil de usar es complicado. La seguridad y la usabilidad siempre están en tensión. Si solo pudieras sacar dinero con simplemente meter tu nombre en la pagina web del banco, cualquier persona que conozca tu nombre y dónde tienes tu cuenta podría robarte fácilmente todo tu dinero.

Por otro lado, si para verificar tu saldo tengas que ingresar un nombre de usuario y una contraseña segura, hacer un escaneo de retina y responder tres preguntas de seguridad, probablemente sentirías que tu dinero este bien protegido. ¡Pero qué rollo!

La ciberseguridad siempre significa hacer concesiones entre **usabilidad** y **seguridad.** Como usuario, deberías evaluar qué tan bien protegen los sitios web los datos que envías: ¿Las contraseñas tienen requisitos de longitud y caracteres? ¿Iniciar una sesión requiere un código de un solo uso enviado por mensaje de texto a un dispositivo separado cada vez, o "autenticación de dos factores"? ¿La URL comienza con "https" o solo "http"?

Los diseñadores de sistemas de cuidado de datos deben equilibrar los requisitos de seguridad con la conveniencia del usuario, pero el equilibrio podría no ser siempre el más adecuado para ti. Siempre puedes alejarte de cualquier sitio web que parezca sospechoso. Recuerda, la única suposición segura y confiable sobre los datos en línea es que ***nada es completamente seguro.***

Cómo saber si un sitio web es seguro

Ambas partes del pacto de confianza entre la persona y la máquina deben cumplir su parte. Como usuarios de sistemas en línea, todos nos familiarizamos rápidamente con las herramientas básicas utilizadas para unirse a una red en línea: el nombre de usuario y la contraseña. Te presentas a una máquina con un nombre de usuario, como en: "Hola, soy FreeToBe@youandme.com. ¿Puedo entrar?" La máquina dice: "Hmm. No estoy segura de creer que eres quien dices ser. Voy a preguntarte algo que solo tú deberías saber." Luego ingresas una contraseña para demostrar que eres tú **(¿recuerdas la autenticación?)**, y obtienes acceso a los datos en ese sistema que tienes permitido ver **(autorización)**. Bastante simple, en teoría, aunque las personas logran estropearlo todo el tiempo. Más sobre eso más adelante.

En el lado de la máquina, las cosas son mucho más complicadas. La información sensible siempre debe estar encriptada. ¿Alguna vez has notado que las direcciones web comienzan con "http" o "https"? **La "s" significa "seguro",** lo que significa que tus datos están encriptados en un galimatías sin sentido mientras se mueven de ti a la máquina y viceversa. Y solo la máquina tiene la clave para traducir, o desencriptar, el galimatías de nuevo en tus datos personales.

¿Qué tan fuertes son tus contraseñas?

¿Crees que sabes cómo crear una contraseña fuerte? La mayoría de la gente no lo sabe.

Una contraseña de ocho letras puede ser descifrada en aproximadamente cinco segundos. Agrega unos pocos números y toma alrededor de un minuto.

Descifrar contraseñas simples es un juego de niños incluso para hackers novatos. Las contraseñas más comunes son cosas como 123456, contraseña, déjame entrar, abc123, y así sucesivamente. Si alguna de tus contraseñas se parece a estas, deja de leer este libro y cámbialas ahora.

Una contraseña fuerte es única, un código único que usas solo una vez. Debe ser más bien larga que corta (más de ocho caracteres). Usa números, letras mayúsculas y minúsculas, y símbolos. Evita la información personal. Lo mejor de todo es idear un sistema que puedas usar para generar, recordar y usar contraseñas. Incluso puedes usar oraciones o frases completas, como "lluvia, lluvia, vete" o "mi avatar tiene el pelo azul." Los gestores de contraseñas también pueden funcionar, siempre y cuando no olvides la contraseña principal.

Obtén muchos más consejos sobre contraseñas y otras prácticas de seguridad en línea en StaySafeOnline .org.

El pacto de confianza

Las organizaciones deberían tener reglas estrictas sobre quién puede ver la información que proporcionas y quién puede hacer algo como cambiarla, moverla o venderla (lo que sucede todo el tiempo). Las máquinas que almacenan tu información deben estar encendidas, accesibles y físicamente protegidas en todo momento, con sistemas de respaldo en su lugar para los inevitables contratiempos.

Muchas cosas pueden salir mal en ambos lados de este pacto de confianza, y cuando lo hacen, el nivel de confianza sufre. Si ingresas tu contraseña incorrectamente demasiadas veces, la máquina podría decir: "Lo siento, vuelve más tarde e intenta de nuevo". Cuando descubres que una máquina ha manejado mal tus datos, deberías pensarlo dos veces antes de compartir más datos.

Pero incluso cuando las cosas van bien entre tú y la máquina, las cosas pueden salir mal en línea. Tu teléfono se infectó con malware porque los hackers explotaron una amistad tuya para manipular la transmisión de un mensaje de texto aparentemente inofensivo. Leíste el mensaje, hiciste clic en un enlace, y ocurrieron cosas malas como resultado.

Para cuidar mejor de tus datos, imagina cómo las cosas pueden salir mal para mejorar las posibilidades de que las cosas salgan bien. Desarrolla una

mentalidad de seguridad.

Debes llevarla contigo a donde vayas en línea.

Una mentalidad de seguridad

Pero nada de esto ocurrió por una falla en la seguridad de la máquina. Todo fue un error humano, inducido por la llamada ingeniería social. **La ingeniería social implica engañar a las personas para que crean que están involucradas en intercambios confiables.** De hecho, estos intercambios están "diseñados" exclusivamente para parecer confiables, trucos destinados a engañar. Muchas cosas malas suceden en línea porque las personas confían en cosas que no son lo que parecen. Y esta confianza les lleva a hacer cosas que no deberían hacer.

Una de las formas más comunes de ingeniería social en línea es el **"phishing",** que se asemeja al mensaje de texto de Space Noodle. Llega un mensaje fingiendo ser de alguien ya conocido para el destinatario. Pide información que permite al remitente obtener acceso indebido a la máquina del destinatario, a su cuenta en línea u otro activo digital. No importa cuán bien guardemos contra estos trucos, aún funcionan. Un estudio encontró que el 30 por ciento de las personas abren correos electrónicos de phishing y el 12 por ciento hacen clic en enlaces en ellos.

El phishing es solo una de las armas en el arsenal de engaño y trucos de los criminales cibernéticos. **Una mezcla de brujas de viruses, estafas, esquemas disruptivos y ataques directos acecha en los rincones oscuros de internet.** El problema es que nunca sabes de dónde vendrá el próximo ataque. Entonces, ¿qué hacemos?

Como principio general, asume que todas las redes que almacenan y transmiten datos no son seguras. Si esperas que todos los sistemas de cuidado de datos tengan fallas, abordarás cualquier solicitud digital de un clic o información personal con una mayor precaución. Desarrollarás el hábito de buscar formas en que las cosas pueden salir mal en los sistemas de seguridad en línea. En otras palabras, comenzarás a desarrollar una **"mentalidad de seguridad"**, una capacidad para pensar como un atacante, no solo como un usuario, de redes en línea.

Los mejores profesionales de la ciberseguridad, sin importar el papel que tengan en la protección de internet, abordan sus tareas con una mentalidad de seguridad. En la Parte 3, aprenderás más sobre cómo puede ser una mentalidad de seguridad y cómo comenzar a desarrollar tu propia versión de ella. Podría ser la mejor herramienta de seguridad en línea que aprendas a usar.

CUIDA LO QUE DICES, ENVÍAS O CAPTURAS

A los niños les encantan las aplicaciones de textos. Es tan fácil enviar un "¿qué tal?" o una broma, un selfie divertido, un video, lo que sea. Y luego el mensaje desaparece, ahogado en un hilo que crece rápidamente, a medida que pasa el momento. Excepto cuando el mensaje no desaparece. Y es algo privado, como una foto que el mundo definitivamente NO debería ver. Las peores pesadillas de selfies

de los adolescentes se hicieron realidad en 2014 cuando más de 100,000 mensajes reveladores de Snapchat fueron hackeados, y en poco tiempo, miles de fotos y videos extremadamente inapropiados de niños, algunos tan jóvenes como de 13 años, se publicaron en línea para que todo el mundo los viera. ¿La lección? Cuenta con cualquier cosa que publiques o compartas en línea se haga pública. Una vez que haces clic en enviar, pierdes el control, y el mensaje queda suelto en el mundo.

PARTE 2 CONCLUSIONES

→ **Cuenta con que cualquier cosa que publiques o compartas en línea se haga pública.**

→ **Los hackers de phishing cuentan con que las personas no presten mucha atención a los correos electrónicos y simplemente hagan clic o respondan sin mirar detenidamente lo que están haciendo.**

→ **Para confiar en un sistema de datos en línea, necesitamos tener fe en tres cosas: la confidencialidad, la integridad y la disponibilidad de nuestros datos.**

→ **Una contraseña fuerte contiene al menos ocho caracteres, incluidos números, letras mayúsculas y minúsculas, y símbolos.**

→ **La ingeniería social implica engañar a las personas para que crean que están involucradas en intercambios o actividades confiables.**

→ **Desarrollar una "mentalidad de seguridad" te mantendrá más seguro en línea y podría llevarte a una carrera emocionante.**

El día mejora... eventualmente

8:15 AM: Vestido para las fotos, entras a la escuela preguntándote qué es lo qué te van a decir tus amigos con teléfonos infectados con malware.

8:22 AM: Después de que tres personas te empujen sus teléfonos llenos de demandas de rescate mal escritas bajo la nariz, acompañadas de variaciones de "¿oye, esto?!", obtienes tu respuesta. La gente está molesta.

8:25 AM: Adele, esa chica a veces antipática con un casillero cerca del tuyo, te mira de arriba a abajo mientras guardas tu mochila. "¡Ja!" dice ella. "¡Qué mona te ves! ¿No sabías? El mensaje de texto sobre las fotos escolares fue una broma. ¿Lees mucho el calendario escolar?"

10:15 AM: Para cuando llegas al recreo de la mañana, te das cuenta de que eres una de las pocas personas que cayó en la broma de las fotos escolares. Pasar todo el día con ropa formal se siente como tener una etiqueta de "perdedor" pegada en la espalda.

GETTY IMAGES/ JON FEINGERSH PHOTOGRAPHY INC

12:30 PM: En el almuerzo, te enteras de que atraparon a los chicos que enviaron el mensaje de broma. Resulta que se colaron en la oficina del director, encontraron el nombre de usuario y la contraseña para la cuenta de mensajes de texto de la escuela un Post-it, y enviaron el mensaje como una broma. No hubo daños reales, pero aun así es un gran problema para aquellos chicos, y una lección para el director de cuidar mejor sus credenciales de inicio de sesión.

3:45 PM: Tu papá está emocionado por algo cuando llegas a casa. "Oye, mira, podemos conseguir gafas de sol Ray-Ban por $20 en una super oferta, solo por hoy. Vi un tweet al respecto." Tus antenas reciéntemente sensibilizadas del cuidado de datos se activan de inmediato. "¡¿Qué?! Papá, eso suena totalmente sospechoso. Nunca están en oferta. ¿Un tweet? ¡Vamos!"

3:55 PM: Efectivamente, una búsqueda rápida de "estafa de venta de Ray-Ban" muestra múltiples desmentidos. Tu papá te da una mirada avergonzada. "Um, gracias. Debería haberlo sabido mejor después lo que nos pasó esta mañana." Tú respondes, "Exacto. Estoy listo para apagar mi teléfono para siempre."

4:15 PM: ***Buzz.*** Tu teléfono se enciende con un mensaje de texto de tu amigo Rafael. "¿Quieres jugar a Murder Mystery 2 en mi servidor privado?" Te vas a la tierra de Roblox. Tal vez los teléfonos no sean tan malos después de todo.

LAS PERSONAS HACEN COSAS TONTAS

En una visita a la *Oval Office* de la Casa Blanca en 2018, Kanye West sacó su teléfono e ingresó su código de acceso para desbloquearlo, frente a un grupo de cámaras de televisión que transmitían el evento en vivo. Millones de personas aprendieron al instante que el código de acceso de Kanye era "000000", algo tan fácilmente adivinable y revelado de forma tan descuidadaque casi podías escuchar el golpe de las palmas de las manos en las frentes de los expertos de seguridad en línea el país.

Pero resulta que, Kanye está lejos de ser el único en tomar malas decisiones sobre la seguridad en línea. Un estudio de IBM encontró que casi todas las brechas de seguridad en línea, un 95 por ciento en total, ocurrieron por personas cometiendo errores o haciendo cosas tontas con el acceso a los datos en línea. Cuando la contraseña más común utilizada en línea es "123456" y la segunda más común es "123456789", es fácil imaginar cuán poco pensamiento dedican las personas a cuidar los datos. Lo que solo demuestra cuán seguro sería internet si no fuera por las personas que lo usan.

EXAMEN RÁPIDO

¡Hora de demostrar lo que sabes! Haz este cuestionario para ver qué tan bien puedes evaluar el riesgo en escenarios de la vida real que involucran datos personales.

1. Todos los que conoces quieren un WhatZaDoodle. Encuentras uno en http://www.WtZaDoo4U.com, y por la mitad de lo que cuesta en Amazon. Te apresuras a ingresar la información de la tarjeta de crédito de tus padres y haces clic en el botón de "comprar". ¿Seguro o no? ¿Y por qué?

RESPUESTA: ¡No es seguro! La dirección del sitio web dice "http", no "https"; debes asumir que la información sensible estará expuesta porque el sitio web no encripta automáticamente los datos de las transacciónes en línea.

2. Puedes obtener un virus en tu teléfono o computadora al abrir un correo electrónico. ¿Verdadero o falso?

RESPUESTA: Falso. Debes hacer clic en un enlace o descargar un archivo adjunto para que un virus infecte tu dispositivo. Aun así, si aparece un correo electrónico sospechoso en tu bandeja de entrada, es mejor eliminarlo sin abrirlo.

Vivir con el riesgo en línea

A veces, hay que aprender una leccion de manera dificil. Al final de un día terrible con tu teléfono, aplicaste un nuevo entendimiento de cómo las cosas pueden salir mal en línea para salvar a tu papá de entregar la información de su tarjeta de crédito a los estafadores de gafas de sol. Tu mentalidad de seguridad en acción te ayudó a reconocer un riesgo claro y presente, y actuaste para mantener a tu familia a salvo de problemas en internet.

Como sabes ahora, cada intercambio de datos en línea implica un riesgo. Pero eso no nos impide ir en línea. Cada vez que compartimos o recopilamos datos, tenemos que evaluar el riesgo decidir si hacer o no lo que nos hemos propuesto hacer. Para tu seguridad personal en línea y tus opciones de carrera, manejar el riesgo es fundamental. Así que hablemos del riesgo.

El riesgo puede entenderse como una combinación de dos factores: la probabilidad de que ocurra algo malo y cuán malo sería si llegara a ocurrir. En otras palabras, la probabilidad de daño y el grado de daño. Es necesario analizar ambas variables para evaluar el riesgo de cualquier intercambio de datos en línea. A veces, la probabilidad de riesgo podría ser alta pero el daño potencial no tan grave, y por lo tanto, sigues adelante. Colgar una foto tonta de ti mismo en Instagram podría ser embarazoso pero probablemente no dañino, así que lo haces de todos modos.

Otras veces, la probabilidad de daño es baja pero el daño potencial es serio. Pagarle a alguien por PayPal conecta tu cuenta bancaria o tarjeta de crédito con la institución financiera de otra persona, pero la encriptación y la seguridad general de la transacción son tan fuertes que lo haces por conveniencia. Y luego hay momentos en los que tanto la probabilidad de daño como el daño en sí son demasiado grandes para completar la transacción, como con la estafa de las gafas de sol.

En todos estos casos, **evalúas los factores de riesgo en juego y luego tomas una decisión sobre qué acción tomar**. Es exactamente este cálculo el que está en el corazón de casi todos los trabajos que puedas imaginar en el mundo profesional del cuidado de datos.

Cómo los profesionales del cuidado de datos evalúan el riesgo depende del tipo de responsabilidad que sus trabajos les dan para proteger los datos. Trabajos de cuidado de datos se dividen entre tres campos amplios dentro del panorama de carreras. Mirar hacia atrás a los problemas que tuviste con tu teléfono puede ilustrar de qué se tratan estos campos.

GRAN IDEA 3: El riesgo

El riesgo forma parte de nuestra vida todos los días. Siempre estamos juzgando qué tan malo podría ser algo contra la posibilidad de que llegue a ocurrir a la hora de tomar decisiones sobre qué hacer o qué NO hacer. Evaluar el riesgo para los datos y sistemas en línea ocupa la atención de los profesionales del cuidado de datos. Es casi una fórmula: **la posibilidad de daño a una red o sistema por la probabilidad de que dicho daño realmente ocurra.**

Tres factores básicos impulsan la evaluación del riesgo por parte de los profesionales del cuidado de datos, y cada uno de estos factores se basa en diferentes tipos de habilidades e intereses. Sigue leyendo para ver dónde podrías encajar en el negocio de evaluar riesgos:

LA VULNERABILIDAD: Una debilidad de la seguridad de un sistema, como una cerradura rota en la puerta de tu casa. Encontrar vulnerabilidades puede requerir conocimientos técnicos de programas, computadoras y redes. El trabajo puede ser como navegar por un laberinto o resolver un cubo de Rubik. Si te gustan estos tipos de actividades, esta área del cuidado de datos podría ser divertida para ti.

LA AMENAZA: Los tipos malos, los ladrones merodeando por la noche buscando casas para robar. Identificar y rastrear amenazas significa averiguar quién podría querer hacerse con los datos en un sistema que estás protegiendo. Podría ser cualquiera, desde los tipicos malos hasta criminales organizados o fuerzas militares o de inteligencia de otros países. Si te gusta pensar en qué motiva a otras personas, analizar amenazas podría ser un buen trabajo para ti.

EL ATAQUE: El evento en sí, un ladrón entrando y buscando algo para robar. Los ataques pueden venir de cualquier dirección en cualquier momento. Tienes que estar alerta y preparado, listo para defender tus redes contra un ataque y luego para contraatacar. Si los tipos malos te hacen hervir la sangre y te gusta la intensidad de la competencia, podrías encontrar satisfacción en trabajo.

Cómo funcionó la estafa

La estafa de Space Noodle tenía dos partes: (1) malware escrito por alguien con malas intenciones y (2) una estrategia para engañarte y hacer que confiaras en un mensaje de texto fraudulento.

El desarrollo y la entrega del malware son aspectos del **"campo lógico"** de las carreras de cuidado de datos. Las personas en el campo lógico estudian las formas en que los chicos malos usan software y dispositivos en línea para atacar redes y datos de redes. También desarrollan programas y maquinaria, todo basado en la "lógica" de los circuitos y la electrónica, para proteger contra todo tipo de ciberataques.

La estrategia para engañarte se basa en tu confianza en un amigo, y muestra la importancia de comprender la psicología y el comportamiento humano. Este **"campo social"** aborda los elementos interpersonales, o sociales, de los intercambios en línea, ya sea que comiencen en la vida real y se trasladen en línea o tomen forma totalmente digital. Las personas en este campo estudian y/o intentan moldear los procesos de pensamiento, acciones y valores que aportamos a las actividades en línea. Maestros, investigadores, funcionarios gubernamentales, empresarios y agentes de la ley están entre aquellos preocupados por cómo nuestros seres sociales, del mundo real, pueden exponernos a riesgos en línea.

La broma de las fotos escolares ocurrió porque los niños obtuvieron acceso físico a los datos en un lugar destinado a estar fuera de límites. Entonces, en este **"campo físico"**, las personas trabajan en controles de seguridad, creando y protegiendo espacios donde se almacenan datos y equipos. Eso incluye a todos, desde arquitectos e ingenieros involucrados en el diseño, hasta constructores y personal de seguridad, y fabricantes y vendedores de tecnologías utilizadas para monitorear y proteger los espacios físicos.

El cuidado efectivo y confiable de los datos requiere de muchas personas haciendo muchos tipos de trabajos.

Sea lo que sea en lo que seas bueno o te guste hacer,

hay un lugar para ti.

El mundo te necesita

Cualquiera que sea su trabajo en estos campos, los profesionales del cuidado de datos dependen de las mismas capacidades básicas: **evaluar riesgos**, **conocer sus áreas de especialización** y **resolver problemas con imaginación.** Y lo que los impulsa a todos es el compromiso de hacer del internet un lugar más seguro para todos.

Cuanto más puedas aprender sobre los trabajos reales que estas personas hacen, mejor podrás decidir si una carrera en uno de estos campos podría funcionar para ti. A estas alturas, ya sabes bien que los profesionales en estos campos se centran en mantener nuestros datos seguros en todas las formas en que se transmiten y almacenan en línea. En la Parte 4, comenzarás a aprender cómo **conectar tus habilidades e intereses con posibles carreras en estos campos**. Y descubrirás más sobre lo que significa "mantener nuestros datos seguros" en trabajos que las personas hacen.

PARTE 3 CONCLUSIONES

➜ **Casi todas las brechas de datos son el resultado de malas decisiones que toman las personas. Nosotros, las personas, presentamos el mayor riesgo para nuestros propios datos.**

➜ **Para evaluar el riesgo, necesitas entender la probabilidad de que ocurra algo malo y cuán malo sería si llegara a ocurrir.**

➜ **El riesgo está en todas partes en línea. Pero aún así usamos el internet todo el tiempo. Tenemos que ser inteligentes al respecto.**

➜ **Los trabajos de cuidado de datos involucran una increíble variedad de habilidades e intereses. Los trabajos se pueden dividirse en tres áreas generales: el campo lógico, el campo social y el campo físico.**

➜ **No hay duda de que encontrarás un lugar en el campo que funcione para ti, si así lo deseas.**

Cómo hacen lo que hacen

Las personas que trabajan en el cuidado de datos **hacen muchas cosas diferentes en sus trabajos**. Podrías suponer que escriben código, trabajan en computadoras y estudian datos y tráfico de redes en línea. Y eso a menudo es cierto. Pero igual de frecuente, no escriben nunca una línea de código en toda su carrera.

En su lugar, ponen en práctica otras habilidades y capacidades. Las personas que son buenas en—y disfrutan de—trabajos en el cuidado de datos recurren a la **imaginación y la persistencia** para resolver problemas. Problemas difíciles. Encuentran patrones y conexiones donde otras personas solo ven diferencias. Les gusta resolver rompecabezas con palabras, números, imágenes o piezas. Crucigramas, Sudoku, Tangrams, esos rompecabezas 3D que se resuelven con piezas de madera entrelazadas.

A muchos de ellos les gusta **resolver problemas difíciles en equipos** o, aún mejor, en competencia con otros equipos.

PHOTO BY FAUXELS FROM PEXELS

Trabajar juntos, bajo presión, y contra reloj, saca lo mejor de ellos. Son buenos para escuchar las ideas de los demás, conectar esas ideas con lo que ellos mismos saben y poner todo junto de una manera que ninguno de ellos podría hacer.

Los trabajos que realizan son importantes. Los ciberataques pueden costar mucho dinero a personas, empresas y gobiernos. También pueden causar daños reales. A principios de 2021, unos hackers irrumpieron en el sistema de control de una planta de tratamiento de agua en Florida y comenzaron a envenenar el suministro de agua de una ciudad de unas 15,000 personas. Los operadores de la planta fueron avisados a tiempo y pudieron detener el ataque y restaurar el sistema. La noticia del ataque provocó revisiones y mejoras generalizadas de los sistemas informáticos utilizados para gestionar programas de seguridad del agua en todo el país.

En un trabajo de cuidado de datos, siempre estarás trabajando **para proteger algo valioso e importante para tu organización, tu comunidad, tal vez incluso tu país**. Tendrás que ser imaginativo, colaborador y tenaz en el cumplimiento de tu misión. Si piensas que eso suena divertido, podrías estar encaminado hacia el éxito en el campo.

TODO ESTÁ EN CÓMO LO MIRAS

¿Te gusta resolver acertijos y rompecabezas difíciles? ¿Puedes ver los problemas desde un ángulo ligeramente diferente al de otras personas? Si es así, podrías ser un buen candidato para trabajar en el cuidado de datos. Intenta resolver estos problemas. Busca formas creativas y diferentes de "ver" las preguntas. Recuerda, puedes aprender y mejorar en la "resolución de problemas imaginativa" una vez que te acostumbras.

1. Qué tiene la palabra murcielago de especial?

2. Estudia las primeras tres lineas para averiguar el patron y el numero que vendria entre el 96 y el 78.

46, 10, 28
17, 8, 44
39, 12, 57
96, __, 78

3. Considera estos nombres para averiguar un patron:

Lucero, Manuel, Martin, Juan, Victor, Samuel, Santiago

PISTA 1: Fíjate en la primera letra de cada nombre.

PISTA 2: Fíjate en el orden de esas letras.

RESPUESTA #1: *Contiene los cinco vocales.*

RESPUEST #2: *Los numeros en el medio son iguales a las sumas de los digitos de los numeros en cada lado. Por lo tanto, el numero que falta en la cuarta linea es 15 (9+6, 7+8).*

RESPUESTA #3: *Las nombres empiezan con las mismas letras que los dias de la semana: Lucero-lunes; Manuel-martes etc.*

¿Es la ciberseguridad adecuado para ti?

Aprender sobre ejemplos del mundo real de brechas de datos y ciberataques puede ayudarte a entender qué significa realmente "mantener nuestros datos seguros". Las noticias sobre fallas en la seguridad de los datos aparecen casi todas las semanas. Puedes encontrarlas en la televisión, en el periódico, en línea, en cualquier lugar donde buscas información sobre lo que está sucediendo en el mundo. Y puedes pedirles a tus padres o profesores que te ayuden a profundizar más en estas historias. Busca documentales, artículos de revistas y libros, e incluso personas en tu propia escuela que trabajan con las computadoras y redes utilizadas por estudiantes, profesores y personal.

Cada vez más clubes y programas extracurriculares se centran en temas de la ciberseguridad y la seguridad en línea. GenCyber, por ejemplo, es un programa de campamento de verano que se lleva a cabo en los campus universitarios de todo el país. ¡Patrocinado por el gobierno federal, es gratis asistir! Visita www.gen-cyber.com. Y puedes aprender mucho más sobre el campo en el sitio web de la *National Cryptologic Foundation* (www.cryptologicfoundation.org).

ICONS BY KEVIN MYERS

Tipos de trabajos en ciberseguridad

En la batalla contra los delincuentes en línea, las personas con trabajos más técnicos y centrados en la seguridad están en la primera línea.

INVESTIGADORES	**Investigan y revisan los ciberdelitos.**	A menudo trabajan con las fuerzas del orden y la contrainteligencia.
ANALISTAS	**Recogen y analizan información sobre amenazas de múltiples fuentes.**	También evalúan las capacidades y actividades de los delincuentes cibernéticos.
PROTECTORES	**Buscan debilidades en software, hardware y redes.**	También conocidos como "hackers éticos", trabajan en muchos campos diferentes.
PROGRAMADORES	**Conceptualizan, construyen y prueban sistemas informáticos seguros.**	También crean herramientas para la detección de viruses, spyware o malware.
GERENTES	**Supervisan el programa de ciberseguridad.**	También ofrecen asesoramiento y recomendaciones legales o de políticas.

Conoce a algunas personas en la ciberseguridad

Rachel Tobac es una hacker de sombrero blanco y la CEO de SocialProof Security, una empresa que ofrece capacitación y consultoría en ingeniería social para empresas e individuos. Los clientes de SocialProof incluyen PayPal, Snapchat, Facebook, la Fuerza Aérea de los EE.UU. y Uber.

Alissa Abdullah es Subdirectora de Seguridad en Mastercard, una de las empresas de servicios financieros más grandes del mundo. Trabajó en temas de seguridad en la Casa Blanca para el Presidente Obama y ha liderado numerosos esfuerzos para atraer a niñas al campo de la ciberseguridad.

Yonesy Feliciano Nuñez es Director de Seguridad de la Información en Jack Henry & Associates, una empresa que maneja pagos para clientes de servicios financieros. Ha creado nuevas herramientas para mantener el dinero y la información seguros en línea.

Diva Hurtado es Gerente de Producto en Dashlane y tiene experiencia en juegos móviles. Ella imparte clases de autodefensa digital para mujeres y otras personas que son desproporcionadamente vulnerables a los ciberataques.

O'Shea Bowens es Fundador y CEO de Null Hat Security, una empresa propiedad de minorías que se enfoca en soluciones de seguridad y alcance a audiencias diversas, tanto individuales como corporativas. Comenzó como hacker en su adolescencia y siguió aprendiendo hasta convertirse en un orador y consultor de seguridad muy solicitado.

Chris Krebs fue Director de la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EE.UU. hasta noviembre de 2020. Lideró los esfuerzos altamente exitosos del gobierno federal para garantizar una elección segura y justa para la presidencia en 2020. Se involucró en la ciberseguridad después de estudiar ciencias ambientales en la universidad y luego obtener un título en derecho.

Tu escuela probablemente ofrecerá clases de informática cuando llegas a 9º grado. Toma una o dos clases para aprender los conceptos básicos. Aunque gran parte del contenido puede ser técnico, recuerda que los trabajos en el campo varían mucho. Todos deberían entender algo sobre computadoras y redes, pero hay tantos o más trabajos esperándote en los campos "social" y "físico" como en el "lógico".

Proteger el mundo en línea es una misión y un desafío que todos compartimos. A medida de que más y más de nuestras vidas se trasladan al internet, necesitamos cuidar mejor de nuestros datos como individuos y como país. Hemos tratado de mostrarte cómo cuidar mejor de los datos en tu vida personal, y cómo puedes hacerlo en una carrera. Lo que necesitas decidir es si quieres hacerlo. Necesitamos personas como tú, nuestros mejores y más brillantes estudiantes con el deseo de hacer del mundo un lugar mejor, para ayudarnos a todos a llevar vidas más seguras y mejores en línea.

PARTE 4 CONCLUSIONES

- **Las personas con carreras en el cuidado de datos hacen muchas cosas diferentes, pero todas recurren a la imaginación y la persistencia para resolver problemas.**
- **Trabajando juntos en problemas difíciles, los profesionales del cuidado de datos logran cosas que no podrían hacer por su cuenta.**
- **Los ciberataques pueden causar daños reales. En un trabajo de cuidado de datos, siempre estarás protegiendo algo valioso e importante para otras personas.**
- **Aprende más sobre el campo siguiendo las noticias de ciberataques y tomando algunas clases de informática.**
- **Proteger el mundo en línea es una misión que todos compartimos. Necesitamos a nuestros mejores y más brillantes estudiantes para ayudar a hacer que internet sea más seguro para todos nosotros. ¿Podrías ser tú uno de ellos?**

The National Cryptologic Foundation (NCF) tiene ofertas educativas para estudiantes, maestros, consejeros, administradores y padres.

➜ La NCF y nuestro socio estratégico *Teach Cyber* desarrollaron las ***High School Cybersecurity Curriculum Guidelines***. Las CCG de la Escuela Secundaria alienta a los proveedores de currículos, maestros e empresas a crear un currículo diseñado para inspirar a los estudiantes de secundaria a seguir una profesión en ciberseguridad y desarrollar pensadores con una mentalidad de ciberseguridad que mejorará cualquier carrera que persigan. Las pautas están disponibles para los departamentos de educación estatales y los distritos escolares de todo el país a través de nuestro socio *Teach Cyber*.

➜ Con nuestro socio *Teach Cyber*, ahora está disponible **un curso introductorio de ciberseguridad para la escuela secundaria** de un año de duración basado en el CCG. El objetivo del curso es introducir a los estudiantes a los conceptos, principios y herramientas fundamentales de la ciberseguridad. Todos los materiales desarrollados están bajo licencia de Creative Commons y están disponibles sin costo alguno para las 130,000 instituciones K-12 a través de *Teach Cyber*.

➜ La NCF organiza **talleres de desarrollo profesional en ciberseguridad para maestros** sobre el CCG y el curso de ciberseguridad. La capacitación prepara a los maestros para enseñar ciberseguridad al desarrollar de manera significativa su conocimiento en ciberseguridad y cómo enseñarlo.

➜ La NCF lleva la educación en ciberseguridad a las aulas y hogares a través del **podcast #CyberChats**. #CyberChats es un podcast para fanáticos nuevos y experimentados de la ciberseguridad, de entre 11 y 18 años, que revela lo que los hackers y secuestradores no quieren que sepas. El podcast presenta a profesionales de la ciberseguridad de la industria, el gobierno y la academia, así como a un joven que trabaja en ciberseguridad. Los oyentes aprenden de estos expertos cómo proteger sus datos y celebran historias de éxito en nuestra comunidad de cibernautas.

➜ La NCF organiza educación interactiva móvil a través de su **Cybersecurity Escape Room** en cualquier lugar cercano a Maryland, como en una escuela secundaria o preparatoria, evento de scouts o centro comunitario.

Contacta a Alisha Jordan, Directora de Educación, para programar o hablar de cualquiera de las ofertas del Programa Educativo de la NCF: ajordan@cryptologicfoundation.org.

Esta publicación se presenta con el apoyo agradecido del Capítulo Central de Maryland de la AFCEA. ¡Gracias!

El Capítulo Central de Maryland de la AFCEA (AFCEA-CMD) es una asociación sin fines de lucro dedicada a apoyar a nuestros futuros líderes en STEM (Ciencia, Tecnología, Ingeniería y Matemáticas) mientras construimos relaciones entre el gobierno, el ejército, la industria y la academia. Nos esforzamos por tener un impacto a través de nuestro programa KickStarters (K-12), otorgando más de $5 millones en becas universitarias, proporcionando subvenciones a las escuelas, apoyando a la comunidad local de inteligencia y más.

Publicación de Start Engineering, LLC

CEO: Bob Black
Directora Creativa: Stacie Harrison
VP, Aprendizaje y Comunicaciones: Eric Iversen

Ilustraciones de Huan Tran

Para copias impresas adicionales de esta publicación, contacta a Bob Black en bblack@start-engineering.com o al 202-841-1524.

NUESTRA MISIÓN

La NCF fortalece la confianza en el ecosistema digital para asegurar la democracia y la libertad.

Educamos e involucramos a nuestros ciudadanos para que sean individuos ciberinteligentes y desarrollamos caminos para nuestra futura fuerza laboral en ciberseguridad y criptología.

★ ★ ★

Involucramos y reunimos a socios para abordar cuestiones emergentes en ciberseguridad y criptología.

★ ★ ★

Conmemoramos nuestra historia criptológica y a aquellos que sirvieron.

★ ★ ★

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21061
443-795-4498 ★ www.cryptologicfoundation.org
Dra. Alisha Jordan, Directora de Educación de la NCF ★ ajordan@cryptologicfoundation.org

National Cryptologic Foundation

ncfcyber

@NCFcyber_DirEdi

National Cryptologic Foundation