SEA CIBERNÉTICAMENTE INTELIGENTE

#CyberMonth

MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021

¿Qué es el Mes de Concientización sobre Seguridad Cibernética?

El Mes de Concientización sobre Seguridad Cibernética fomenta la sensibilización sobre la importancia de la seguridad cibernética en toda nuestra Nación.

Seguridad cibernética "¿y qué?"

¿Sabía usted?

Hay software antivirus disponible para los dispositivos móviles, los cuales son un blanco fácil y común para los piratas informáticos y otros malhechores.

Sentido común sobre la seguridad cibernética

- ¡Estar seguro en Internet no es tan diferente de estar seguro en el mundo físico!
- ¡Manténgase tranquilo y confíe de sus instintos!

Términos de uso común

- Malhechor
- Pirata informático
- Ataque cibernético

Ponga de su parte. #BeCyberSmart.

La seguridad cibernética empieza con USTED y es responsabilidad de **todos**.

Actualmente, hay un estimado de 5,200 millones de usuarios de Internet o el 63% de la población mundial.

DELINCUENCIA CIBERNÉTICA

¿Qué es?

La delincuencia cibernética es cualquier delito cometido electrónicamente.

Puede incluir...

- Robo
- Fraude
- A veces hasta asesinato.

Ejemplos

- Robo de Identidad
- Materiales de abuso sexual de niños
- Robo financiero
- Violaciones de derechos de propiedad intelectual
- Programas maliciosos
- Ingeniería social maliciosa

¿Por qué le debe importar a usted?

- ¡La delincuencia es un peligro en la vida real y en Internet!
- Los fundamentos de la autodefensa cibernética pueden ayudar mucho para mantener a usted y sus datos fuera de manos de malhechores.

PROGRAMAS MALICIOSOS

¿Qué es?

Cualquier software destinado para...

- Causar daños
- Deshabilitar
- O dar a alguien un acceso no autorizado a su computadora u otro dispositivo conectado a Internet

¿Por qué le debe importar a usted?

- La mayoría de los delitos cibernéticos empiezan con algún tipo de programa malicioso. Es casi seguro que usted, su familia y su información personal estarán en riesgo si un programa malicioso llegue a instalarse en su computadora o sus dispositivos.

Ejemplos

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Virus
- Gusanos informáticos

RANSOMWARE

¿Qué es?

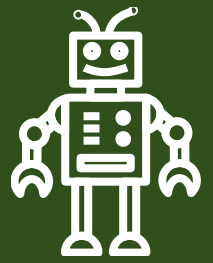
Programas maliciosos diseñados para prevenir el acceso de una víctima a sus datos o sus equipos informáticos hasta que se pague un rescate.

Ejemplos

- Cryptolocker
- Winlock
- Cryptowall
- Reveton
- Bad rabbit
- Crysis
- Wannacry

¿Por qué le debe importar a usted?

- Frecuentemente se descarga de enlaces maliciosos en correos electrónicos
- Causa daños a la estabilidad financiera y la reputación
- No hay ninguna garantía que obtendrá sus datos de nuevo, incluso si paga
- Se suele usar como señuelo para distraer de otras actividades maliciosas



BOTS

¿Qué es?

Los bots son un tipo de programa que se usa para automatizar tareas en Internet.

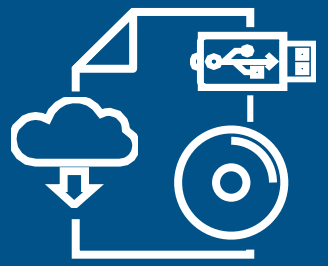
¿Sabía usted?

No todos los bots son malos. Cuando usa un buscador, estos resultados son posibles gracias a la ayuda de los bots que "rastrean" el Internet e indexan el contenido. Chatbots como Siri y Alexa son otro tipo común de bots "buenos".

¿Por qué le debe importar a usted?

Los bots maliciosos pueden:

- Guardar contraseñas
- Registrar pulsaciones en el teclado
- Obtener información financiera
- Apoderarse de cuentas en las redes sociales
- Usar su correo electrónico para enviar spam
- Abrir puertas traseras en el disco infectado



ATAQUES CIBERNÉTICOS FÍSICOS

¿Qué es?

Los ataques cibernéticos físicos utilizan los equipos, dispositivos de almacenamiento externos u otros vectores de ataque para infectar, dañar o comprometer de otra manera los sistemas digitales. Puede incluir...

- Dispositivos de almacenamiento USB
- CD/DVD
- Internet de las cosas (IoT, por sus siglas en inglés)

¿Por qué le debe importar a usted?

- Es fácil ignorarlos
- Es difícil identificar y detectarlos
- Es extremadamente difícil eliminarlos
- Pueden hacer cualquier cosa, tal como instalar ransomware, modificar o enviar copias de sistemas informáticos o desmantelar redes

¿Sabía usted?

Cualquier cosa conectada a Internet podría estar vulnerable, desde los monopatines eléctricos hasta las computadoras portátiles hasta los buques de carga.

INGENIERÍA SOCIAL

¿Qué es?

- Los delincuentes cibernéticos pueden aprovechar de usted con información que se puede obtener fácilmente a través de...
- Plataformas de redes sociales
- Ubicaciones compartidas en redes
- Conversaciones en persona

¿Por qué le debe importar a usted?

- Su privacidad no es solo un lujo – es una medida de seguridad
- Los ataques pueden resultar exitosos con pocos conocimientos o habilidades de programación, o ningunos
- Las medidas de seguridad tecnológicas solo pueden protegerlo hasta cierto punto – usted es su propia mejor defensa

Ejemplos

- Phishing
- Pretextos fraudulentos
- Baiting
- Quid pro quo
- Colarse
- Trabajo interno
- Swatting

PHISHING

¿Qué es?

Mensajes falsos de una fuente que parece fiable o reputada, los cuales son diseñados para convencerle a usted a que...

- Divulgue información
- Permita acceso no autorizado a un sistema
- Haga clic en un enlace
- Comprometerse en una transacción financiera

Ejemplos

- Correos electrónicos
- Mensajes de texto
- Llamadas telefónicas
- Mensajes y publicaciones en redes sociales
- Enlaces sospechosos

¿Por qué le debe importar a usted?

- Extremadamente comunes
- Pueden tener consecuencias graves
- El problema está en los detalles

¿Este correo electrónico engañaría a usted?

Mensaje nuevo

De Legitimate-Looking-Source@notquiteyourworkemail.com

Asunto Actualización informática urgente: vulnerabilidad de software

Actualización de software

Buenas tardes Tom,

Se ha identificado una vulnerabalidad en "Software de Marca Conocida" que permite a un atacante grabar llamadas y videos de la computadora de usted sin su conocimiento. Por favor, instale la actualización adjunta antes del fin del día o su computadora quedará bloqueada.

También hemos creado una aplicación para que todos los empleados puedan determin si han sido afectados por esta vulnerabilidad. Haga clic aquí para ejecutar la aplicación.

Sinceramente,
El Jefe
Departamento Informático de su Compañía

www.fakewebsite.com/gotcha.exe
Haga clic para seguir el enlace

RESPONDER

SWATTING

¿Qué es?

Un ataque centrado en ubicaciones compartidas en redes en el cual los malhechores llaman a la policía y afirman que la víctima ha cometido un delito...

- Amenazas con bombas
- Intruso armado
- Incidente violento

¿Por qué le debe importar a usted?

- Consecuencias físicas e inmediatas
- A veces se hace como una forma de broma pesada
- Puede resultar en arresto y lesiones graves
- Reducir el riesgo al compartir su ubicación solamente con individuos de confianza, y comparta las fotos de sus vacaciones solamente después de estar seguro en casa de nuevo

Ejemplos

Su ubicación se incorpora como metadatos en cada foto que toma con su teléfono. Desactive los servicios de ubicación cuando no los está usando para que sea más difícil para los malhechores ver esta información.

OTRAS MANERAS DE ATACAR

¿Qué es?

- Internet de las cosas
- Cualquier dispositivo conectado a su red
- Recolección de información
- Acceso a distancia
- Bluetooth
- Puertos abiertos

Ejemplos

- Dispositivos inteligentes
- Teléfono móvil
- Termostato
- Vehículos
- Consolas de juegos
- Impresoras
- Equipo médico
- Sistemas industriales

¿Por qué le debe importar a usted?

- Se puede usar la red de usted para atacar a otros
- Cualquier dispositivo que guarda información o que está conectado al Internet puede ser una vulnerabilidad
- Debe presumir que usted está vulnerable, y tomar medidas para entender y mitigar el riesgo
- No sea el blanco fácil

¿Cómo puede protegerse de mejora manera en Internet?

Asegurar sus redes.

Para los delincuentes cibernéticos, los enrutadores inalámbricos son una manera de acceder a dispositivos conectados.

Si lo conecta, protéjalo.

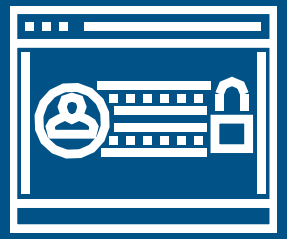
Una defensa comprobada contra intrusiones es actualizar a la última versión de software antivirus.

Manténgase al día.

Mantenga el software actualizado a su última versión y configure un software de seguridad para realizar análisis regulares.

Duplique la protección de sus credenciales.

Habilite la autenticación por múltiples factores (MFA, por sus siglas en inglés) para asegurar que la única persona con acceso a sus cuentas sea usted mismo.



Consejos para contraseñas

¿Sabía usted?

El relleno de contraseñas o credenciales es un ataque cibernético que trata de "rellenar" los usuarios y contraseñas comprometidos de un sitio en otro sitio con la esperanza de que el usuario utilice los mismos credenciales en diferentes plataformas.

- ****** Use contraseñas distintas en sistemas y cuentas diferentes
- ****** Use la contraseña más larga que se permite
- ****** Use una mezcla de letras mayúsculas y minúsculas, números y símbolos
- ****** Cambie su contraseña cada cuantos meses
- ****** Use un administrador de contraseñas

Tema del Mes de Concientización sobre Seguridad Cibernética

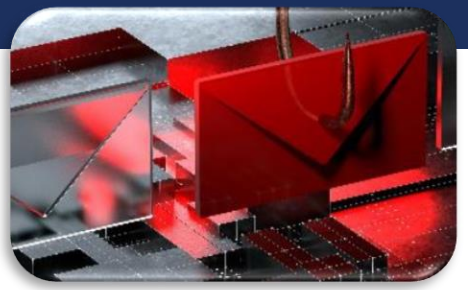
Tema:

- Ponga de su parte. #BeCyberSmart.

Calendario del Mes de Concientización sobre Seguridad Cibernética de 2021

1 de octubre:
Lanzamiento oficial

SEMANA 1:
Semana del 4 de octubre:
Sea cibernéticamente inteligente.

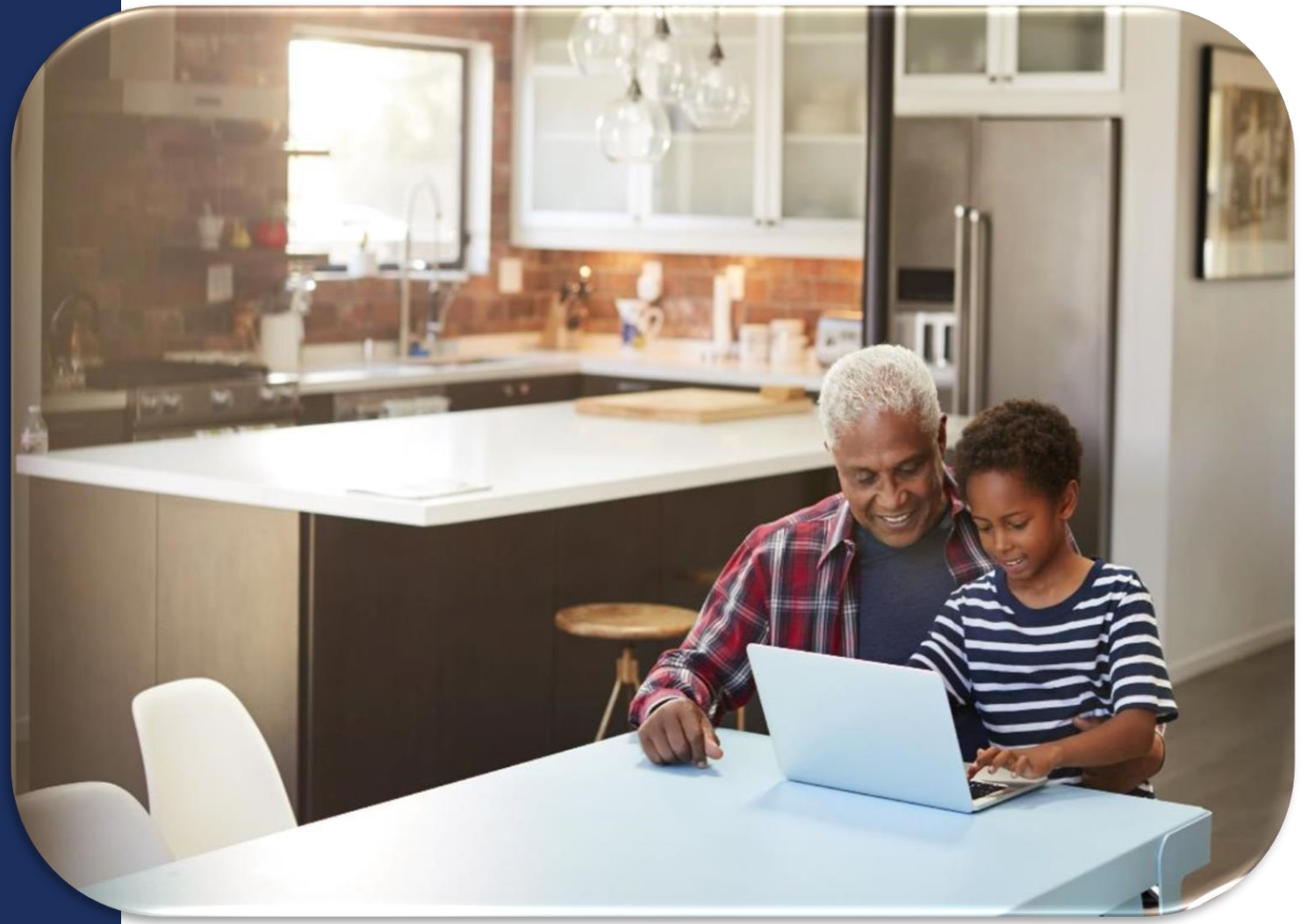


SEMANA 2:
Semana del 11 de octubre
¡Luche contra el phishing!

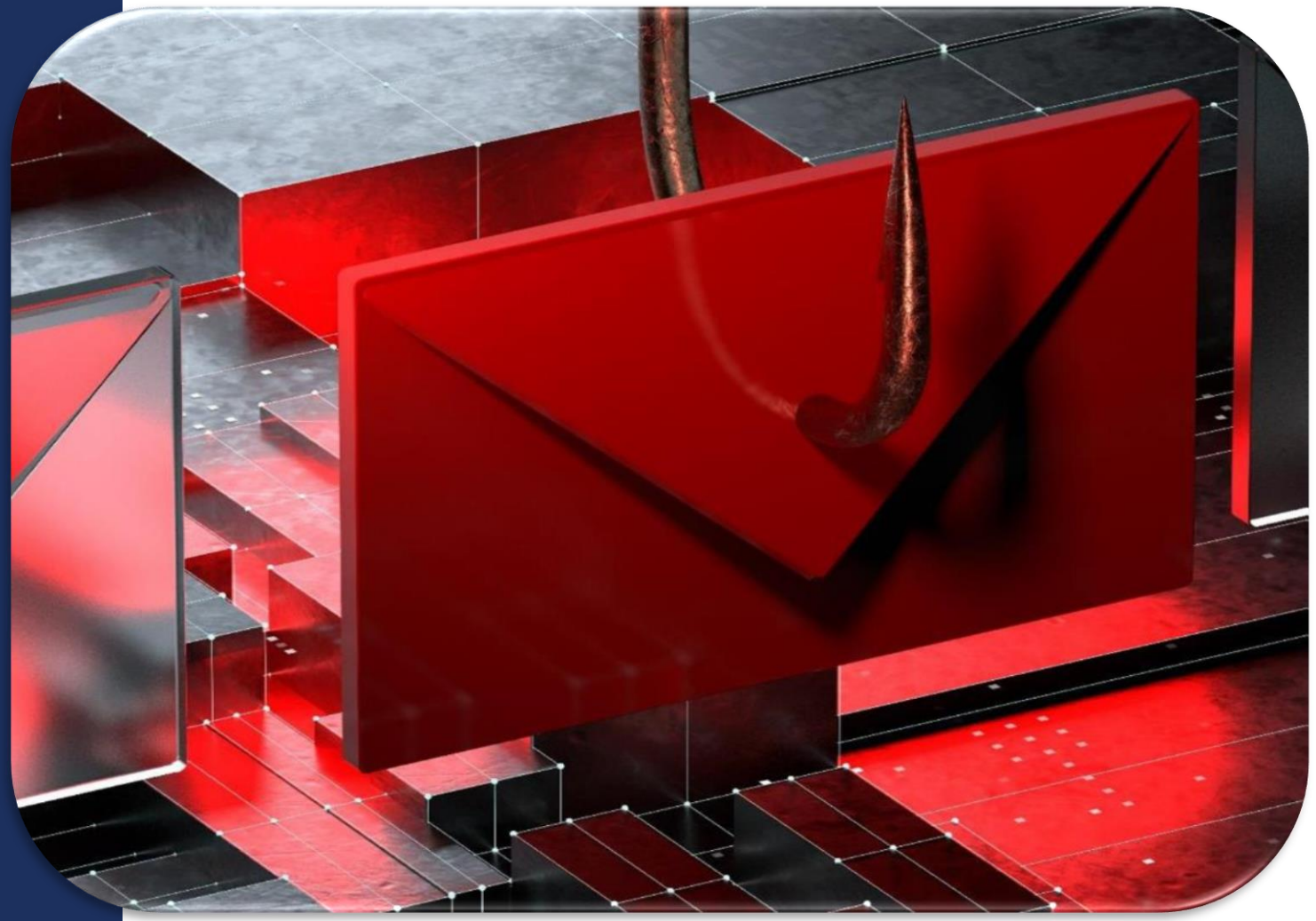
SEMANA 3:
Semana del 18 de octubre
Explore. Experimente. Comparta. (Semana de Concientización sobre Carreras de Seguridad Cibernética)

SEMANA 4:
Semana del 25 de octubre:
La seguridad cibernética primero

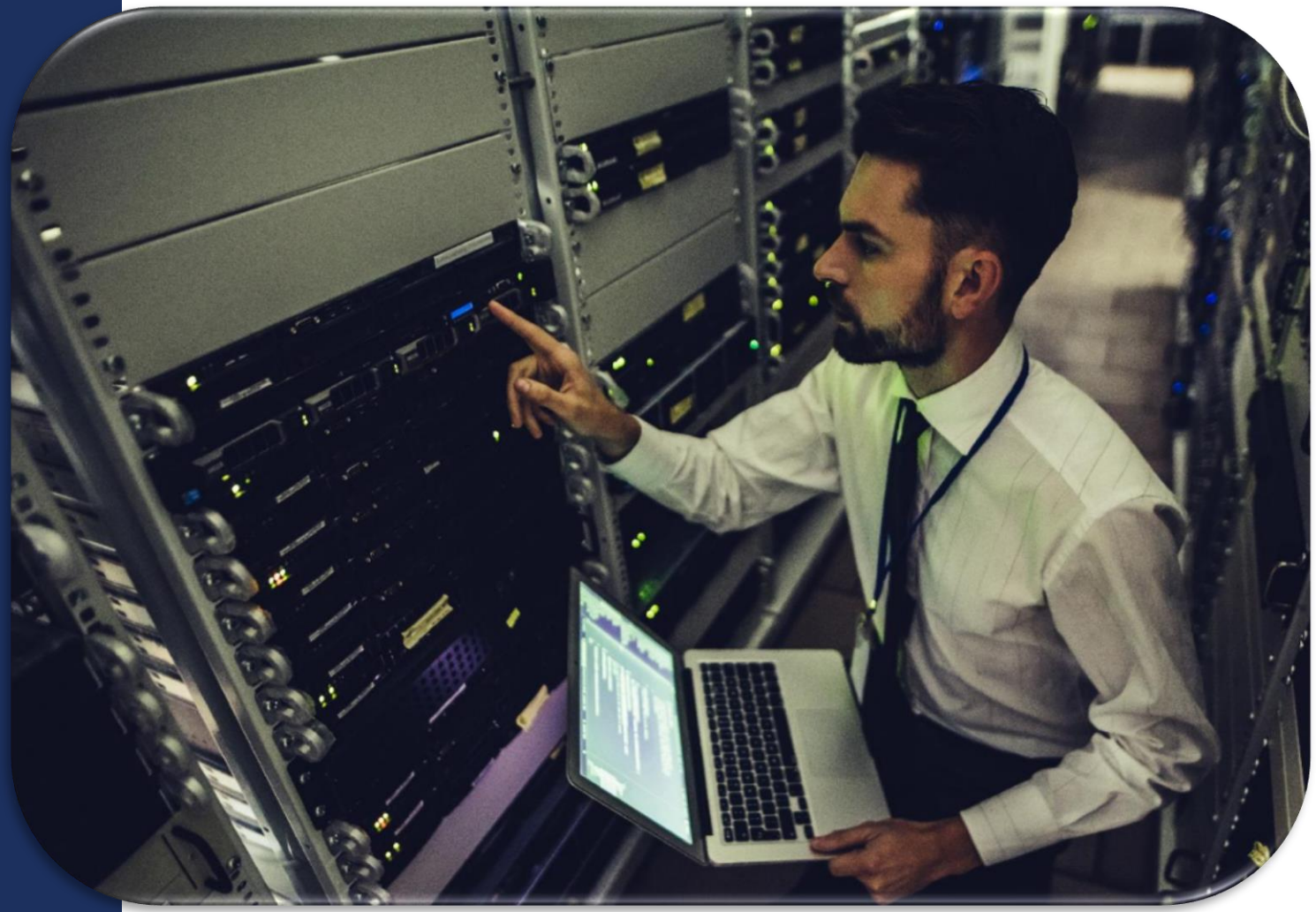
Semana 1:
Sea cibernéticamente inteligente.



Semana 2:
¡Luche contra el phishing!



Semana 3:
Explore.
Experimente.
Comparta.
Semana de Concientización sobre Carreras de Seguridad Cibernética



Semana 4:
La seguridad cibernética primero.

Fomente la sensibilización e involúcrese

- Sea un Campeón del Mes de Seguridad Cibernética
- **Promocione el Mes de Concientización sobre Seguridad Cibernética en las redes sociales; use la etiqueta #BeCyberSmart.**
- Ofrézcase como voluntario para hablar en Eventos del Mes de Concientización sobre Seguridad Cibernética
- Difunda los consejos de seguridad cibernética a sus amigos, su familia y sus compañeros

Para más información, comuníquese con CyberAwareness@cisa.dhs.gov

Visite cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/ para más recursos.