GUÍA

Planificación de su calendario de concientización y capacitación en ciberseguridad

Dado que el panorama de las amenazas está cambiando rápidamente y se está volviendo más malicioso, los programas de concientización sobre la seguridad deben evolucionar y garantizar que se mantienen al día con las amenazas actuales. La creación de un ciclo de aprendizaje continuo ayuda a integrar una cultura de concientización cibernética dentro de una organización y garantiza que todo el mundo desempeñe un papel en la protección contra las amenazas.

Por qué es importante el aprendizaje continuo

Es importante que la capacitación sea continua y oportuna. El psicólogo alemán Hermann Ebbinghaus fue pionero en los estudios experimentales sobre la memoria a finales del siglo XIX, que culminaron con su descubrimiento de "La curva del olvido". Descubrió que, si no se aplica la nueva información, olvidaremos el 75 % de ella después de solo seis días.[1]

Aunque crear un gran módulo de capacitación que marque las casillas de los mandatos de cumplimiento de la capacitación y entregarlo a los empleados una vez al año puede ser atractivo, el desafío resultante es que la concientización sobre la seguridad no estará a la vanguardia de las operaciones diarias.

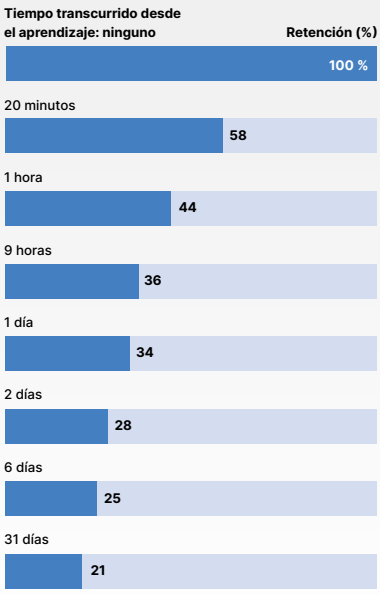
Construir una cultura que recompense los comportamientos positivos que una organización desea ver no tiene por qué ser complejo y difícil de implementar. Un poco de planificación y creatividad por adelantado, con algunas revisiones durante el año, puede ayudar a garantizar que se logre la concientización sobre la ciberseguridad de la organización durante todo el año.

Este documento pretende ser un generador de ideas para ayudarlo a elaborar su calendario programado de concientización y capacitación en ciberseguridad.

Este paso, la elaboración del calendario, se hace después de definir los objetivos y la estrategia del programa. Para obtener ayuda con el primer paso, consulte Guía para definir los objetivos y planificar su programa de concientización y capacitación en ciberseguridad.

La curva del olvido

Si no se aplica la nueva información, olvidaremos el 75 % de ella después de solo seis días.



Fuente: Hermann Ebbinghaus

Concientización y capacitación en ciberseguridad alineada a la incorporación de los empleados

Cuando un nuevo empleado se incorpora a su organización es importante que la concientización y capacitación en ciberseguridad se incluya en ese proceso de incorporación.

Presentarles a los nuevos empleados lo esencial de un buen comportamiento con respecto a la seguridad desde el primer día ayuda a comunicar a los nuevos contratados que la organización valora la seguridad y la protección de sus datos, redes y usuarios.

Comience con un módulo de capacitación introductoria que enseñe a los estudiantes a describir el concepto de concientización y capacitación en seguridad de la información, y que enumere las acciones que pueden tomar para proteger la información personal y de la empresa.

A partir de ahí, elija módulos adicionales específicos que aborden las áreas clave que son importantes para su organización. Por ejemplo, si sabe que la suplantación de identidad es una preocupación particular para su organización, entonces también deberá seleccionar los módulos de suplantación de identidad, ingeniería social y seguridad de correo electrónico. Estos módulos pueden incluirse en el módulo de introducción u ofrecerse durante un período de incorporación definido.

A continuación, puede poner a prueba a sus usuarios con ejercicios de simulación de suplantación de identidad. A partir de ahí, los usuarios que sean víctimas de la suplantación de identidad simulada pueden redirigirse a micromódulos adicionales para que se les recuerden las enseñanzas clave.

Ejemplo de incorporación

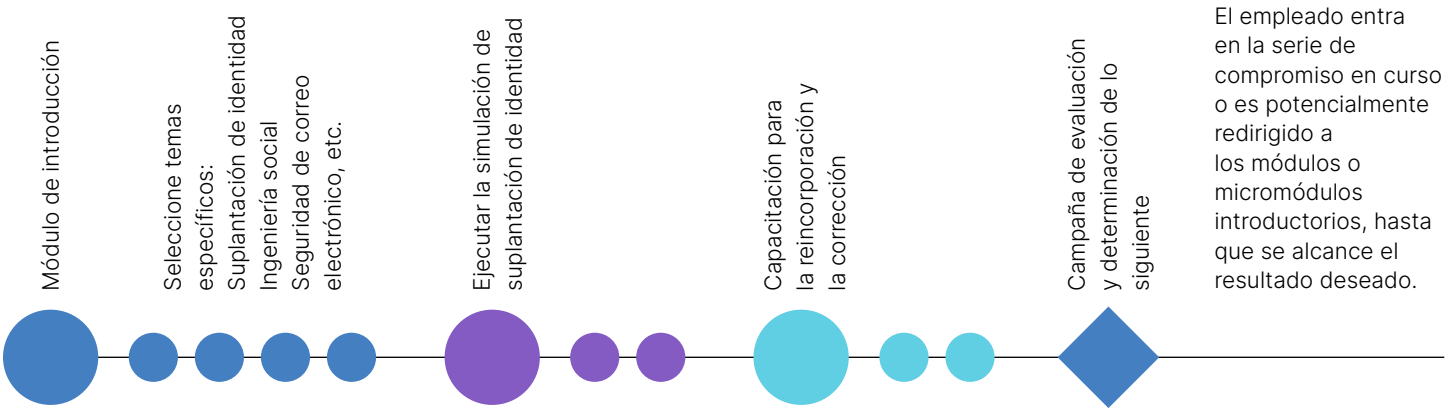


Figura 1: El tiempo entre los módulos de capacitación puede durar días o semanas, dependiendo de su proceso de incorporación.

Construya una cultura de seguridad con un compromiso continuo

A lo largo del año, es una buena práctica darles seguimiento a los empleados y ofrecerles oportunidades de aprendizaje rápido que lo ayuden a fomentar una cultura de concientización sobre la seguridad. El envío de nuevos contenidos cada mes puede ayudar a mantener a los empleados interesados y comprometidos. Es importante que la capacitación esté adecuadamente dirigida a la función correcta y que sea fácil de digerir, comprender y aplicar. No abrume a sus empleados con grandes bloques de capacitación en una sola sesión.

A continuación, se presenta un ejemplo de campaña que puede desglosarse en un tema, o una colección de temas, para hacer un tema cada mes. También se pueden incluir los correspondientes simulacros de suplantación de identidad, simulacros de tailgating, controles puntuales de escritorio limpio y otros tipos de pruebas, combinados con la distribución de recursos de comunicación que ayuden a reforzar las enseñanzas clave.

El siguiente ejemplo tiene lugar durante un periodo de tres meses; sin embargo, la idea es que los diferentes temas continúen a lo largo del año. Esta es una instantánea de tres meses de un programa de un año de duración. Si una frecuencia mensual es demasiado para su organización, considere la posibilidad de construir el mismo modelo, pero espaciándolo trimestralmente, en lugar de mensualmente.

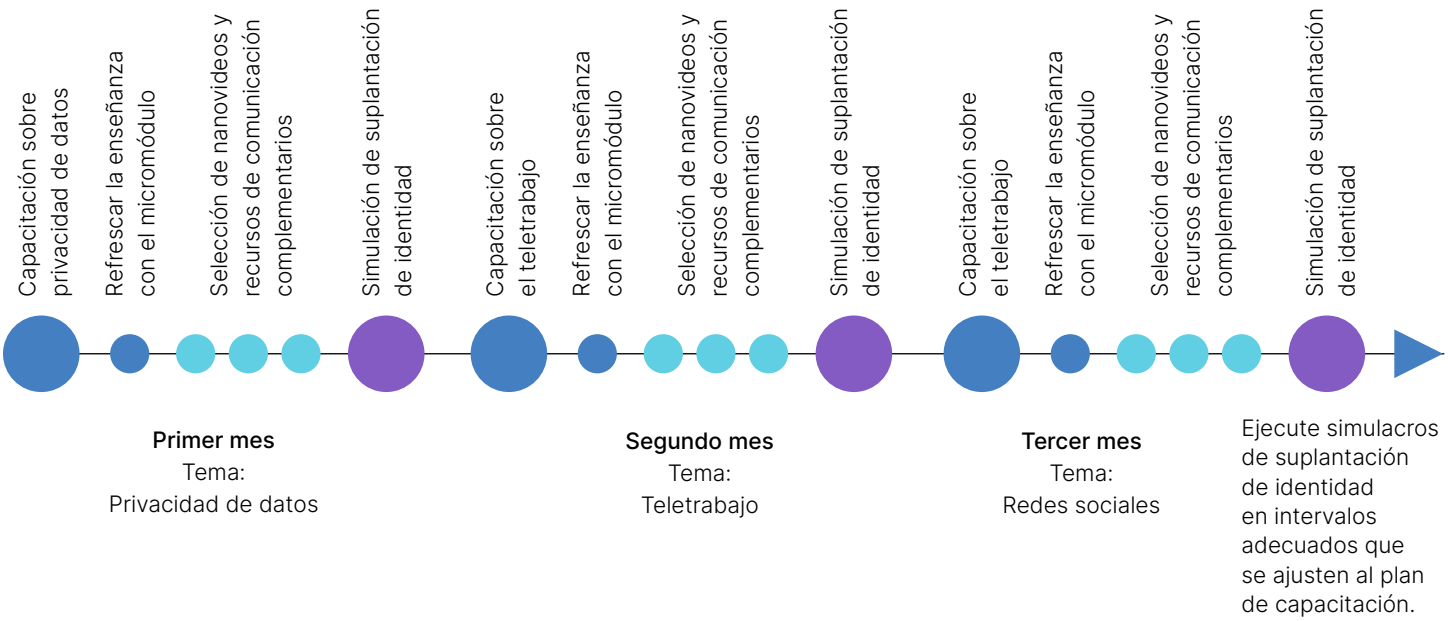


Figura 2: Instantánea de tres meses de un programa de un año de duración.

Tematizar la concientización y la capacitación sobre diferentes eventos y festividades mundiales y regionales

Conectar la capacitación y la concientización con los temas de la industria o los días festivos es una gran manera de reforzar las enseñanzas clave. Sus empleados también pueden leer sobre estos temas en otras publicaciones o en las redes sociales, lo que ayuda a reforzar la importancia de la ciberseguridad.

A continuación, se indican algunos días festivos clave o celebraciones señaladas en torno a los cuales se puede crear una campaña:

Octubre es el mes de la concientización sobre la ciberseguridad

El mes de la concientización sobre la ciberseguridad es una campaña reconocida internacionalmente que se celebra cada octubre para ayudar al público a conocer mejor la importancia de la ciberseguridad.

El Instituto Nacional de Estándares y Tecnología ofrece algunos consejos útiles, temas y recursos que puede utilizar durante este mes.

El Black Friday y la temporada navideña

El Black Friday y el Cyber Monday dan el comienzo a la temporada de compras navideñas en EE. UU. De hecho, el 30 % de todas las ventas minoristas se producen entre el Black Friday y el día de Navidad. Desde la llegada del Cyber Monday, tanto las tiendas físicas como las de comercio electrónico generan una parte importante de sus ingresos anuales durante este fin de semana de compras.

FortiGuard Labs observa cada vez más estafas relacionadas con sitios web falsificados que parecen ser sitios legítimos de comercio electrónico. Estos sitios pueden parecer seguros, pero si no está prestando atención, pueden robar su pago (y posiblemente la información de pago) a través de una compra que creía legítima. Los sitios de comercio electrónico falsos se están convirtiendo rápidamente en la última amenaza para los consumidores, y abarcan una amplia gama de productos para atraer a posibles compradores.

Lleve a cabo campañas antes de estas fechas para educar a sus empleados sobre esta amenaza y sobre cómo pueden ser fácilmente presa de estos sitios. Lea más en el Fortinet blog.

Día de la privacidad de datos/día de la protección de datos

El día de la privacidad de los datos, o el día de la protección de datos, como se conoce en Europa, se celebra el 28 de enero de cada año. El objetivo de este día es aumentar la concientización y promover las mejores prácticas de privacidad y protección de datos.

Este es un buen momento para centrar su capacitación en la seguridad y la privacidad de los datos. Si busca más recursos sobre este tema, muchas regiones y gobiernos tienen campañas específicas en el país que las organizaciones pueden aprovechar.

Temporada de impuestos

Los cibercriminales andan sueltos, deseosos de aprovecharse del estrés y la incertidumbre que rodean a la temporada de impuestos. Los ataques pueden adoptar la forma de campañas de correo electrónico de suplantación de identidad o incluso de llamadas telefónicas de personas que afirman ser del IRS o de una agencia de cobros. Los datos robados también pueden dotar a estos estafadores de información personal, incluidos los números del Seguro Social, lo que les hace parecer legítimos incluso cuando no lo son.

Además de las campañas de phishing implementadas a través de un modelo de "regar y esperar" que envía miles de correos electrónicos con la esperanza de que al menos una persona sea víctima, también están aumentando los ataques de suplantación de identidad dirigida.

En vísperas de la temporada de impuestos, haga campañas para asegurarse de que sus empleados no se distraigan y caigan en un ataque de suplantación de identidad dirigida más sofisticado. Los ataques de suplantación de identidad dirigida pueden ser más difíciles de detectar que los de suplantación de identidad, ya que se presentan en forma de correos electrónicos personalizados y dirigidos que a menudo parecen enviados por alguien que conoce al destinatario.

Otros:

- Votación
- Vacaciones
- Emergencias de salud pública como COVID-19 o vacunas
- Estados de emergencia como inundaciones, incendios forestales, etc.

Simulación de suplantación de identidad

La simulación de suplantación de identidad es una herramienta importante para reforzar la concientización y capacitación en ciberseguridad centrada en las amenazas basadas en el correo electrónico, como la suplantación de identidad, la suplantación de identidad dirigida, el compromiso del correo electrónico empresarial y los ataques de ransomware mediante el correo electrónico.

La simulación de suplantación de identidad debe ser una actividad continua (al menos bimensual) para toda su base de empleados y usuarios, aunque los temas y la frecuencia pueden variar. Además, la simulación o prueba de suplantación de identidad debe incorporar capacitación y contenidos de aprendizaje que se activen al hacer clic en un correo electrónico de prueba.

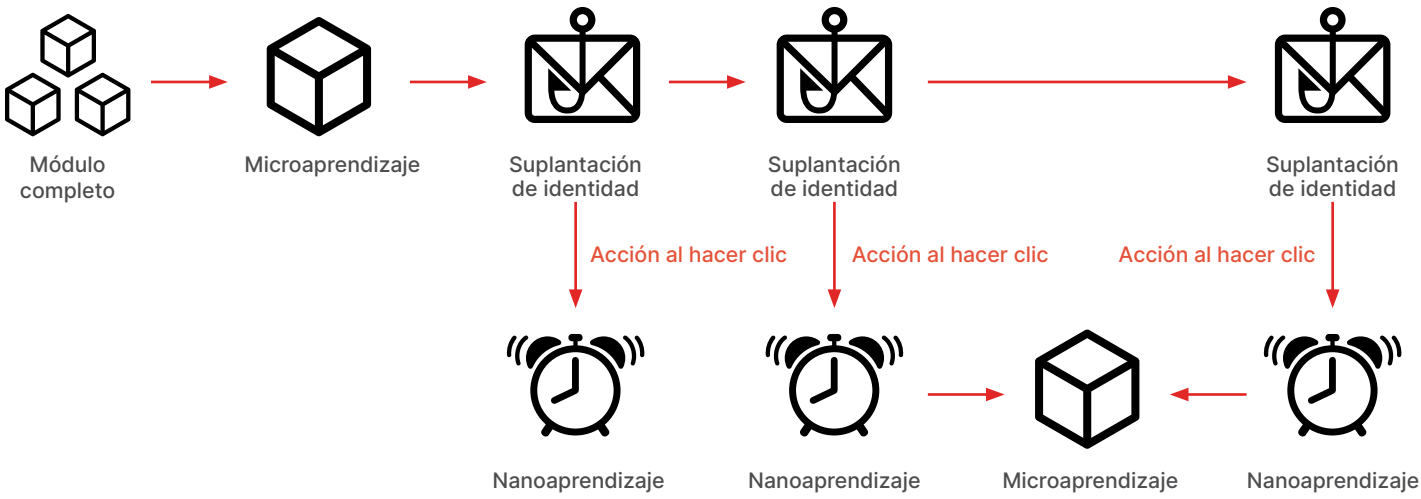


Figura 3: Construcción de una "campaña" de suplantación de identidad.

Al establecer un programa de simulación de suplantación de identidad, su enfoque no debe consistir necesariamente en poner a prueba a todos los empleados con los mismos correos electrónicos de suplantación de identidad. Deberá adoptar un enfoque más reflexivo que tenga en cuenta algunos puntos de vista, como, por ejemplo:

- ¿Hay grupos o departamentos de empleados o usuarios que deban someterse a pruebas con menor/mayor frecuencia o sobre temas o tácticas diferentes?
- ¿Qué tácticas son las más importantes para probar y reforzar la vigilancia? Por ejemplo, si su organización recibe correos electrónicos supuestamente del CEO en los que se les pide que actúen, debería poner a prueba a sus empleados y usuarios con correos electrónicos de prueba similares.
- Asegúrese de hacer pruebas que incorporen enlaces sospechosos simulados y archivos adjuntos juntos y por separado.
- Considere los temas de suplantación de identidad que se relacionan con actividades que aparentemente solo conocen los empleados, como anuncios de cambios en la nómina o en los recursos humanos, restablecimiento de contraseñas, avisos de cortes de capacitación, boletines internos, etc. Los atacantes astutos crearán mensajes de correo electrónico que intenten emular estas comunicaciones internas, por lo que también es bueno poner a prueba a sus empleados y usuarios.
- Considere la posibilidad de crear una campaña de educación y pruebas de suplantación de identidad especializada para las personas que hacen clic repetidamente o los empleados que hacen clic constantemente en los correos electrónicos de prueba de suplantación de identidad.

Cuando sus campañas de pruebas de suplantación de identidad finalicen, asegúrese de revisar el rendimiento y otras métricas para determinar cómo le va a su organización. Su análisis debe tomar varios puntos de vista, como el rendimiento de sus campañas, el rendimiento de los grupos individuales en las campañas, las tácticas que los empleados y los usuarios parecen tener problemas para identificar con éxito, y los individuos que hacen clic en serie en las pruebas y requieren capacitación y refuerzo adicionales.

No se olvide de la formación de corrección

Haga que la capacitación de corrección sea positiva, no punitiva.

Como parte de un ciclo de vida de capacitación y concientización continua, se puede hacer un seguimiento de los empleados para determinar si lo que se les está enseñando está ayudando y está cambiando los comportamientos. Los seguimientos pueden indicarse mediante varias acciones:

- Bajo rendimiento en las pruebas y evaluaciones
- Hacer clic accidentalmente en correos electrónicos de simulación de suplantación de identidad
- Violación de datos o de la privacidad
- Rendimiento deficiente en otros tipos de pruebas, como los controles de escritorio al azar, los simulacros de tailgating, etc.

Si los empleados tienen un mal rendimiento en alguno de estos puntos, los microvideos o nanovideos son excelentes activos para enviar recordatorios específicos de lo que debe hacerse en cada escenario aplicable. Es importante que la capacitación de corrección no se presente como una lección, que puede percibirse como una forma negativa de refuerzo. En su lugar, la capacitación de corrección debe apoyar y elevar la moral, para crear un compromiso con los empleados. El objetivo es reeducar y reforzar las enseñanzas clave, no administrar un castigo.

"Incluso en medio de las limitaciones de tiempo vinculantes, busque oportunidades para volver a visitar, revisar y replantear".[2]

Sobre el nuevo servicio de capacitación y concientización en ciberseguridad de Fortinet

El servicio de capacitación y concientización en ciberseguridad de Fortinet aporta una concientización oportuna y actual sobre las amenazas de ciberseguridad de hoy en día y ayuda a que los empleados de una organización sean ciberconscientes y puedan reconocer y ayudar a detener los ataques. Creado especialmente para satisfacer las necesidades de las PYMES y las empresas, el servicio proporciona una oferta llave en mano que incluye una interfaz de administrador intuitiva para la creación de campañas, el monitoreo y la elaboración de informes, módulos de aprendizaje para el usuario final, micromódulos o nanomódulos de refuerzo y recursos de concientización.

Más información

[1] Steve Glaveski, Where Companies Go Wrong with Learning and Development, Harvard Business Review, 2 de octubre de 2019.

[2] Robert F. Bruner, Repetition is the First Principle of All Learning, ResearchGate, agosto de 2001.

julio 29, 2022

1376807-0-0-ES