Ciberseguridad

Kit de herramientas
para la Campaña de Concientización

Organización de los Estados Americanos | Más derechos para más gente

La Organización de los Estados Americanos (OEA) es el principal foro político de la región que promueve y apoya la Democracia, los Derechos Humanos, la Seguridad Multidimensional y el Desarrollo Integral en las Américas. La OEA busca prevenir conflictos y brindar estabilidad política, inclusión social y prosperidad en la región a través del diálogo y acciones colectivas como por ejemplo la cooperación, la implementación de mecanismos de seguimiento a los compromisos de los Estados Miembros y la aplicación de las normas del Sistema Interamericano y el Derecho Internacional.

Esta herramienta fue posible gracias al apoyo financiero de los gobiernos de Canadá y de los Estados Unidos.

Aviso Importante
Los contenidos de esta publicación no reflejan necesariamente los puntos de vista de la OEA o de alguna de las organizaciones contribuyentes.

Octubre 2015
© Secretaría de Seguridad Multidimensional de la OEA
1889 F Street, N.W., Washington, D.C., 20006
United States of America
www.oas.org/cyber/

Ciberseguridad

Kit de herramientas
para la Campaña de Concientización

Organización de los Estados Americanos | Más derechos para más gente

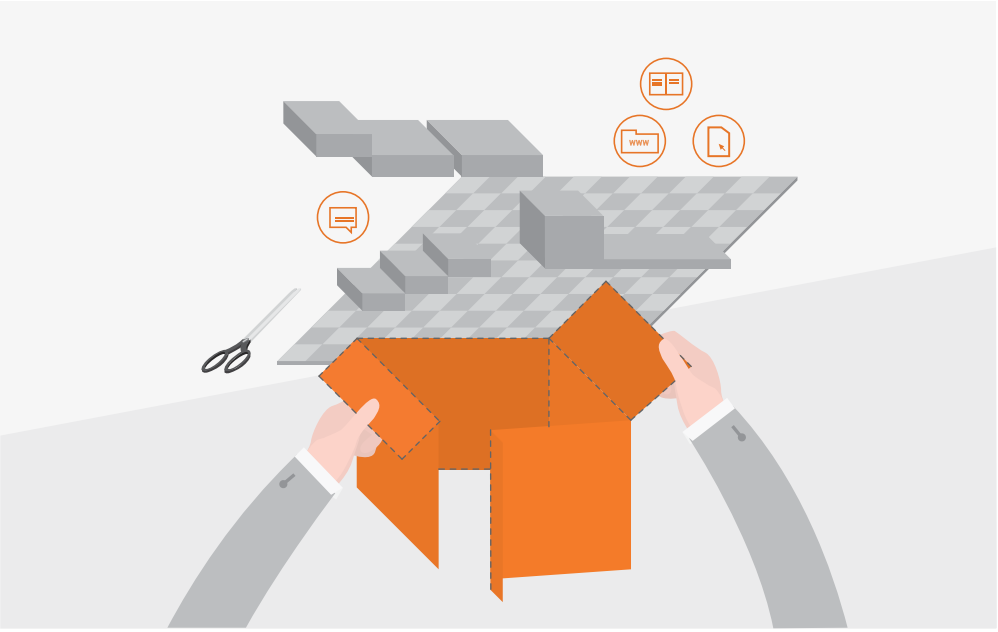
Tabla de contenidos

Apéndice

Introducción

Este kit de herramientas está diseñado para proporcionarles, a los gobiernos o a las organizaciones, orientación y recursos para el desarrollo de una campaña de concienciación en materia de seguridad cibernética.

Nuestro objetivo es ayudarlo a realizar una campaña de concientización sobre la seguridad cibernética según las necesidades de su país y brindar orientación sobre cómo ejecutarla de la mejor manera, ya sea que usted tenga un presupuesto amplio o recursos limitados. Queremos ayudarlo a construir una campaña que sea sostenible por un largo período, que eduque a sus ciudadanos y que ayude a construir una cultura nacional de seguridad cibernética.



Antecedentes

Vivimos en un mundo conectado digitalmente. El gobierno electrónico, comercio electrónico, la comunicación, banca en línea, y los servicios de salud en línea son parte de la vida cotidiana. La información sensible, redes digitales y las infraestructuras críticas son susceptibles a las amenazas cibernéticas, desde ataques patrocinados por el estado a crimen organizado a delincuencia cibernética menor. Todos, desde los más altos funcionarios del gobierno, empresarios, el público en general y niños y niñas, son vulnerables a las amenazas de seguridad cibernética. Prevenir el delito cibernético no es la responsabilidad de una sola persona o entidad sino una responsabilidad compartida. Los gobiernos, empresas y particulares tienen un papel que desempeñar en la protección del mundo digital. El gobierno debe proteger la infraestructura crítica y la información confidencial, proporcionar portales de gobierno electrónico seguros y proteger numerosas redes sensibles. Las empresas deben proteger la propiedad intelectual, la información financiera, las redes y la información personal del cliente y de los empleados. Los particulares necesitan proteger sus finanzas personales y otra información, a la vez de proteger la seguridad de sus hijos en el Internet. Debido a la naturaleza interconectada del Internet, un eslabón débil o una falla en cualquiera de estos sistemas pueden afectar a otros. Una vulneración de datos en una empresa puede tener efectos de largo alcance. Puede causar estragos en las finanzas personales de los particulares y también erosionar la seguridad económica nacional del país en el que ocurre. Una pieza de malware descargada involuntariamente al dispositivo de un particular podría lograr llegar a una red gubernamental o corporativa si no están implementadas buenas políticas para el uso de dispositivos personales en el lugar de trabajo.

El Internet llega a casi todo el mundo en muchos aspectos de la vida. El público puede considerarse prácticamente todo el mundo: niños y niñas, familias, educadores, negocios, el gobierno y el público en general. Incluso si alguien no está en línea, la seguridad cibernética lo afecta porque en algún lugar, otro, ya sea una empresa, gobierno o alguien en su círculo social, tiene información personal sobre ellos en una computadora que está conectada al Internet. Esto dirige la atención a los delitos cibernéticos. Una amplia

gama de diferentes comportamientos y técnicas constituyen los delitos cibernéticos, que incluyen el robo de identidad, explotación infantil, acoso cibernético, amenazas internas, suplantación de identidad (phishing), suplantación de identidad dirigida a un objetivo (spear phishing) y muchos, muchos otros, que se deben abordar. Por lo tanto, aunque el público para una campaña de sensibilización es de un tamaño casi inconmensurablemente, usted debe tener en cuenta el hecho de que el mensaje debe ser elaborado en función del sector específico del público al que busca llegar. Por ejemplo, un mensaje dirigido a un director general no será el mismo mensaje dirigido a un niño o maestro. Deberá enfocarse en los temas particulares a los que se enfrenta el país.

El mensaje debe atraer la atención, ser frecuente y unificado.

Educar a la gente acerca de la seguridad cibernética es de suma importancia para la creación de una cultura de seguridad cibernética. La conciencia es el primer paso hacia el desarrollo de una ciudadanía con inteligencia cibernética. La sensibilización sobre la seguridad cibernética y la capacidad de afectar el comportamiento no es una tarea sencilla. El mercado para campañas de sensibilización ya se encuentra cargado y la gente tiene un ancho de banda limitado. El mensaje debe atraer la atención, ser frecuente y unificado para abrirse camino por el constante bombardeo de anuncios, el ciclo de noticias de 24 horas y el flujo continuo de los medios sociales. El mensaje debe ser convincente y memorable. No se trata de vender aparatos; se trata más bien de influir en el comportamiento. Usted debe apelar a los corazones y las mentes de su público a través de mensajes que los animen a apropiarse de su propia seguridad cibernética y de esa manera, convertirse en un aliado en la lucha contra la delincuencia cibernética.

Instrucciones

Dentro de este kit de herramientas se encuentra una guía de planificación que explica los pasos para realizar una campaña de sensibilización de seguridad cibernética, planes de comunicación, ejemplos de mensajes, numerosos recursos en línea, ejemplos de investigación, orientación en medios sociales y ejemplos de métricas. Con la guía de planificación de campaña de sensibilización de seguridad cibernética buscamos ayudarlo a identificar sus metas y construir una estrategia para ejecutar una campaña de sensibilización. Junto con la guía de planificación usted encontrará ideas, información y recursos para ayudarlo a implementar su campaña. Muchos de los recursos que se incluyen son gratis o de bajo costo. Las ideas y las estrategias que se incluyen también tienen el propósito de ayudarlo a hacer el mejor uso de los recursos que tiene.

Lea todo el material. Hay una gran cantidad de información a su disposición. Después de la lectura del material y de hacer su investigación, identifique su grupo de interés (hay más información sobre esto en la página 11) y comience a seguir los pasos. Convoque a una reunión con su grupo de interés para discutir la campaña. Esta reunión probablemente durará casi un día, o más. Tome el tiempo suficiente para que todos tengan la oportunidad de expresar su opinión.

Después de la reunión, usted deberá contar con una lista de puntos de acción. Esperemos que esta lista lo guíe en la construcción de su campaña, ya sea hacer más investigación o comenzar a armar una estrategia de ejecución de su campaña.

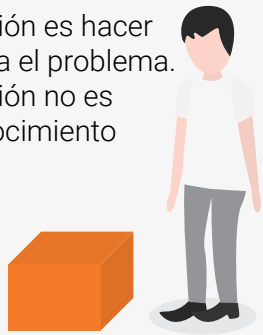
Este kit de herramientas tiene como objetivo proporcionar la orientación necesaria para construir una campaña estratégica de sensibilización de seguridad cibernética. Este es un tema complicado sin respuestas fáciles, pero hay un camino a seguir. Al ser estratégica, mediante la comprensión de su público, la presentación a ellos de un mensaje que les llegue y los ponga en acción y el compromiso de una campaña a largo plazo, usted podrá lograr un cambio y el desarrollo de una cultura de seguridad cibernética.

El proceso de la sensibilización y la educación

A medida que usted comience a pensar en sus objetivos para una campaña de sensibilización y cómo educar a su público, es importante distinguir entre sensibilización y educación. No son la misma cosa. El proceso de sensibilización puede conducir a la educación y, finalmente, a un cambio de comportamiento. El siguiente diagrama muestra este proceso:

1
SENSIBILIZACIÓN

La sensibilización es hacer que se conozca el problema. La sensibilización no es igual a un conocimiento profundo.



2
EDUCACIÓN

La educación es la presentación de la información específica que el público necesita saber.

3
CONOCIMIENTO

El conocimiento se logra cuando se ha retenido el material educativo.

6
HÁBITO

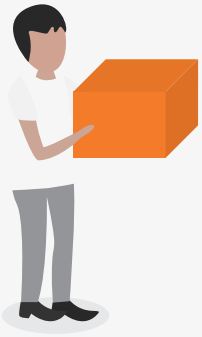
El hábito se produce cuando las habilidades y conocimientos se ponen en práctica y se arraigan en la rutina diaria.

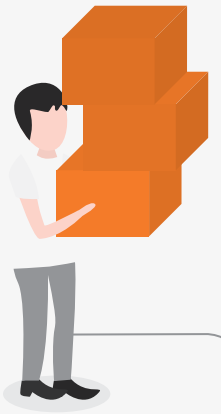
A medida que su público adquiere habilidades y capacidades, el mensaje y la información necesitarán evolucionar para continuar la sensibilización y el conocimiento de los diversos aspectos de la seguridad cibernética.

Un cambio social de esta naturaleza lleva mucho tiempo, en algunos casos puede tomar una generación o más, para integrarse completamente como una norma social, por lo tanto, se deben establecer objetivos realistas dentro de los plazos establecidos.

4
HABILIDADES

Las habilidades se construyen sobre el conocimiento adquirido. Las habilidades requieren práctica y se desarrollan con el tiempo.



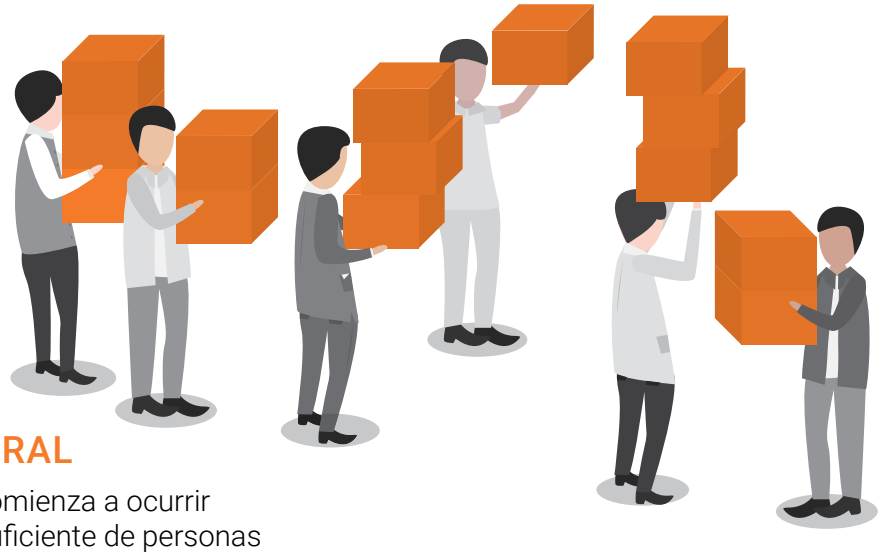


5
CAPACIDAD

La capacidad es poder llevar a cabo las habilidades necesarias para la destreza.

Los primeros cinco pasos del proceso pueden ocurrir casi simultáneamente o puede que tomen un tiempo más largo, dependiendo del éxito del mensaje, receptividad del público y el nivel actual de conocimiento.

La constante repetición del mensaje nos lleva a la sexta etapa, en la que los hábitos diarios se arraigan hasta el punto de volverse natural. Una vez que esto sucede, comenzará a producirse un cambio cultural en la que la seguridad cibernética se vuelve una práctica diaria de las personas, empresas y el gobierno.

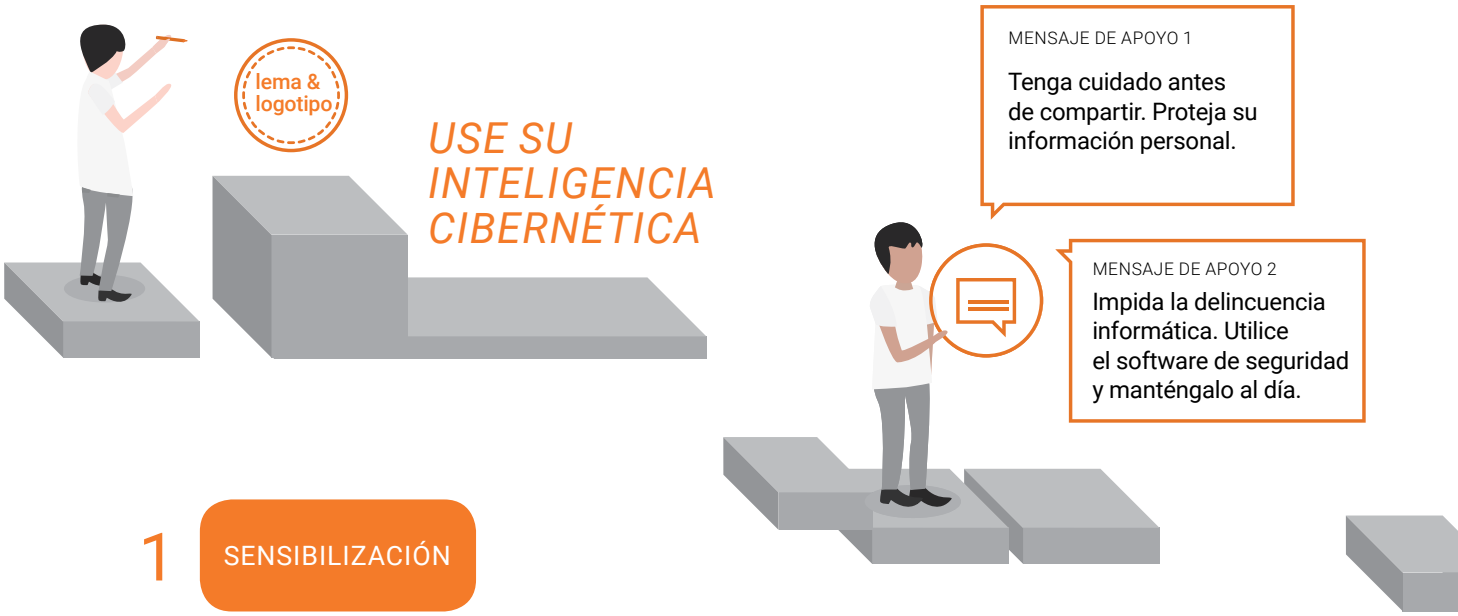


7
CAMBIO CULTURAL

Un cambio cultural comienza a ocurrir cuando un número suficiente de personas han incorporado los buenos hábitos.

Estructura de la campaña

Para asegurarse de que se logre la sensibilización y la educación, es necesaria una campaña bien estructurada y planeada. Piense en su campaña como una estructura estratificada; el nivel superior lleva el lema de la campaña y el logotipo.



1 SENSIBILIZACIÓN

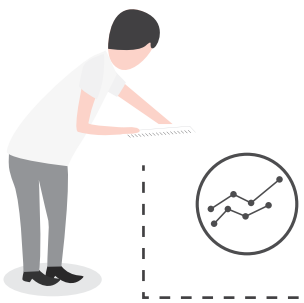
Lema y logotipo

El lema es esa frase corta, concisa, que, con suerte, será fácilmente reconocible y establecerá el tono de la campaña. El mensaje y el logotipo proporcionan la identidad de su campaña. Juntos, el lema y el logotipo son el mensaje breve y la imagen gráfica que les anuncia a todos "presten atención, aquí hay algo en lo que ustedes deben pensar o que deben saber". Estos dos elementos constituyen los elementos de marca de la campaña.

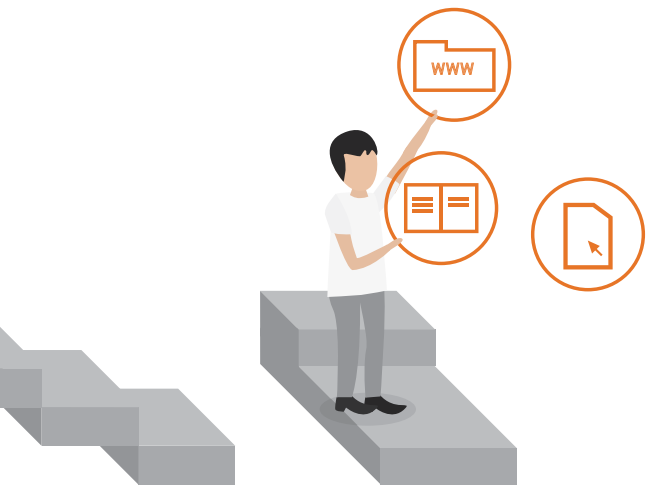
2 EDUCACIÓN

Mensajes de apoyo

El segundo nivel de su campaña son mensajes de apoyo. Estos mensajes comienzan a ser de naturaleza más didáctica. Se le ofrecen al público sugerencias y consejos simples u orientación sobre dónde obtener información más detallada.



El lema y el logotipo son la piedra angular sobre la que se basará su campaña.



3 INFORMACIÓN DETALLADA

Sitio web, materiales para la educación, programas

El tercer nivel de la campaña es la parte educativa. Aquí es donde usted ofrece información detallada, ya sea que se trate de instrucciones sobre cómo crear contraseñas seguras y configurar un servidor de seguridad o un programa sobre la creación de buenas políticas laborales en seguridad cibernética para directores generales.

INVESTIGACIÓN Y MÉTRICAS

Esta es la base fundacional para cualquier campaña

Los datos son de vital importancia para la comprensión de si están funcionando los mensajes y la ejecución de la campaña o no. Como resultado, debe llevarse a cabo investigación en múltiples etapas de su campaña. Antes de comenzar su campaña de planeación, observe qué datos están disponibles. Algunas cosas que debe saber son:

- **¿Cuán conectado está su país?**
- **¿Dónde y cómo se conectan las personas al Internet?**
- **¿Quién está en línea?**
- **¿Cómo se utiliza el Internet para los negocios?**
- **¿Cuáles son los riesgos de seguridad cibernética a los que se enfrenta su país?**
- **¿Cuáles son las pérdidas económicas por amenazas cibernéticas?**

Su gobierno, proveedores de servicios de Internet, operadores móviles, software (de seguridad y de otro tipo) y las universidades pueden tener ya algo de esta información. Establezca alianzas con estas instituciones para tener acceso a la investigación que estas puedan estar adelantando para ayudar aún más a su campaña.

Las métricas son los datos que miden el éxito de su campaña. La recolección de datos antes y durante su campaña le permite tener una mirada crítica a si está o no está cumpliendo sus objetivos y lo ayuda a evaluar la efectividad de su campaña. Estos datos le pueden decir si hay un área en la que hay que centrarse o si necesita considerar la posibilidad de ajustar el mensaje o cambiar de táctica.

K Véase el **Apéndice K** para ejemplos de investigaciones y encuestas

El mensaje

El corazón mismo del mensaje debe ser simple y fácil de entender para todos.

Es fácil caer en la trampa de entregar mucha información, y muy técnica, por el deseo de convertir a su público en uno muy conocedor. La gran parte de su público no tiene que ser muy conocedor; más bien debe saber cómo protegerse. Entregarle demasiada información técnica lo abrumará. Así como se enseña a contar antes de sumar, restar y multiplicar, el enfoque de la seguridad cibernética debe ser similar: enseñar lo básico primero.

El mensaje y el material educativo complementario deben estar en un lenguaje sencillo y se debe hacer un esfuerzo por evitar la jerga técnica. Debe mantenerse al mínimo cualquier información adicional (como consejos y asesoramiento) para no abrumar al público con una lista de demasiadas cosas por recordar. Los consejos deberán enmarcarse en un lenguaje positivo y contener pasos de acción.

Los mensajes positivos animan a las personas a moverse y son más eficaces que aquellos basados en el miedo. La investigación muestra que la seguridad cibernética[1] no es diferente. Los mensajes basados en miedo para la seguridad cibernética dejan en las personas una sensación de

Por Ejemplo:

Consejos **Negativos**

Los computadores que **no tienen software** de seguridad actualizado están **en riesgo de ser atacados** por la delincuencia cibernética.

Consejos **positivos, orientados a la acción**

Ayude a **impedir** la delincuencia informática, al **mantener actualizado** el software de seguridad. Utilice la configuración de actualización automática **para que sea fácil.**

Consejos **Negativos**

Compartir **demasiada** información personal en sitios de redes sociales puede conducir al **robo de identidad**.

Consejos **positivos, orientados a la acción**

Tenga cuidado con su información personal en las redes sociales. **Revise** la configuración de privacidad y **limite** la cantidad de información que pone a disposición de otros.

1. http://stopthinkconnect.org/research-surveys/

impotencia y les hace creer que la situación no tiene salida. Pero los mensajes positivos, de empoderamiento, dan como resultado que la gente siente que puede afectar a la situación y que, al tomar medidas, se convierte en parte de la solución.

El lema y los mensajes complementarios (y el logotipo) deben captar la atención de su público y movilizarlos. La única manera de saber si lo ha logrado es a través de la investigación. Es posible que su presupuesto dicte qué tipo de investigación será y cuán rigurosa. El lema y el logotipo son la piedra angular sobre la que se basará su campaña. Los mensajes complementarios son elementos vitales. La investigación sobre estos elementos para asegurar que le llegarán a su público es una inversión en el éxito de su campaña. (Véase el Apéndice L para conocer un ejemplo de este tipo de campañas, la campaña PARA. PIENSA. CONECTATE.)

Una campaña de este tipo es un compromiso de largo alcance. El mensaje debe ser coherente, persistente y flexible. A medida que su público se vaya concientizando, el mensaje debe evolucionar con ellos para acompañarlos en la adquisición de nuevos conocimientos y abordar la naturaleza evolutiva de la seguridad cibernética.

La siguiente tabla es una plantilla sencilla para ayudarle a idear sus mensajes, identificar su público, determinar lo que su público necesita saber y los mensajes clave para lograr ese objetivo.

Audiencia	Lo que necesitan saber	Mensajes clave
 **Público general**	• Cómo estar seguro en línea • Cómo proteger sus finanzas • Cómo proteger su identidad • Qué recursos están disponibles • Dónde acudir para obtener ayuda	› Mantenga actualizado el software para ayudar a prevenir el delito cibernético. › Proteja sus finanzas. Solo use redes confiables y seguras para acceder a su información financiera.
 **Negocios**	• Cómo proteger sus negocios • Cómo proteger sus finanzas • Cómo proteger sus datos • Cómo educar a sus empleados • Qué recursos están disponibles • Dónde acudir para obtener ayuda	› Proteja su negocio. Mantenga las redes y datos seguros. › Conozca los riesgos. Edúquese y a sus empleados.
 **Niños y niñas**	• Cómo ser usuarios seguros de Internet • Cómo proteger su identidad • Qué recursos están disponibles • Dónde acudir para obtener ayuda	› Sea un buen ciudadano cibernético. Sea respetuoso y amable en línea. › Piense antes de publicar.

L Véase el **Apéndice L** para conocer un ejemplo de este tipo de campañas.

Guía de planificación de campaña

Guía de planificación de campaña

Una campaña es más que un simple mensaje. Una campaña es una operación para lograr un objetivo particular; en este caso, la sensibilización y educación. Esta guía de planificación de campaña lo guiará por los pasos para desarrollar una campaña con objetivos claros, una estrategia y tácticas para alcanzar esas metas y métricas para medir el éxito.

Cada paso se descompone en un proceso secuencial, comenzando con la conformación de un grupo crítico de interesados. Dado que la seguridad cibernética no es un problema de "una persona o una entidad", estamos proponiendo el establecimiento de un proceso grupal para construir alianzas para la creación de una campaña en la que pueden participar varios grupos de interés, ya sea que se trate de múltiples agencias gubernamentales o de una alianza público-privada.

El siguiente diagrama de flujo es una descripción de alto nivel de los pasos para construir una campaña.

Actores Críticos

¿Quién debe ser parte del proceso de planeación?

· Gobierno - ¿Qué entidades?
· Empresas
· Tecnología
· Telecomunicaciones
· Servicios financieros
· Ventas al por menor
· Comunidad/Las ONG

Objetivos

¿Qúe se quiere lograr?

· Crear un cambio en actitudes y comportamiento
· Desarrollar ciudadanos confiados en línea
· Reducir la incidencia de delitos cibernéticos

Audiencia

¿A quién está tratando de impactar?

· Público en general
· Empresas
· Juventud
· Educadores
· Gobierno

Análisis situacional

¿Cuál es su situación actual?

· ¿Qué es lo que ya saben?
· ¿Qué necesitan saber?
· ¿Cuáles son los temas más importantes que deben abordarse?
· ¿Qué recursos (capacidades internas y plataformas de financiación existentes, sociedades) están disponibles?
· ¿Qué barreras al éxito deben ser abordados?
· ¿Hay algo que usted no quiere que le suceda a la campaña?

Estrategia

¿Cómo va a lograr su(s) objetivo(s)?

· Desarrollar el lema y mensaje de la campaña
· Construir una fuerte presencia en la web
· Implementar un conjunto de mensajes dirigidos
· Desarrollar programas de difusión

Tácticas

¿Qué es exactamente lo que va a hacer para poner en práctica su estrategia?

· Construir un sitio web
· Utilizar un mediador social para entregar mensajes de forma continua
· Tener un blog quincenal
· Desarrollar y difundir carteles en todas las agencias del gobierno
· Desarrollar un programa de educación para la eduación primaria y secundaria

Éxito ¿Cómo se medirá?

Productos

· Cobertura de los medios - cantidad
· Alcance de los medios y web (número de personas potenciales)
· Eventos/asistencia a evento
· Material de marketing distribuido
· Visitas a la web

Resultados (contenido y alcance)

· Cobertura de los medios - calidad
· Conciencia de marca
· Cambio de actitud
· Cambios de comportamiento

Resultados (impacto)

· Menos delitos cibernéticos
· Más uso de software de seguridad
· Inclusion de la seguridad cibernética en el presupuesto
· Mejor denuncia de delitos cibernéticos
· Aumento de la confianza del consumidor

Actores críticos

¿Quién debe ser parte del proceso de planeación?

La propia naturaleza de la seguridad cibernética es que no es "propiedad" de una entidad o particular. El gobierno, las empresas (en particular, los proveedores de servicios de Internet, telecomunicaciones, software y servicios financieros) y los particulares tienen la responsabilidad de mantener una parte del Internet seguro. Lo ideal sería que una campaña de sensibilización fuera apoyada por una multitud de socios que pueden aportar recursos, ya sea a través de la financiación directa, el desarrollo de recursos o la inclusión en materiales de producto o de marketing.

Todas estas entidades tienen un gran interés en la creación de un entorno de seguridad cibernética más seguro y en la construcción de la confianza del consumidor en el ecosistema en línea. Una alianza que entregue un mensaje unificado será más eficaz que numerosos esfuerzos distintos, lo que aumenta las posibilidades de éxito. El compromiso con la campaña por parte del Gobierno, las empresas, la academia y las organizaciones comunitarias/no gubernamentales proporcionará una amplia plataforma para entregar los mensajes, llegar a muchos públicos y, con suerte, ayudar a darle longevidad a la campaña.

Líderes de la industria de la tecnología, financiera y de telecomunicaciones deben participar ya que son recursos confiables en el mercado y son proveedores de servicios en línea de los que depende el público en general y las empresas. Estas empresas tienen un interés en la construcción de la confianza del consumidor en el mercado en línea y en la protección de las redes y los servicios que prestan. Les resultaría muy natural educar al público sobre cómo ser más seguro y protegido durante el uso de sus servicios. En virtud de que a menudo están en constante comunicación con los consumidores, tienen una plataforma natural para crear conciencia y proporcionar educación. Tiene sentido que las instituciones financieras eduquen a los consumidores acerca de prácticas bancarias seguras en línea y que los operadores de telefonía móvil proporcionen información sobre la seguridad móvil. El lanzamiento de una campaña coordinada con todos los agentes refuerza el mensaje para todos.

Las organizaciones no gubernamentales y organizaciones basadas en la comunidad también son socios naturales. A través de sus respectivas misiones para proporcionar asistencia y educación a sus públicos, pueden convertirse en grandes vehículos para ofrecer programas educativos, sobre todo a un público al que de otra manera podría ser difícil llegar. También pueden tener conocimiento especial de las necesidades específicas de una población que podría ser valioso a medida que usted desarrolla su campaña y programa.

La creación temprana de un grupo de actores críticos de campaña le ayudará a incrementar apoyo y participación. Desarrolle una lista de quién cree usted que debería ser parte de su grupo de interés. Una vez que haya identificado su grupo inicial de interesados, invítelos a participar en una discusión facilitada sobre las necesidades de la campaña. La inclusión de estas personas en el inicio del proceso de construcción los ayudará a apropiarse de la campaña, lo que aumentará sus posibilidades de participación en el futuro. Ellos también podrían contribuir con opiniones o recursos valiosos como plataformas de investigación y distribución.

Las siguientes secciones lo guiarán por una serie de temas a considerar. Estas secciones están diseñadas para ayudarlo a recopilar información sobre sus grupos de interés, posteriormente esta información formará parte de su estrategia.

Permita que fluya libremente la conversación en cada tema. Un facilitador neutral ayudará a eliminar cualquier sesgo y alentará a todas las partes interesadas a participar desde su punto de vista.

H Véase el **Apéndice H** para conocer directrices de reuniones y de facilitación.

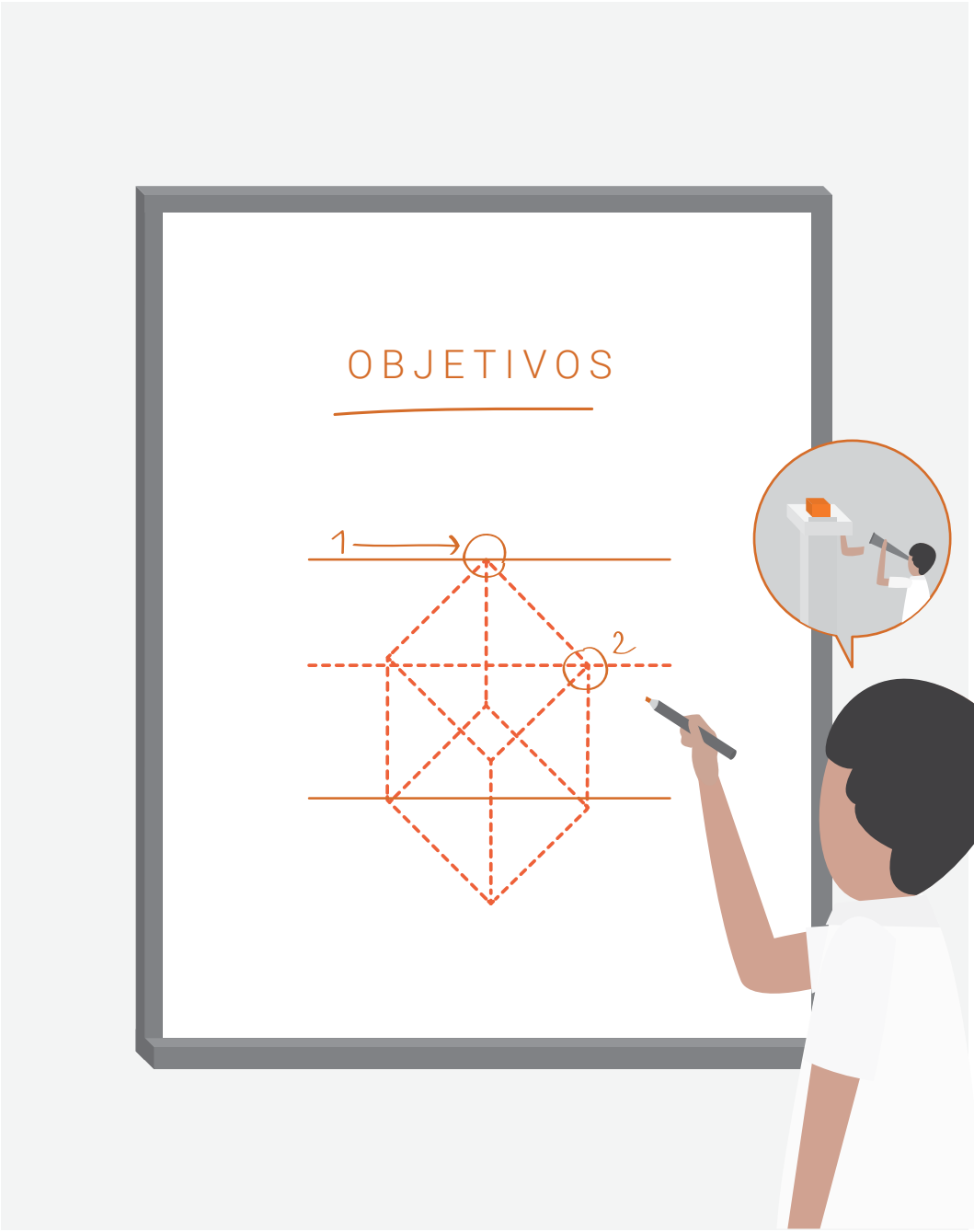
Objetivos

¿Cómo sería el éxito?
¿Cuáles son los objetivos de la campaña?

Ahora que ha reunido a su grupo crítico de interesados, la primera parte de la discusión debe enfocarse en las necesidades y los objetivos de la campaña. Usted probablemente encontrará una gran cantidad de metas muy variadas.

Algunos ejemplos de éxito

- ✓ Actitud basado en el riesgo/ cambios de comportamiento
- ✓ Comprensión de los riesgos a la hora de adoptar nuevas tecnologías y aplicar estrategias para abordarlos
- ✓ Menos incidentes de seguridad cibernética
- ✓ El usuario comprende toda la información y se convierte en portador del mensaje. La transición de estudiante a maestro
- ✓ El empoderamiento de los padres para facilitar el uso responsable de la tecnología por parte de los niños y niñas
- ✓ Mejora de la protección de la propiedad intelectual en línea


OBJETIVOS
1
2

Audiencia

¿A quién se pretende llegar con la campaña?

Esto debería ser bastante sencillo. ¿A quién hay que educar? Es probable que su grupo llegue a la conclusión de que todo el mundo necesita ser educado (el público en general, dueños de negocios, empleados, niños y niñas). ¿Hay grupos específicos que requieren una consideración especial (por ejemplo, los de mayor edad, hablantes no nativos, pequeña empresa)? ¿Hay un público en particular que tiene mayor prioridad sobre los demás?

Gobierno

Aunque el gobierno puede liderar esta campaña, el gobierno también se considera público para esta campaña. El gobierno recoge y mantiene todo tipo de datos sensibles que, en caso de vulneración, podrían resultar perjudiciales para los particulares, la seguridad nacional o la economía nacional. Además, redes sensibles que son vitales para el funcionamiento del país no pueden darse el lujo de estar en riesgo. Los empleados gubernamentales deben ser conscientes de la cibernética y entender su papel en ayudar a mantener una fuerte postura de seguridad cibernética.

D Vea el **Apéndice D** para un ejemplo de campaña.

Público en general

La seguridad cibernética afecta a todos, incluso a aquellos que no están "en línea". Todo tipo de entidades, incluyendo el gobierno, negocios, grandes y pequeños, proveedores de salud e instituciones financieras mantienen en sus sistemas datos personales. El correo electrónico, las redes sociales, compras en línea, banca en línea, en casa y en movimiento se están convirtiendo en actividades cotidianas para muchas personas. Toda esta información y datos son de mucho cuidado. Cada vez que hay una violación o se ve comprometida una cuenta, se erosiona la confianza en Internet. Al dotar a las personas con conocimientos y habilidades para estar más seguros cibernéticamente ayuda a construir la confianza en el mercado de Internet y frustrar la delincuencia cibernética.

F Vea el **Apéndice F** para un ejemplo de campaña.

Niños y niñas

Se debe educar a los niños y niñas sobre el uso seguro de la tecnología. Así como les enseñamos a andar por una ciudad o el pueblo y aprender las reglas de la carretera, ellos también deben aprender a navegar por el mundo digital. El acceso a la tecnología y el Internet abunda, como computadores personales en la escuela (y a menudo con el requisito del uso de Internet para completar o entregar una tarea), el uso de dispositivos móviles, todas las formas en que nos comunicamos, y cómo compartimos o accedemos a la información. Las preocupaciones son numerosas: la seguridad del niño, la seguridad de la tecnología y la información, y la ética del uso y la comunicación. La formación sobre el uso adecuado y responsable de la tecnología y el Internet debe comenzar cuando el niño comienza a utilizarlas, que a menudo es a una edad muy joven.

E Vea el **Apéndice E** para un ejemplo de campaña.

Padres

Los padres necesitan ser educados junto con sus hijos. A menudo los niños y niñas saben más acerca de cómo utilizar la tecnología que sus padres, que puede llevar a una sensación de impotencia y evitar abordar la cuestión. Provean a los padres con la información y los recursos que necesitan para ayudar a guiar a sus jóvenes mientras navegan el mundo digital. Tal vez no sepan cómo utilizar toda la tecnología pero pueden orientar y proporcionar sabiduría sobre cómo tomar buenas decisiones.

E Vea el **Apéndice E** para un ejemplo de campaña.

Maestros

Los maestros serán fundamentales para educar a los niños y niñas acerca de todo tipo de seguridad en línea. Proporciónenles oportunidades para que aprendan, materiales de clase y educación continua. También deben entregárseles programas que cubran la seguridad básica en línea y las prácticas de seguridad, el acoso cibernético, la privacidad, la seguridad cibernética (virus, engaños, fraudes, etc.) y medios de comunicación social. Como muchos de estos problemas pueden ser bastante complejos, es aconsejable realizar sesiones de capacitación vivenciales para permitir que se realice un debate en profundidad.

E Vea el **Apéndice E** para un ejemplo de campaña.

Escuelas

Las escuelas deben desempeñar un papel fundamental en la educación de los niños y niñas sobre la seguridad en línea. Aunque la mayoría de los niños y niñas tienen acceso a la tecnología y el Internet, no todos tienen padres o tutores con el conocimiento y la capacidad para facilitarles una buena orientación sobre cómo navegar mejor el mundo digital. No solo existe una necesidad social de que las escuelas ayuden a desempeñar este papel, sino que también existe la expectativa de que los niños y niñas usen la tecnología y el Internet para apoyarlos en sus estudios. Así como hay reglas y expectativas de comportamiento seguro en el aula, también debería haberlas para la tecnología e Internet. Por otra parte, a medida que los jóvenes dejan la escuela y entran a la universidad y al lugar de trabajo, la expectativa será que son usuarios versados en tecnología.

E Vea el **Apéndice E** para un ejemplo de campaña.

Empresas

Las empresas, ya sean grandes o pequeñas, deben tener un interés propio en la seguridad cibernética. La propiedad intelectual, las finanzas, la información del cliente e información de los empleados son todos datos sensibles que no pueden permitirse perder. Dicho esto, las empresas pueden ser un público difícil de llegar, sobre todo las pequeñas y medianas empresas que no entienden la gravedad de la amenaza cibernética o cuyos propietarios y operadores están completamente inmersos en las operaciones del día a día del funcionamiento de una empresa. El educar a los ejecutivos de negocios y la fuerza laboral es también una oportunidad para educar al usuario en general ya que muchos de las medidas de seguridad que los empleados deben tomar en el lugar de trabajo son las mismas que deben ser implementadas en casa.

G Vea el **Apéndice G** para un ejemplo de campaña.

Análisis de la situación

¿Cuál es la situación actual?

Una buena comprensión del estado de la cuestión es de suma importancia para el desarrollo y el lanzamiento de una campaña exitosa. Es importante asegurar que el análisis de la situación se haga integralmente.

Recopile toda la información que sea posible antes de esta reunión. Una parte importante de la fase de planeación es entender el contexto local. Las siguientes preguntas pueden ayudarle a ilustrar cómo es el perfil de amenazas de seguridad cibernética en su país. Le ayudarán a proporcionar el contexto de por qué es importante una campaña de sensibilización y le otorgarán credibilidad a las solicitudes de participación y financiación. Es posible que su gobierno, los proveedores de servicios de Internet, los operadores móviles, el software (seguridad, proveedor de servicios, de búsqueda) y las universidades ya tengan algo de esta información. Otras fuentes son las siguientes.

OEA
Organización de los Estados Americanos
http://www.oas.org/

UIT
Unión Internacional de Telecomunicaciones
http://www.itu.int/

Centro de Investigación Pew
http://www.pewglobal.org/

APWG
Grupo de Trabajo Anti-Phishing
http://www.antiphishing.org/

Una búsqueda a través de los medios de comunicación también puede resultar en algo de inteligencia, particularmente con respecto a las violaciones a los negocios orientados al consumidor que han impactado a su país.

Si no puede encontrar datos relevantes para algunas de estas preguntas, es posible que desee considerar la realización de investigación según los recursos que tenga disponibles. Tener una sólida comprensión del panorama de seguridad cibernética es importante, a medida que construye su campaña. Por lo tanto, es importante ponerse en contacto con las partes interesadas que pueden ayudar a determinar:

AVERIGÜE

- ¿Cuán conectado está su país?
- ¿Dónde y cómo se conectan las personas al Internet?
- ¿Quién está en línea?
- ¿Con qué tipo de dispositivos?
- ¿Qué tipos de sistemas operativos y canales de comunicación?
- ¿Para qué tipo de productos y servicios?
- ¿Cómo se está utilizando el Internet para los negocios?
- ¿Cuál es la escala de esas empresas (por ejemplo, ¿empresas individuales? ¿Cooperativas agrícolas? ¿PYME para servicios? ¿Fabricación ligera)?
- ¿Cuáles son los riesgos de seguridad cibernética a los que se enfrenta su país?
- ¿A qué tipo de delitos cibernéticos se enfrentan los consumidores minoristas?
- ¿A qué tipo de delitos cibernéticos se enfrentan sus empresas?
- ¿Se distinguen estos delitos cibernéticos por cohorte?
- ¿Cuáles son los riesgos de su infraestructura crítica?
- ¿Ha habido grandes violaciones, ya sea gubernamental o comercial, en el pasado reciente?
- ¿Hay amenazas de grandes violaciones en el futuro?
- ¿Cuáles son las pérdidas económicas o el potencial de las amenazas cibernéticas?

Las preguntas anteriores deben ayudar a proporcionarle un marco del problema. La siguiente serie de preguntas tiene la intención de ayudarle a pensar más profundamente en su campaña para determinar las prioridades que se deben discutir con su grupo de interés:

¿Qué es lo que el público ya sabe? ¿Qué necesita saber?

No dé por sentado ni el conocimiento ni la falta de conocimiento. Por ejemplo, usted podría asumir que su público no sabe que debe utilizar contraseñas. La realidad podría ser que el público si sabe que debe usar contraseñas, pero no sabe cómo crear contraseñas fuertes o cómo gestionarlas. ¿Hay alguna investigación existente que se pueda contribuir a su campaña? ¿Será necesario llevar a cabo más investigaciones para tener una mejor comprensión de lo que su público sabe y no sabe?

¿Cuáles son los temas más importantes que deben abordarse?

¿Hay determinados temas de seguridad cibernética que son más preocupantes que otros? Defina su métrica para establecer prioridades: (Por ejemplo, costo para las empresas; costo para las personas; número de afectados por tema de seguridad cibernética)

¿Qué recursos (capacidades internas, financieras, plataformas existentes, sociedades) están disponibles?

¿Qué barreras al éxito deben abordarse?

¿Existen peligros potenciales que necesitan ser evitados? ¿Hay algún problema específico con la soberanía que deba ser tratada desde el principio para asegurar que sea una campaña exitosa?

¿Hay algo que usted no quiere que suceda con la campaña?

Piense en otras campañas que has visto. ¿Qué fue lo que no le gustó de ellas? ¿Dónde le han fallado esas campañas a su país de una manera que se quiera evitar en el despliegue del programa de sensibilización sobre la seguridad cibernética de la nación?

Teniendo en cuenta los recursos que se han identificado, la prioridad de las cuestiones y los públicos que deben abordarse, ¿Cuál sería una meta realista para el inicio de esta campaña? ¿Cuáles son las tres prioridades más importantes?

Al responder a las preguntas anteriores usted deberá poder identificar cuáles son sus objetivos para una campaña. Usted podrá encontrar que se pueden articular metas de corto plazo y de largo plazo. Utilice la información de estas preguntas para definir su estrategia y establecer sus prioridades para la campaña. Es posible que usted identifique un área donde se necesite realizar una investigación con el fin de tener una idea clara sobre el tema.

K **Vea el Apéndice K** para conocer ejemplos de algunos de los tipos de investigación e informes que se han realizado.

Estrategia

¿Cómo logrará su/s objetivo/s?

Una vez que haya identificado sus objetivos, incluyendo sus principales prioridades, es necesario determinar: ¿Cómo será la campaña? ¿Habrá relaciones públicas, una presencia en la web, o divulgación a la comunidad de negocios? ¿Habrá investigación continua? ¿Qué estrategias se utilizarán para llevar a cabo la campaña?

Una estrategia no tiene que ser una operación o diseño complejo. Una estrategia debe ser una hoja de ruta clara para lograr el éxito. Asegúrese de incluir un cronograma con su estrategia para ayudar a establecer parámetros mensurables para la campaña. Ejemplo:

Año 1

- Establecer el logotipo de la campaña, lema y mensajes clave
- Realizar investigación de referencia
- Construir una fuerte presencia en la web
- Llevar a cabo una amplia difusión en los medios
- Enfoque en la juventud y la familia
- Implementar un conjunto de mensajes dirigidos
- Desarrollar un programa de divulgación
- Identificar las métricas con las que medir el éxito

Año 2

- Llevar a cabo investigaciones de referencia para medir el progreso de la campaña
- Continuar el enfoque en la juventud y familia
- Construir y lanzar la campaña para negocio
- Lanzar anuncios de servicio público nacional

Año 3

- Llevar a cabo investigaciones de referencia para medir el progreso de campaña
- Continuar el enfoque hacia la juventud y familia
- Continuar la campaña empresarial
- Desarrollar la formación de los docentes y educación en las aulas

Su estrategia le ayudará a definir el panorama. Proporciona la hoja de ruta para la campaña y establece los objetivos de alto nivel para mantener el rumbo. Una estrategia claramente definida también le ayudará a dividir la campaña en metas realistas al priorizar el trabajo que hay que hacer.

A Vea el **Apéndice A** para conocer el ejemplo de las estrategias de campaña.

B Vea el **Apéndice B** para el ejemplo de las estrategias de relaciones con los medios.

Táctica

¿Qué hará exactamente para poner en práctica su estrategia?

Las tácticas son los detalles de su estrategia. Aquí es donde usted entra en el detalle del programa y cronogramas. Piense cada parte de la estrategia. ¿Cómo logrará ese objetivo? ¿Qué actividades deben llevarse a cabo? ¿Qué recursos se necesitan? ¿Cuál es el plazo para la finalización? También debe establecer cómo se medirá cada actividad.

Por Ejemplo:

Construir una fuerte presencia en la web

Construir y poner en marcha un sitio web para consumidores dentro de los primeros 3 meses de la campaña

métricas

- Establecimiento de la página web
- Números de Visitantes
- Números de páginas visitadas
- Duración de la estancia en la página
- Números de descargas (contenido como carteles, banderas de la web, etc.)

Utilización de medios sociales para entregar mensajes de forma continua

- Construir una página de Facebook para atraer a los jóvenes
- El uso de Twitter para la difusión diaria
- Utilice Vine y YouTube para publicar videos cortos de seguridad cibernética

métricas

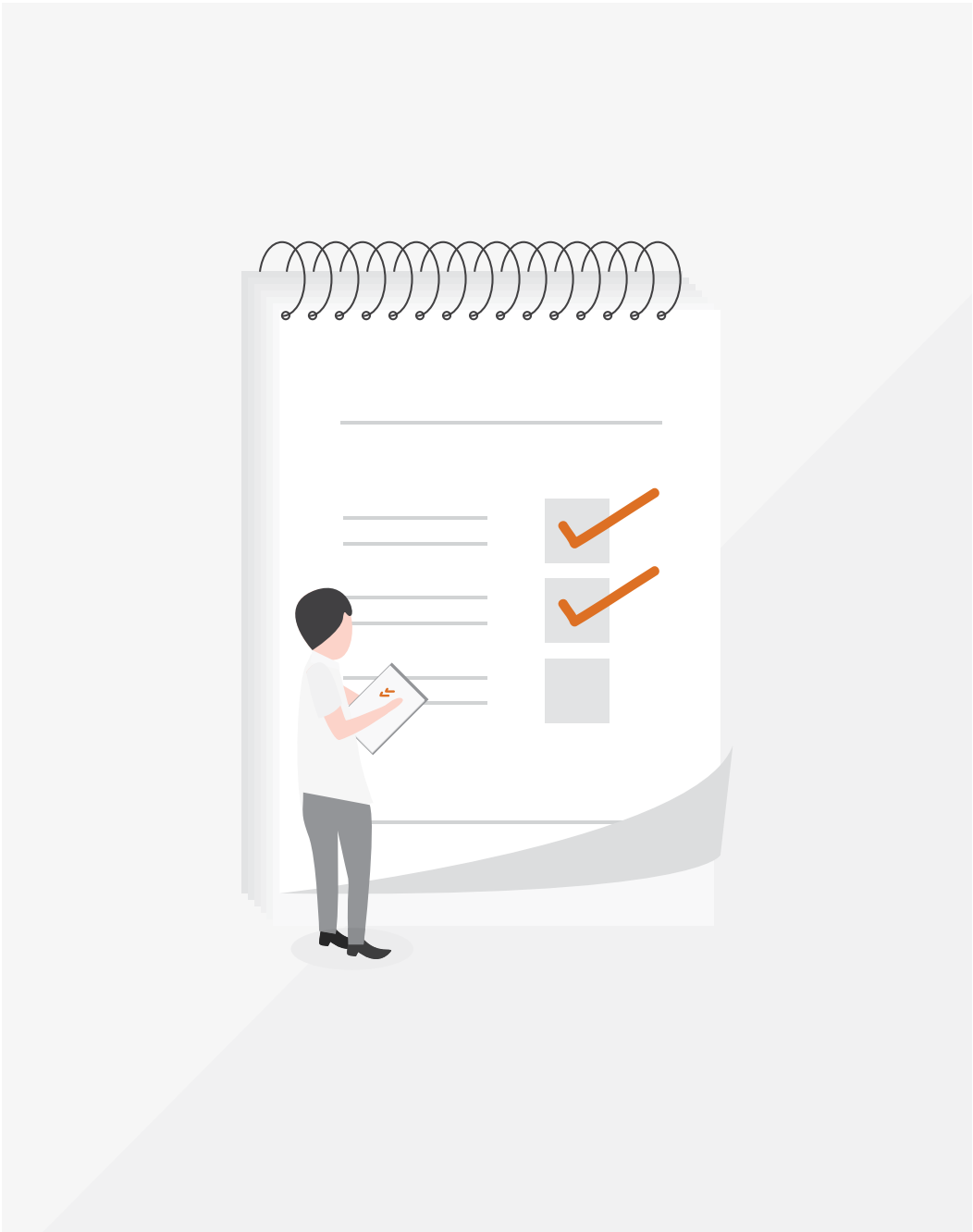
- Participación del público: Número de seguidores, gustos, opiniones, re-tuit, compartir (cada plataforma de medios sociales tiene una manera de medir la participación de público)
- Número de publicaciones

Establecer publicaciones en el blog dos veces por semana, al mes 4 de la campaña

- Tener un autor de blog regular o grupo de autores de blog
- Usar autores de blog invitados para completar el contenido
- Establecer un calendario editorial para la entrega

métricas

- Establecimiento del blog
- Número de publicaciones en el blog
- Número de re-publicaciones en el blog (a través de redes sociales, foros de noticias en línea)
- Establecimiento de un calendario editorial



Meta 1

Hacer que la seguridad cibernética sea una cuestión de negocios.

Objetivos

- La seguridad cibernética se convierte en una cuestión de ejecutivos de nivel C (CEO, CFO, etc.)
- La seguridad se convierte en una cuestión relacionada con el negocio y no solo una cuestión de TI: la comprensión de por qué las empresas deberían emplear prácticas seguras
- Inclusión deliberada de fondos para las iniciativas de seguridad cibernética en los presupuestos
- Mejora de la protección de la propiedad intelectual en línea
- Actitud basado en el riesgo/ cambios de comportamiento
- La comprensión de los riesgos a la hora de adoptar nuevas tecnologías y la aplicación de estrategias para abordarlo

El siguiente modelo lógico de táctica de campaña está diseñado para ayudarle a diseñar sus tácticas, los recursos necesarios y cuáles serán los resultados y métricas.

C

Vea el **Apéndice C** para una plantilla.

ACTIVIDADES **Cosas que ocurrirán para alcanzar los objetivos**	• Crear una mesa redonda ejecutiva sobre seguridad cibernética • Llevar a cabo reuniones informativas ejecutivas • Desarrollar y distribuir un kit de herramientas de negocios • Relaciones con los Medios • Construir sitio web para alojar información
INSUMOS/ RECURSOS **Financieros, tecnológicos, humanos**	• Administrador de programas • Los fondos para eventos y desarrollo de material de marketing • Los fondos para las relaciones con los medios • Los fondos para el desarrollo de sitios web • Administrador de Web
PRODUCTOS **Productos tangibles, directos de las actividades que conducen a resultados**	• Eventos de mesa redonda • Lanzamiento sitio web • Cobertura de los medios • Kit de herramientas del director ejecutivo
RESULTADOS **Resultados deseados de las actividades**	• Directores ejecutivos más comprometidos en el tema • Cobertura/ colocación de medios de mayor calidad • Los empleados reciben más educación en el lugar de trabajo
MEDICIÓN **Indicadores que pueden ser medidos**	• Visitas de Página o sitios web • Descargas de contenido • El aumento del gasto en materia de seguridad cibernética • La seguridad cibernética se incluye como partida presupuestal • Cobertura y colocación de medios

Meta 2

Educar a los niños y niñas acerca de cómo estar a salvo y seguro en línea

Objetivos

- Se educa a los niños y niñas en seguridad en línea

ACTIVIDADES **Cosas que ocurrirán para alcanzar los objetivos**	• Educación en el aula • Concurso de video o cartel • Consejo de la juventud de seguridad en Internet • Distribuir información y realizar labores de divulgación a las familias • Asociaciones estratégicas con organizaciones juveniles • Construir sitio web para alojar información • Medios de comunicación social
INSUMOS/ RECURSOS **Financieros, tecnológicos, humanos**	• Administrador de programas • Premios para el concurso de video o cartel • Los fondos para eventos (Consejo de la juventud) • Los fondos para el desarrollo y distribución de material de marketing • Los fondos para el desarrollo de sitios web • Administrador de Web
PRODUCTOS **Productos tangibles, directos de las actividades que conducen a resultados**	• Concurso de video o cartel • Creación de Consejo de la juventud • Lanzamiento del sitio web • Material de marketing (carteles, banderas web) disponibles en el sitio web • Crear alianzas
RESULTADOS **Resultados deseados de las actividades**	• Los jóvenes participarán en concurso • Lanzamiento del Consejo de la juventud • Jóvenes más conscientes y comprometidos en el tema • Asociaciones sólidas con organizaciones juveniles
MEDICIÓN **Indicadores que pueden ser medidos**	• El número de concursantes • Mayor conciencia entre los niños y niñas • Visitas de página y sitio web • Descargas de contenido • Seguidores de Facebook y Twitter • Cobertura y colocación de medios de comunicación • Número y calidad de las asociaciones

I J

Vea Apéndices I y J para tener orientación sobre los medios sociales y el desarrollo de Infografía.

Éxito

¿Cómo sabrá si ha tenido éxito?

El éxito se definió al principio de este ejercicio. Ahora que usted ha tenido discusiones más profundas sobre el tema y tiene los elementos de una campaña exitosa, ¿cómo medirá su éxito? Ya se han discutido algunas maneras de medir el éxito, pero profundicemos un poco más ya que este es un punto crítico. Para poder saber si ha cumplido sus metas, debe establecer formas de medir el éxito.

Hay dos formas de medir el éxito: cuantitativa y cualitativamente

Los datos cuantitativos son los que se pueden medir con un número. El número de visitas a un sitio web, el número de artículos escritos, el número de personas alcanzadas, el tiempo dedicado a una página web, el aumento del gasto, el número de personas con acceso a Internet son todas las cosas que se pueden medir cuantitativamente.

Los datos cualitativos son los que no se pueden medir con un número. Actitud, sentimientos, tono, confianza son cosas que son de naturaleza cualitativa. Los datos cuantitativos pueden dar cifras duras (ejemplo: hubo un aumento del 25% en el gasto de la seguridad cibernética entre 2014 y 2015 o se produjo un aumento del 18% en visitas al sitio web de octubre a noviembre) y se pueden utilizar para estudios a gran escala con análisis estadístico.

Los datos cualitativos no se pueden utilizar para el análisis estadístico, pero pueden proporcionar una visión más clara de cómo se sienten o piensan las personas. Es muy útil para pequeños grupos de enfoque y para aprender más acerca de por qué la gente se siente o se comporta de cierta manera.

métrica

Productos

(Contenido y alcance)

- Cobertura de los medios - cantidad
- Alcance de los medios y web (número de personas potenciales)
- Eventos/asistencia a evento
- Distribución de material de marketing
- Visitas Web
- Eventos sociales para compartir (número de noticias enviadas, etc.)
- Seguidores (en los blogs, correos y cuentas de Twitter)
- Redireccionamiento de eventos (informes de estado 301/302 que experimentan los usuarios, por lo general en el correo basura y los ataques de suplantación de identidad.)
- Comunicaciones malévolas (por ejemplo, el número de enlaces de malware entregados a través de SMS, correo electrónico, fax y mensajes de suplantación de identidad entregados a través de SMS, correo electrónico y fax)
- Comunicaciones abusivas/no deseadas (por ejemplo, el número de correo basura entregados, número de IVR y llamadas de entrevistas en vivo por los responsables de suplantación de identidad y estafadores que tratan de defraudar.)

Resultados

(Percepción, conocimiento, comportamiento); Los resultados de sus productos

- Cobertura de los medios - calidad
- Conocimiento de la marca
- Cambio de actitud
- Cambios de comportamiento

Resultados

(Impacto)

- Menos delincuencia cibernética
- Un mayor uso de software de seguridad
- Inclusión de la seguridad cibernética en el presupuesto
- Mejora en la denuncia de delincuencia cibernética
- Aumento de la confianza del consumidor

Hay diferentes maneras de recopilar estas métricas

Las medidas que están directamente relacionadas con su programación, como las redes sociales, visitas al sitio web, la cobertura de los medios de comunicación, participación en el evento y la distribución de material de marketing, deben ser fáciles de establecer y de seguir sobre una base mensual. Estos le darán una idea de cómo está aumentando el programa y, si es necesario, poner más énfasis en alguna parte. Además de la articulación de los aumentos o alcance, usted podrá establecer metas para estos indicadores para ayudar en el avance de su programa:

Aumentar las visitas de sitios web en un 10% cada mes

Aumentar seguidores en las redes sociales en un 25% en el primer trimestre

Llegar a 25.000 seguidores en Twitter a finales de 2015

Organizar 8 eventos (o 2 eventos en cada trimestre) para finales de año

Conocimiento de marca

El conocimiento de marca es otra señal de que su campaña está en camino hacia el éxito. La mejor manera de medir el conocimiento de la marca es a través de una encuesta de estilo de marketing donde las personas pueden identificar la campaña. Generalmente se utiliza una plataforma de teléfono o en línea para este tipo de investigación. Generalmente se les hace unas 10-20 preguntas. Este tipo de encuesta también puede ser útil para recopilar datos sobre el conocimiento y las prácticas de seguridad cibernética en general. La desventaja de este tipo de datos es que son de naturaleza más cualitativa que cuantitativa ya que se basan en información aportada por ellos mismos. La ventaja es que es posible tener una idea de la actitud hacia la seguridad cibernética y la voluntad para participar en mejores prácticas de seguridad cibernética.

Las otras métricas que deben establecerse son las que miden el impacto. La medida de impacto es el verdadero testimonio del éxito de su campaña. La medición de las visitas al sitio web y seguidores de redes sociales es una indicación de que va en la dirección correcta y está llegando a la gente, pero no mide si su mensaje ha creado un cambio de comportamiento. Esta medida será más difícil ya que tendrá que observar el comportamiento del usuario. Encuestas por teléfono/en línea que dependen de la información aportada por ellos mismos son una forma de recopilar esta información. La capacidad para vigilar la interacción y el uso del computador y la red es la manera ideal de obtener esta información, pero requeriría tener acceso a un entorno en el que esto fuera posible. Una empresa grande u otro tipo de sistema, como una universidad, podría proporcionar tal entorno de pruebas.

OTRAS FORMAS DE MEDIR EL IMPACTO

Observe cómo las empresas cambian sus políticas y procedimientos.

- ¿Están asignando más recursos a la seguridad cibernética? ¿Han implementado políticas de privacidad y seguridad cibernética?
- ¿Hay más o menos denuncias de delincuencia cibernética a la policía? ¿Qué tipos de delitos se están denunciando?
- ¿Han visto las instituciones financieras un comportamiento más seguro por parte de sus clientes?
- ¿Ha habido una disminución o un aumento en los ataques de suplantación de identidad?

Esta es un área difícil. La medición del comportamiento de los usuarios en los computadores es complicada. Hay que ser creativo y ver qué mediciones usted establecerá y continuará supervisando.

Cuanta más información de base pueda establecer al principio de su campaña, mejor será su campaña. Las métricas le ayudarán a entender su campaña, si usted va por buen camino o si necesita cambiar de táctica. Las métricas lo orientarán y lo ayudarán a tomar decisiones acerca de sus próximos pasos de manera racional.

Organizarlo todo

Ahora que ha reunido la información, posiblemente realizó algunas investigaciones, estableció y se reunió con un grupo de interesados y exploró los detalles de lo que quiere lograr en su campaña, es el momento de juntar las piezas para organizar un plan. Pero recuerde que este no es un solo evento; su campaña debe ser repetible, debe poder detectar cambios y adaptarse a las necesidades del usuario contemporáneos.

Se incluyen en el apéndice ejemplos de estrategias de campaña (A), estrategia de relaciones con los medios (B), y estrategias específicas del público: Gobierno (D), jóvenes, padres y educadores (E), público en general (F) y empresas (G). Utilice estas estrategias para su inspiración y para tener ideas.

Apéndice

A

Estrategias de Campaña

Relaciones con los medios

Las relaciones continuas con los medios son una táctica importante para impulsar el conocimiento de la campaña y proporcionar información y educación sobre cuestiones de seguridad cibernética a todos los públicos. Se debe buscar adelantar iniciativas para trabajar con los medios de comunicación para asegurarse de que comprenden las cuestiones de seguridad cibernética y que están proporcionando la información adecuada acerca de cómo los negocios y las personas pueden protegerse a sí mismas.

Sitio Web

Un sitio web único para la campaña puede albergar todos los materiales de la campaña. Una ubicación consolidada hará que sean más fáciles y más eficientes las actualizaciones de contenido y recopilación de métricas, como visitas al sitio web y descargas de materiales de la campaña.

Medios sociales

Facebook, Twitter, Vine y LinkedIn son excelentes espacios para la campaña. Un posicionamiento estratégico de la campaña a través de estos canales es de importancia clave para proporcionar una divulgación continua y generar la participación del público.

Investigación y datos

Establezca el perfil de línea de base de seguridad cibernética para su país a partir de investigación existente y nueva investigación y planee llevar a cabo estudios e investigaciones de forma regular (al menos anualmente).

Programas y materiales educativos

Desarrolle programas de educación diseñados para las necesidades específicas de sus públicos individuales. Un programa para educar a directores ejecutivos podría consistir en un foro de mesa redonda de directores ejecutivos y la guía y kit de herramientas de seguridad cibernética para negocios que sirva para educar a los empleados. Un programa para la juventud podría incluir una guía de educación para padres, carteles y videos para niños y niñas, planes de estudio para la clase para los profesores y carteles para colgar en el hogar y la escuela.

Alianzas estratégicas

Establezca alianzas estratégicas con asociaciones empresariales, organizaciones basadas en la fe, organizaciones comunitarias y organizaciones juveniles. Estas asociaciones ayudarán a divulgar la campaña e involucrar a diversos públicos.

Eventos

Los eventos pueden ayudar a centrar la atención en la cuestión y son una gran manera de atraer al público deseado. Se organizarán y realizarán varios tipos de eventos para diferentes públicos.

Anuncios de servicio público

Los anuncios de servicio público son una gran manera de llegar a su público y si se hacen bien se pueden usar durante años. Los anuncios de servicio público deben ser de naturaleza positiva, usar el humor y siempre ofrecer pasos que las personas pueden tomar para protegerse a sí mismos. Mientras que los anuncios de servicio público con calidad de emisión de televisión pueden ser caros en su desarrollo, los anuncios de servicio público de radio son relativamente baratos de producir. Los anuncios de servicio público de vídeo para la distribución a través de Internet también son una gran inversión y se pueden hacer por un costo significativamente menor que lo que se necesita para la televisión.

Voceros que son una celebridad

Las celebridades pueden ejercer enorme influencia y poder. Encontrar a una celebridad que sea vocero/a(os/as) en la campaña sería una gran ganancia. En función de los presupuestos y la pasión por la causa, esta(s) persona(s) se puede(n) utilizar en anuncios de servicio público, eventos y medios de comunicación. (Esta táctica particular se considera como una herramienta útil pero no es una necesidad, ya que podría resultar muy costoso).

B

Estrategias de las Relaciones con los Medios

Una estrategia fuerte de relaciones con los medios es de importancia crítica para esta campaña. Los medios locales y nacionales pueden llamar la atención sobre la seguridad cibernética como un problema para el público en general, padres, maestros y la comunidad empresarial. Es de suma importancia que los medios de comunicación entiendan bien la situación. Así como todos los actores necesitan ser educados sobre el tema de seguridad cibernética, también deben hacerlo los medios de comunicación. Su público se orientará por los medios de comunicación a los que considera una fuente confiable de información vital y cobertura oportuna. Trabaje con los medios de comunicación para asegurarse de que entiendan los problemas de seguridad cibernética y de que tengan una buena fuente de información de antecedentes y comentarios. Se debe contratar a un profesional de relaciones públicas (ya sea como una persona interna que trabaja en la campaña o una agencia externa) para hacer el trabajo de relaciones de medios de comunicación para esta campaña.

Resultados Deseados

- Informes con amplio contenido e ilustrados
- Cobertura en profundidad de la seguridad cibernética
- Aumento de la presentación de informes sobre cuestiones de seguridad cibernética.

Estrategias y Tácticas

Divulgación: Educar a los medios de comunicación

Asegúrese de que los medios de comunicación estén hablando de seguridad cibernética. Si bien el énfasis en los medios de comunicación de tecnología será importante, también adelante actividades de divulgación a los medios de comunicación de negocios, estilo de vida, paternidad y educación.

- ¿Cómo afecta la seguridad cibernética a su país?
- ¿Qué le preocupa al gobierno?
- ¿Qué les debería preocupar a los ciudadanos?
- ¿Por qué deberían preocuparse los negocios?
- ¿Cuál es el impacto en la seguridad nacional?
- ¿Cuál es el impacto económico nacional?
- ¿Cuáles son los pasos básicos para estar más seguros cibernéticamente?
- ¿Cuáles son los posibles problemas y amenazas que hay que evitar?
- ¿Qué deben estar enseñándoles los padres a sus hijos?

Estos son solo un puñado de preguntas que deberían abordar los medios de comunicación. Después de que se produzcan violaciones importantes o haya titulares en los medios sobre una amenaza particular, ofrezca la participación de expertos en seguridad cibernética (ya sea del gobierno o del sector privado) para hacer comentarios a los medios de comunicación.

Hojas Informativas

Los medios adoran los hechos y las cifras, ya que ayudan a contar mejor las historias. Proporcione hojas informativas a los medios de comunicación acerca de cómo afecta a su país la seguridad cibernética.

Infografía

Además de ayudar a contar la historia, las infografías pueden (i) ayudar a impulsar la colocación de los medios de comunicación, (ii) ser usadas en los sitios web y en los medios de comunicación social, y (iii) compartirse con las organizaciones asociadas.

Historias personales

Pasar de una idea abstracta de una amenaza cibernética (ya sea a una empresa o a un particular) a un incidente real puede ayudar a que el público se conecte y se identifique con el tema.

Mesa redonda trimestral con los medios

Reúna a un pequeño grupo de expertos del gobierno y del sector privado para hablar sobre seguridad cibernética con los medios de comunicación. En el transcurso del año abarque una amplia gama de temas: La amenaza cibernética, el impacto en la infraestructura crítica y la economía, la juventud y la seguridad cibernética, el impacto en el público en general. Junto con la descripción de la(s) amenaza(s), no se le olvide de incluir siempre información sobre las medidas que se pueden tomar para aumentar la seguridad.

Gira de medios de comunicación satelitales y de radio

Lance la campaña con una gira de medios. Designe a 1 o a 2 expertos (alguien del gobierno y alguien del sector privado) para hablar de la campaña, de por qué la sensibilización de la seguridad cibernética es importante y unos sencillos pasos que la gente puede tomar para comenzar a protegerse a sí misma.

Métrica

- Cobertura de los medios de comunicación - calidad y alcance
- Información justa y equilibrada

C

Plantilla de modelo lógico de las tácticas de la campaña

META 1.

ACTIVIDADES Cosas que ocurrirán para alcanzar los objetivos	
INSUMOS/ RECURSOS Financieros, tecnológicos, humanos	
PRODUCTOS Productos tangibles, directos de las activi-dades que conducen a resultados	
RESULTADOS Resultados deseados de las actividades.	
MEDICIÓN Indicadores que pueden ser medidos	

Objetivos:

META 2.

ACTIVIDADES Cosas que ocurrirán para alcanzar los objetivos	
INSUMOS/ RECURSOS Financieros, tecnológicos, humanos	
PRODUCTOS Productos tangibles, directos de las activi-dades que conducen a resultados	
RESULTADOS Resultados deseados de las actividades	
MEDICIÓN Indicadores que pueden ser medidos.	

Objetivos:

D

Gobierno

El siguiente es un breve resumen de la estrategia de una campaña, la táctica y la métrica para una campaña teniendo a los empleados del gobierno como el público.
Implemente una campaña de educación y sensibilización por todo el gobierno. Dado que es uno de los principales grupos de interés en seguridad cibernética y posiblemente el líder de su campaña, será importante comenzar con el gobierno como un público importante para la campaña. Será una muestra de buena fe para el público que el gobierno toma en serio la seguridad cibernética y que adopta buenas prácticas cibernéticas. Esta adopción primaria de la campaña también preparará a los distintos ministerios o departamentos en comenzar a abordar las necesidades de educación y sensibilización del sector privado.
Si no está ya implementada, la seguridad cibernética en el lugar de trabajo, el intercambio de información y las políticas de privacidad deben establecerse y destacarse como parte de los esfuerzos de sensibilización y educación por todo el gobierno.

Resultados Deseados

- El Congreso y el gabinete ministerial están educados en las medidas que deben adoptarse en relación con la seguridad cibernética (obtención de convencimiento de alto nivel/ejecutivo)
- Inclusión deliberada de fondos para iniciativas de seguridad cibernética en los presupuestos
- Mejora de la protección de la propiedad intelectual en línea
- Una mayor colaboración entre el sector público y privado (directrices unificadas/ estrategias)
- Involucramiento del sector privado

Estrategias y Tácticas

El gobierno tiene tres públicos básicos que deben abordarse: ejecutivos, empleados en general y empleados de TI/SI. La entidad designada para encabezar esto debe liderar los esfuerzos para asegurar la mensajería y distribución de material consistente. Un grupo de trabajo de campaña de todo el gobierno o un consejo compuesto por una persona designada al interior de cada ministerio podría ser útil para ayudar a coordinar las actividades y necesidades de todos.

Ejecutivo

Es importante contar con el apoyo de los más altos niveles dentro de cada ministerio para comenzar a desarrollar una cultura de seguridad. Si no se toman en serio las mejores prácticas de seguridad cibernética y no se cuenta con el apoyo de los ministros y funcionarios de alto nivel, el compromiso en los empleados será más difícil de lograr. La oportunidad de liderar el cambio cultural comienza desde arriba.
Desarrolle materiales de educación ejecutiva para garantizar que todos los ministros y altos funcionarios entiendan las amenazas cibernéticas, tomen las precauciones apropiadas y apoyen el esfuerzo mayor de educar a todos los empleados. Las tácticas para lograr estos objetivos incluyen:

- Sesiones informativas
- Memorandos
- Actualizaciones mensuales/semanales

Empleados en general

Crear una campaña continua para educar a empleados. Los mensajes deben estar orientados a las mejores prácticas de seguridad cibernética en el lugar de trabajo, y además trasladables al entorno doméstico:

- Sitio web

- Enlace a la web externa de la campaña
- Información en los sitios web del ministerio/intranets

- Sesiones de capacitación

Realice sesiones de capacitación presenciales, trimestrales o semestrales, para todos los empleados gubernamentales. Refuerce el mensaje de seguridad cibernética con consejos durante todo el año a través de:

- Mensajes del protector de la pantalla del computador/inicio de sesión (o icono de campaña)
- Señalización en el lugar de trabajo
- Artículos en boletines
- Mensajes de blog
- Reuniones mensuales de discusión durante el almuerzo

Se debe cubrir una amplia variedad de temas incluyendo asuntos relacionados con el trabajo y personales o familiares. Posibles temas pueden ser:

- Asegurar el lugar de trabajo
- Privacidad, medios sociales y usted
- Niños y niñas digitales: lo que los padres deben saber
- El Internet de las cosas

Empleados de tecnología de información y seguridad de la información

El departamento de TI/SI debe ser un aliado en la educación de todos los usuarios de computadoras. La comunicación proactiva entre la administración y el personal de TI/SI es primordial para lograr un buen programa de sensibilización de seguridad cibernética. Un equipo de TI empoderado puede ser un gran recurso y aliado para educar al resto del personal. El personal de TI/SI debe tener acceso a programas de educación continua para mantenerse al día en las mejores prácticas de seguridad cibernética. Todos los ministerios deben tratar de establecer una relación positiva con el personal en estos departamentos para permitir que fluya la comunicación sobre amenazas actuales, amenazas de las que se deben cuidar todos los empleados (campañas de suplantación de identidad y suplantación de identidad dirigida a un objetivo, correos electrónicos y sitios Web maliciosos, etc.).

Métrica

- Visitas a la página/sitio web
- Participantes en eventos (incluyendo presenciales y en línea)
- Eventos de capacitación y participantes
- Alcance de las comunicaciones (blogs, correo electrónico, boletines, notas)
- Gabinete ministerial y el Congreso han sido educados
- Se han incluido los fondos para iniciativas de seguridad cibernética en los presupuestos
- El número de asociaciones que se han establecido

E

Jóvenes, padres y educadores

El siguiente es un breve resumen de una estrategia de campaña, la táctica y la métrica para una campaña dirigida a jóvenes, padres y educadores.

Resultados Deseados

- Las escuelas comienzan a educar a los estudiantes acerca de la seguridad en línea
- Los padres y maestros tienen el poder de facilitar el uso responsable de la tecnología por parte de los niños y niñas
- Los maestros, padres y estudiantes se convierten en ciudadanos seguros en línea
- Los usuarios se vuelven tan conocedores que se convierten en portadores del mensaje

Estrategias y Tácticas

Investigación

Lleve a cabo una encuesta para identificar qué saben los profesores sobre la seguridad en línea y qué están enseñando en el aula. También lleve a cabo investigaciones sobre cómo utilizan los jóvenes la tecnología, el tipo de tecnología al que tienen acceso y qué saben acerca de la seguridad en línea. Utilice esta investigación como base de una encuesta anual para medir la efectividad de la campaña e identificar donde necesitan educación adicional los maestros y los jóvenes.

Programas de computadoras portátiles

Si su país (o territorio o estado) está realizando un programa de computador portátil de uno-a-uno, esta es la oportunidad perfecta para proporcionarles material educativo a los estudiantes y padres de familia. Incluya en cada portátil:

- Directrices y hoja de consejos de seguridad estudiantil
- Contrato de "código de conducta" del estudiante
- Guía de información de seguridad en línea para padres (la guía de la Comisión Federal de Comercio es un excelente ejemplo del tipo de material que puede incluir: https://www.onguardonline.gov/articles/pdf-0001-netcetera_0.pdf)

Maestros

Los maestros serán fundamentales para educar a los niños y las niñas acerca de todo tipo de seguridad en línea. Establezca oportunidades para que ellos aprendan, entregue materiales de clase y provea educación continua. Deben suministrarse programas que cubran prácticas de seguridad básica en línea, el acoso cibernético, la privacidad, la seguridad cibernética (virus, engaños, fraudes, etc.) y medios de comunicación social. En virtud de que muchos de estos problemas pueden ser bastante complejos, se aconseja que se programen sesiones de capacitación presenciales para fomentar un debate en profundidad. También deben estar disponibles recursos en línea a través del Ministerio o Departamento de Educación para proporcionar a los maestros información y herramientas para utilizar en el aula.

La Escuela

- Asambleas Escolares

Las asambleas escolares son una manera efectiva de realizar el lanzamiento de la campaña en el entorno escolar. Pueden ocurrir en cualquier momento del año, pero es importante tener en cuenta las siguientes fechas: el comienzo del año escolar, el mes de concientización en seguridad cibernética (octubre), el día de la privacidad de los datos (29 de enero), el día de seguridad de Internet (10 de febrero), y el mes de la seguridad en Internet (junio).

- Concurso de video/cartel

A los niños y niñas les encantan los concursos. Aproveche su energía creativa con un concurso de video y/o cartel. Esto se puede hacer en la escuela, el distrito y

nacionalmente. Haga que los niños y niñas usen los consejos de la campaña nacional de concientización sobre seguridad cibernética como base para su creación. Deles reglas y pautas a seguir (por ejemplo, el cartel o video deben usar el lema de la campaña, el cartel y/o video debe ser de naturaleza positiva, el cartel o video debe contener al menos un consejo de cómo mantenerse seguro en línea).

- Educación continuada - lecciones en el aula

Los profesores deben dictar lecciones en el aula apropiadas a la edad de los estudiantes como parte del plan general de estudios. Las lecciones pueden estar vinculadas a la utilización de Internet y la tecnología, ya que se utilizan para otras actividades (por ejemplo al repasar las "reglas del camino" antes de ir en línea) o lecciones independientes. Los temas deben incluir la seguridad básica en línea, el uso responsable de la tecnología, la privacidad, el acoso cibernético, medios de comunicación social, y la seguridad cibernética. Los materiales de clase deben incluir:

- Planes de lecciones y actividades
- Carteles
- Hojas de consejos

Padres

- Foros de padres

Organice foros de padres durante todo el año para discutir temas de seguridad en línea. Reúna a un pequeño grupo de expertos para realizar una discusión facilitada. Invite a expertos de la industria (telecomunicaciones, ISP, The Internet Society - ISOC), seguridad en línea, el director de la escuela y agentes de la ley. Asegúrese de que el foro sea abierto y permita todo tipo de preguntas. Tenga materiales a la mano para distribuir después (la guía de seguridad en línea para padres, hojas de consejos, lista de los recursos en línea). Los temas pueden incluir: medios sociales, seguridad cibernética, seguridad y privacidad en línea, seguridad cibernética para el hogar, gestión de la vida digital de su hijo. Hay varias fechas durante el año que son naturales para tener un foro: el comienzo del año escolar, el mes de concientización en seguridad cibernética (octubre), el día de la privacidad de los datos (29 de enero), el día de seguridad de Internet (10 de febrero), y el mes de la seguridad en internet (junio).

- Boletín/folleto

Proporcione información de forma regular a través de un boletín de la escuela u otro de comunicación ya existente (blog, sitio web, las redes sociales). O envíe un volante al hogar con los niños y niñas periódicamente durante todo el año con consejos y recordatorios acerca de la seguridad en línea y la seguridad en el hogar.

- Sitio web

Distribuya información y recursos sobre la campaña a los padres y sitios web de la escuela y el Ministerio de Educación.

Alianzas

Establezca alianzas estratégicas con organizaciones basadas en la fe y organizaciones comunitarias para fortalecer la divulgación de información hacia a la juventud. Los programas de la sociedad civil y las organizaciones sin fines de lucro ofrecen oportunidades para conectar con los niños, niñas y jóvenes sobre el tema de la seguridad cibernética y la seguridad en línea. Involucre a estas organizaciones para averiguar qué tipos de temas de interés han identificado y los tipos de materiales y recursos que les parecen más útiles. Desarrolle programas fáciles de implementar y actividades diseñadas específicamente para su uso por estas organizaciones (3-6 planes de clases para los distintos grupos de edad). Comparta los materiales de la campaña, asegúrese de tener invitados expertos en el tema y solicite participar en sus conferencias.

Seguridad en Internet y Consejo de Seguridad Juvenil

Establezca un consejo para abordar las inquietudes sobre seguridad cibernética y seguridad en línea. El consejo debe estar compuesto por una amplia muestra representativa de las personas que están involucradas en el sistema educativo. Este consejo será una oportunidad para que los padres, estudiantes y personal de la escuela debatan sobre seguridad cibernética y los problemas de seguridad en línea que los preocupa, respectivamente, y provea una oportunidad de colaborar en los programas y políticas para implementar en el sistema escolar.

- Ministerio de Educación
- Directores/líderes escolares
- Maestros
- Padres
- Juventud
- ONG
- Los líderes de programas de educación no tradicionales

Voceros que son una celebridad

Las celebridades pueden ejercer enorme influencia y poder. Involucre a una celebridad

popular entre los jóvenes como vocero y que pueda ofrecer una gran variedad de mensajes de seguridad cibernética y seguridad en línea. Esta persona puede participar en eventos, anuncios de servicio público y ser un portavoz de la campaña frente a los medios de comunicación. Cualquier vocero que es una celebridad debe ser gestionado por la persona designada de Relaciones Públicas para garantizar la coherencia de los mensajes. Como esto es un elemento potencialmente de alto costo, un vocero que es una celebridad debe estar al final de la lista de prioridades al momento de decidir cómo invertir en la campaña si el presupuesto es limitado.

Medios de comunicación

Céntrese en los medios de educación, estilo de vida y de crianza para lanzar las historias y ofrecer entrevistas reactivas.

- Comunicados de prensa

Emita datos, anuncie nuevos programas y eventos

- Artículos aportados - editoriales de opinión

Ofrezca un editorial de opinión o artículo mensual o semanal que se refiera a asuntos de seguridad en línea de la familia con un énfasis en los niños y niñas.

Medios de comunicación social

- Establezca una entrada de blog semanal en el sitio web que cubra temas de seguridad en línea para jóvenes. Desarrolle un grupo de autores de blog invitados para cubrir diversos temas y ayudar a mantener la necesidad constante de contar con nuevos contenidos. Un calendario editorial ayudará en el enfoque del contenido, pero es importante que sea flexible para permitir que haya una observación oportuna sobre los acontecimientos actuales.
- Use Twitter y Facebook para enviar un flujo de mensajes tanto proactivos como reactivos. Utilice estos foros para la polinización cruzada y establezca un amplio grupo de expertos y de mayor alcance público.
- Realice chats de Twitter mensual o trimestralmente para ayudar a impulsar el mensaje de la campaña y logre la participación de un público en línea para tener debates sobre temas de seguridad cibernética. Los temas a cubrir incluyen el acoso cibernético, los jóvenes y el uso apropiado de la tecnología (dentro y fuera del aula), y la crianza de un niño expuesto al mundo digital. Invite a las organizaciones aliadas a ser socios oficiales en los chats de Twitter, ampliando así el alcance de la campaña y generar nuevos seguidores.
- Distribuya anuncios de servicio público a través de radiodifusión tradicional y medios impresos. Si el presupuesto lo permite, la publicidad ambiental también es un buen método de distribución de anuncios de servicio público.

Métrica

- Visitas a la página/sitio web
- Descargas de contenido
- Seguidores de Facebook y Twitter
- Número de alianzas desarrolladas
- Participantes en eventos (incluyendo presenciales y en línea)
- Cobertura y colocación de los medios de comunicación
- Maestros capacitados
- Programas en la clase implementados
- Materiales distribuidos
- Distribución/alcance de los anuncios de servicio público

Muestra del código de conducta de computador de jóvenes

Este código de conducta fue escrito teniendo en mente un programa de computador portátil uno-a-uno, pero fácilmente podría ser utilizado entre el padre/tutor y el niño o niña, o podría ser modificado fácilmente para un uso generalizado de la computadora de la escuela.

Yo [NOMBRE COMPLETO] acepto la responsabilidad de este computador. Siendo la persona responsable de este equipo, me comprometo con lo siguiente (poner sus iniciales en cada viñeta):

- Este equipo ha sido confiado a mí y yo soy responsable de él.
- Lo trataré con respeto.
- Lo utilizaré para el aprendizaje.
- No lo dañaré intencionalmente y no lo utilizaré de una manera que pueda dañarlo.
- Lo guardaré en un lugar seguro.
- Yo Seguiré Buenos Hábitos de Seguridad en Línea.
- Yo Mantendré Una Máquina Limpia. Esto significa que tendré actualizados mi sistema operativo, software de seguridad y los navegadores web. Si no sé hacer esto yo mismo, le pediré a un adulto que me ayude.
- Yo Protegeré Mi Información Personal.
- No compartiré contraseñas.
- Tendré cuidado con quién y cómo comparto información personal como mi cumpleaños, dirección y número de teléfono.
- Yo Me Conectaré Con Cuidado. Tendré cuidado con hacer clic en enlaces y descargar contenidos (vídeos, música, juegos).
- Yo seré un Buen Ciudadano en Línea. Lo que hago en línea me puede afectar a mí mismo y a los demás de manera positiva o negativa.
- No publicaré cosas malintencionadas o chismes sobre otros.
- Seré una persona leal - alguien que cuida de mis amigos y compañeros de clase.
- No compartiré la información personal de otros.
- Seré respetuoso y considerado con los demás.
- Yo le voy a Pedir Ayuda A Un Adulto cuando vea que algo que está mal o me hace sentir incómodo/a.

_____ _____

Firmado por
[FIRMA DEL ESTUDIANTE]

Fecha

Padre o tutor
He revisado el código de conducta con [NOMBRE DEL ESTUDIANTE]. Me comprometo a ayudar a mi hijo/a a seguir el código de conducta y orientarlo/a donde y cuando sea apropiado (o me pondré en contacto con el maestro/escuela si necesito ayuda en la orientación).

_____ _____

Firmado por
[FIRMA DEL PADRE/TUTOR]

Fecha

F

Público en general

El siguiente es un breve resumen de una estrategia de campaña, la táctica y la métrica para una campaña para el público en general.

Resultados Deseados

- Ciudadano en línea confiado
- Actitud basado en el riesgo/ cambios de comportamiento
- Comprensión de los riesgos a la hora de adoptar nuevas tecnologías y aplicar estrategias para abordarlos
- Los usuarios se vuelven tan conocedores que se convierten en portadores del mensaje.

Investigación

Lleve a cabo investigaciones amplias para reunir una base de referencia de lo que la gente sabe sobre la seguridad cibernética, la forma en que se conecta a Internet, cómo está utilizando el Internet y si puede identificar la campaña. Utilice esta investigación de manera que sirva como el inicio de un estudio anual con el que podrá medir el progreso y el éxito de la campaña.

Gobierno Electrónico

Utilice todos los portales gubernamentales que miran al público como una oportunidad para educar a la población. Coloque el logotipo de la campaña y uno o dos consejos de campaña en una bandera en todos los portales o sitios web a los que accede el público.

Alianzas

Aproveche las alianzas existentes y los programas sociales con organizaciones basadas en la fe y organizaciones comunitarias para fortalecer la divulgación al público en general. Céntrese en aquellas poblaciones que pueden ser difíciles de alcanzar y a menudo carecen de estos servicios, como los ancianos y personas con capacidades diferentes. Comparta materiales de la campaña, invita a expertos y solicite participar en las conferencias de esas organizaciones. También involucre a estas organizaciones para averiguar qué temas son motivo de especial preocupación, que ellos puedan ayudar a abordar y qué tipos de materiales y recursos consideran más útiles.

Medios de comunicación

Una estrategia fuerte de relaciones con los medios es de importancia crítica para la educación del público sobre cuestiones de seguridad cibernética. Los medios locales y nacionales pueden llamar la atención sobre el tema en general, así como centrarse en las amenazas actuales y ayudar a que la seguridad cibernética sea más relevante para el público en general. Debe contratarse un profesional de relaciones públicas (ya sea como una persona interna que trabaja en la campaña o una agencia externa) para hacer este trabajo.

- Concéntrese en los medios de comunicación general, de cultura pop, estilo de vida y la familia para posicionar las historias y presentar entrevistas reactivas.
- Artículos aportados y editoriales de opinión

Aporte un editorial de opinión o artículo mensual o semanal que se refiera a una amplia gama de cuestiones de seguridad cibernéti-

ca con énfasis en la protección de los datos y las finanzas personales y las medidas que deben tomar las personas para protegerse contra las distintas amenazas.

Medios de Comunicación Social

- Establezca una entrada de blog semanal al sitio web. Desarrolle un grupo de autores de blog invitados para cubrir diversos temas y ayudar a mantener la necesidad constante de contar con nuevos contenidos. Un calendario editorial ayudará en el enfoque del contenido, pero es importante que sea flexible para permitir la observación oportuna sobre acontecimientos actuales.
- Use Twitter y Facebook para enviar un flujo constante de mensajes tanto proactivos como reactivos. Utilice estos foros para la polinización cruzada y establezca un amplio grupo de expertos y de mayor alcance público.
- Realice chats de Twitter trimestralmente para ayudar a impulsar el mensaje de la campaña y logre la participación de un público en línea para tener debates sobre temas de seguridad cibernética. Los temas a cubrir incluyen la comprensión de la amenaza, el Internet de las cosas, la seguridad cibernética móvil, y la seguridad cibernética de la familia. Invite a las organizaciones aliadas a ser socios oficiales en los chats de Twitter, ampliando así el alcance de la campaña y generar nuevos seguidores.
- Distribuya anuncios de servicio público a través de radiodifusión y medios impresos. La publicidad ambiental (vallas, carteles en buses, etc.) también es un buen método de distribución de anuncios de servicio público.

Métrica

- Visitas a la página/sitio web
- Descargas de contenido
- Seguidores de Facebook y Twitter
- Número de alianzas desarrolladas
- Participantes en eventos (incluyendo presenciales y en línea)
- Cobertura y colocación de los medios de comunicación
- Distribución de los anuncios de servicio público

G

Empresas

El siguiente es un breve resumen de la estrategia de una campaña, la táctica y la métrica para una campaña para los negocios.

Resultados Deseados

- La seguridad cibernética se convierte en una cuestión de ejecutivos de nivel C
- La seguridad se convierte en una cuestión relacionada con el negocio y no solo una cuestión de TI: la comprensión de por qué las empresas deberían emplear prácticas seguras
- Inclusión deliberada de fondos para iniciativas de seguridad cibernética en los presupuestos
- Mejora de la protección de la propiedad intelectual en línea
- Actitud basado en el riesgo/ cambios de comportamiento
- La comprensión de los riesgos a la hora de adoptar nuevas tecnologías y aplicar estrategias para abordarlos

Investigación

Llevar a cabo encuestas para evaluar el grado de preparación en seguridad cibernética de las empresas y sus empleados. Se deben hacer encuestas independientes para pequeñas empresas y empresas más grandes ya que los diferentes recursos (financieros, número de empleados y estructura organizativa) dictan el enfoque de la seguridad cibernética. Utilice estas encuestas como base de encuestas de referencia anual continuas para medir la eficacia de la campaña.

Kit de herramientas de seguridad cibernética para empresas

Los dueños de empresas son personas muy ocupadas. Un kit de herramientas simples con recursos para educarse, educar a sus empleados y empezar a mejorar sus prácticas de seguridad cibernética puede avanzar mucho hacia lograr la participación de los dueños de negocios sobre este tema. En el kit de herramientas entregue:

- Hoja informativa
- Una lista de medidas fáciles de implementar para mejorar de inmediato su situación en seguridad cibernética
- Lista de recursos
- Carteles para el lugar de trabajo
- Banderas Web
- Guía de educación de los empleados
- Muestra de la carta del director ejecutivo a los empleados
- Muestra de la política de seguridad cibernética para el lugar de trabajo que potencialmente incluye temas como:

- Uso de móvil
- El intercambio de información
- El uso de los medios de comunicación social
- Traiga su propio dispositivo (BYOD)

Alianzas

Establezca alianzas estratégicas con organizaciones empresariales e industriales (como el Club Rotario, asociaciones de fabricantes, asociaciones comerciales, asociaciones de gestión de recursos humanos y redes de negocios). Utilice estas organizaciones, en las que los dueños de negocios ya están participando, como un medio para ayudar a difundir información sobre seguridad cibernética. Proporcione un kit de herramientas de campaña que incluye materiales como información sobre la

campaña, un borrador de correo electrónico (a sus interesados), temas de conversación, gráficos, carteles, banderas web, kit de herramientas de negocios y recursos web. Ofrezca entradas de blog mensuales o trimestrales y artículos del boletín de noticias regulares.

Mesas redondas de ejecutivos de negocios en seguridad cibernética

Organice una serie de mesas redondas en seguridad cibernética dirigida específicamente a ejecutivos, propietarios y operadores de 4-6 veces en el transcurso del año. Asóciese con organizaciones como las sociedades de Internet, las sociedades informáticas (ISC (2), APWG, ISOC), y universidades para ofrecer asesoramiento experto en seguridad para pequeñas, medianas y grandes empresas. Provea información sobre las amenazas, historias de empresas que han sido afectadas por amenazas de seguridad cibernética e información acerca de los pasos que las empresas pueden tomar para protegerse. Los posibles temas incluyen:

- La gestión de una red saludable
- Privacidad 101
- Seguridad cibernética: los fundamentos
- Educar a su fuerza de trabajo
- Traiga su propio dispositivo: política
- El panorama de amenazas
- Seguridad cibernética: es su negocio
- Amenazas internas

Oficina de expertos de seguridad cibernética

Tenga como objetivo las organizaciones empresariales para tener oportunidades de hablar sobre el tema de seguridad cibernética. Ofrezca expertos para reuniones mensuales y conferencias anuales. Debata cómo la seguridad en el Internet impacta a negocio y proporcione recursos (sitios web, folletos, oportunidades de discusión de seguimiento) para que las empresas aprendan más.

Medios de comunicación

Concéntrese en revistas y artículos generales de negocios y boletines comerciales de la industria para lanzar historias y ofrecer entrevistas reactivas.

Artículos Aportados – editoriales de opinión

Ofrezca un editorial de opinión o artículo mensual o semanal enfocado en ejecutivos, que cubra una amplia gama de cuestiones de seguridad cibernética empresarial, políticas de trabajo, traiga su propio dispositivo, amenazas internas y construcción de una cultura de seguridad cibernética.

Medios de Comunicación Social

- Establezca una entrada semanal a un blog centrado en negocios a la página web. Desarrolle un grupo de autores de blog invitados para cubrir diversos temas y ayudar a suplir la necesidad constante de contar con nuevos contenidos. Un calendario editorial ayudará en el enfoque de contenido, pero es importante que sea flexible para permitir la observación oportuna sobre los acontecimientos actuales.
- Use Twitter, Facebook y LinkedIn para enviar un flujo constante de mensajes, tanto proactivos como reactivos. Utilice estos foros para la polinización cruzada y establezca un amplio grupo de expertos y de mayor alcance público.
- Realice chats de Twitter trimestralmente para ayudar a impulsar el mensaje de la campaña y logre la participación de un público en línea para tener debates sobre temas de seguridad cibernética. Los temas a cubrir son: la comprensión de la amenaza, el Internet de las cosas, traiga su propio dispositivo y mejores prácticas de seguridad cibernética y privacidad. Invite a las organizaciones aliadas a ser socios oficiales en los chats de Twitter, ampliando así el alcance de la campaña y generar nuevos seguidores.

Métrica

- Visitas a la página/sitio web
- Descargas de contenido
- Seguidores de Facebook, Twitter y LinkedIn
- Número de alianzas desarrolladas
- Participantes en eventos (incluyendo presenciales y en línea)
- Cobertura y colocación de los medios de comunicación

H

Directrices de reuniones

Guía de reuniones y facilitación

Las siguientes directrices proporcionarán un marco para una discusión facilitada.

- *Utilice un facilitador y un tomador de notas*
  - La persona que dirige o facilita la discusión debe poder mantener una postura neutral sobre el tema en discusión. Puede ser útil tener de facilitador a alguien sin un interés personal en el resultado de la discusión.
  - El papel del facilitador es guiar la conversación de tal manera que todos los participantes tengan la oportunidad de ser escuchados. Esta persona también debe poder, en caso necesario, hacer de árbitro, reorientar y hacer que avance la reunión.
  - El tomador de notas debe ser una persona diferente para permitir que el facilitador se centre en la realización de la reunión.

- *Tenga un propósito claro y agenda de la reunión*

  Proporcione una agenda con un conjunto claramente articulado de objetivos para la reunión. Es importante que los participantes en la reunión entiendan cuáles son los objetivos de la reunión para que puedan estar preparados. Envíe la agenda de la reunión y cualquier informe o lectura con mucha anticipación para que todos tengan la oportunidad de prepararse.

- *Establezca reglas básicas para la reunión*
  - Es importante que todos entiendan la manera en que se llevará a cabo la reunión y estén de acuerdo con el conjunto de reglas.
  - Escuche respetuosamente sin interrumpir
  - Respete el punto de vista de otros
  - Permita que todos tengan la oportunidad de hablar
  - Critique las ideas, no las personas

- *Eduque a los participantes*

  Usted puede tener gente de diferentes áreas de experiencia o con diferentes niveles de conocimiento sobre el tema. Provea material de lectura avanzada, pero también dedique un poco de tiempo al inicio de la reunión (o al cambiar temas) para educar a sus participantes en la reunión sobre el tema en cuestión para ayudar a crear una base común de entendimiento. Por ejemplo, al comienzo de la reunión disponga que un experto realice una presentación sobre seguridad cibernética y el impacto en su país o, a medida que analizan las campañas de sensibilización, organice que un profesional de relaciones públicas presente unos elementos de una campaña de sensibilización exitosa.

Medios de comunicación social

Los medios de comunicación social, o medios sociales, son una fantástica manera de bajo costo para llegar al público. Facebook, Twitter y LinkedIn son plataformas que usted debe tener en cuenta para su campaña. Estos canales le permiten estar en contacto permanente con su público, obtener una gran cantidad de seguidores rápidamente, construir una comunidad interesada en la seguridad cibernética, brindar la oportunidad de abordar las cuestiones en tiempo real, posicionarse como un líder de reflexión y responder a las preguntas que su público pueda tener en un foro comunitario. ¡No hay una buena razón para no utilizar los medios de comunicación social!

Consejos para los Medios Sociales

La construcción de una red de medios sociales atractiva puede ser una tarea formidable. Aquí hay algunos consejos para construir su red y atraer a su público de una manera significativa.

- *Tenga un contenido estupendo*

  Los medios sociales no solo tratan de vender su idea o tema; la intención es proporcionar un buen contenido para su público. Además de desarrollar su propio contenido (material de sitio web, entradas de blog, hojas de consejos, infografías, comunicados de prensa y menciones en medios de comunicación), propóngase el hábito de compartir regularmente el contenido relevante de otros (ya sea que se trate de una entidad de gobierno, corporación, reportaje o un particular). Usted será más relevante y generará más seguidores.

- *Construya su red*

  Después de que haya establecido su sitio de medios sociales, invite activamente a las personas a unirse a su red. Haga clic en "Me gusta" (o "Like") en las páginas o actividades de otras organizaciones que son relevantes para la seguridad cibernética y la seguridad en línea. Muy posiblemente otras organizaciones también harán clic en "Me gusta" en su sitio y lo seguirán si usted está dispuesto a apoyar los de estas organizaciones.

- *Involucre a su público en la conversación*

  Haga preguntas en su sitio o actividad. Permita que las personas le respondan. Deje que sus seguidores publiquen preguntas y comentarios y asegúrese de responderles.

- *Sea persistente y publique con frecuencia*

  Tomará tiempo construir su red social. Publique buen contenido a menudo (2-3 veces al día para empezar). Esto le ayudará a construir su red y les dará un motivo a sus seguidores a seguir regresando.

- *Utilice gráficos y vídeos*

  Fotos, gráficos y videos son un muy buen contenido con los que logrará muchos "me gusta" y comentarios.

- *Promueva la polinización cruzada*

  Promueva la polinización cruzada de sus sitios de medios sociales. Conecte con su sitio web (entradas del blog), Facebook, Twitter, LinkedIn e Instagram.

- *Apoye a sus seguidores y organizaciones aliadas*

  Haga una mención del nombre (shout out) de sus organizaciones aliadas cuando anuncien nuevas iniciativas, aparezcan en las noticias o publiquen buen contenido.

- *Use Etiquetas de almohadilla (Hashtags)*

  Las etiquetas de almohadilla (#parapiensaconectate, #paraelbullying, #privacidaddedatos) crean vínculos de búsqueda y ayudan a organizar contenido y discusiones. (A continuación hay un par de recursos que aportan más profundidad al tema de las etiquetas de almohadilla: https://support.twitter.com/articles/49309-using-hashtags-on-twitter y http://mashable.com/2013/10/08/what-is-hashtag/)

Chats en Twitter

Por Emily Eckland, Digital Strategist

Los chats en Twitter son una gran manera de involucrar a su público en línea. Son básicamente una discusión en línea planeada y facilitada. Usted escoge la hora y el tema, invita a unos cuantos expertos que opinen, y luego anuncia a su universo de medios sociales que tendrá esta discusión. El siguiente es un resumen de las preguntas más frecuentes sobre los chats de Twitter, seguido de un par de ejemplos de cómo planear uno.

¿Qué es un chat de Twitter?

Qué: Un chat de Twitter es un debate en línea que se realiza en Twitter y se organiza a través de una etiqueta de almohadilla (#) designada. Los siguientes son ejemplos de etiquetas de almohadilla: #seguridadenlinea, #eleccion, #perritos.

Cómo: La gente sigue el chat mediante la búsqueda de la etiqueta de almohadilla designada. Para participar en el chat, cada tuit debe incluir también la etiqueta de almohadilla designada. Hay sitios web y herramientas que usted puede utilizar para crear una "sala de chat virtual" y organizar sus actividades de Twitter.

Quién: Cualquier persona puede participar en un chat de Twitter. Típicamente hay anfitriones o moderadores y participantes oficiales del chat, pero todos son bienvenidos a la discusión. Por supuesto, para participar también se necesita una cuenta y un usuario (handle) de Twitter (nombre, como @_____).

Por qué: Los chats de Twitter son una manera estupenda, gratis y relativamente fácil de conectarse con gente, aumentar la conciencia de marca y transmitir un mensaje en una plataforma social.

Otras preguntas frecuentes:

¿Cómo creo la etiqueta de almohadilla para mi chat?

La etiqueta de almohadilla es totalmente su decisión, pero es útil incluir la palabra "chat" o "hablar" para identificar que se trata de un chat de Twitter, y no simplemente una etiqueta de almohadilla. (Ejemplos: #TechTalk, #SafetyChat). También puede pensar en usar el nombre de su organización o un acrónimo para construir la identidad de marca. (Por ejemplo, si su organización es la Asociación de Amantes de Gatos, es posible que desee utilizar #AAGChat para la etiqueta de almohadilla.) También es importante revisar si la etiqueta de almohadilla que planea utilizar está siendo utilizada por otra organización. Usted puede hacer esto mediante la búsqueda en la etiqueta de almohadilla en Twitter y ver si hay resultados.

¿Cuánto duran los chats de Twitter?

Twitter es una plataforma rápida, fluida y los chats pasan muy rápidamente. La mayoría de los chats de Twitter son típicamente de una hora o una hora y 30 minutos. Sería difícil de sostener un chat de Twitter en 30 minutos.

¿Cómo debo formatear mi chat de Twitter?

Una gran parte de un chat de Twitter es la conexión con su "público". Los chats de Twitter pueden ser formateados en varias formas diferentes, pero los más populares les hacen una serie de preguntas a sus panelistas y luego le dan tiempo al "público" para que les haga preguntas a sus invitados. Usted también puede mantener un chat sin panelistas y hacerle sus preguntas a todos los participantes en el chat.

Usted debe comenzar cada chat con unos tuits introductorios que repasan el tema y permiten que usted y sus panelistas se presenten ante su "público". Después de eso, el moderador puede empezar a hacer preguntas. Para un chat de una hora con 3-5 panelistas, normalmente de 8-10 preguntas son suficientes para estas y para dejar tiempo para las preguntas del público. Puede tomar de 3-5 minutos para que todos respondan a una pregunta. Es útil tener algunas preguntas adicionales que usted pueda utilizar en caso de tener tiempo de sobra.
Un tuit tiene 140 caracteres, que no es mucho espacio para entregar mi mensaje. ¿Qué pasa si tengo que decir más?
¡No se sienta presionado por tratar de lograr de comunicar toda la información en 140 caracteres! Puede utilizar varios tuits para responder a una pregunta (¡solo asegúrese de incluir la etiqueta de almohadilla!). Es una buena idea escribir sus respuestas de antemano y tener una lista de mensajes o URL prácticos que desee compartir durante el chat.

Twitter parece un poco como una algarabía. ¿Hay alguna manera de crear un chat más ordenado?

Habrá gente tuiteando al mismo tiempo, de modo que puede que las respuestas no aparezcan de forma consecutiva, pero esa es la naturaleza de Twitter. Hay algunas maneras de controlar el flujo del chat, como crear un orden de los tuits para sus panelistas. También ayuda que todo el mundo le ponga etiquetas a las preguntas y respuestas. (Por ejemplo: P1, R1, etc.)

¿Debo estar en la misma habitación que mis participantes del chat de Twitter?

No, y ¡eso es lo bueno de los medios de comunicación social! En cualquier chat, usted podría tener participantes de todo el mundo, en diferentes zonas horarias. Sin embargo, usted puede configurar una línea telefónica de conferencia para utilizar en el chat. Algunas personas usan una línea de conferencia para establecer un orden de tuiteo para panelistas, o para ayudar a abordar las preguntas del público, y para la resolución de problemas en general.

¿Cómo y cuándo debo promover mi chat de Twitter?

Usted puede promover el chat como lo desee, pero vale la pena tener un punto de referencia para que la gente vea todos los detalles de su chat. Esto puede ser una página en su sitio web, un listado en un sitio web de eventos como Eventbrite, o incluso otros medios de comunicación social como Facebook, LinkedIn y Google+. Sería bueno promover el chat en todas formas que sean posibles: correo electrónico, boletines electrónicos, redes sociales (como Facebook, LinkedIn, Google+), en su página web, etc.

Dado que Twitter es tan fluido, usted puede promover el chat en cualquier momento. Pero por lo general las personas empiezan a promoverlo una semana antes y mucho más en los días previos al chat. También puede aprovechar las herramientas como HootSuite, TweetDeck y otros para programar tuits promocionales por adelantado.

¿Qué significa RT y MT?

RT es la abreviatura de re-tuit y aparece en Twitter y en otras plataformas como un ícono con dos flechas. Usted puede RT (esencialmente, copiar lo que un usuario de Twitter publicó y ponerlo a disposición de sus seguidores) pulsando el icono en Twitter o mediante la creación de un nuevo mensaje, copiando el mensaje que desea re-tuitear y escribiendo "RT@ (el usuario de Twitter que usted está re-tuiteando)" de antemano. MT es la abreviatura de modificación de tuit, que es un tuit que usted desea re-tuitear y agregarle su propio mensaje antes de publicar. Muchas veces, un tuit original más su propio mensaje delante de este sumarán más de 140 caracteres, por lo que tendrá que editarlo antes de publicar.

Ejemplo de un RT:

Tuit Original: @PiesFelices: me encanta bailar y me hace muy feliz.
Tuit RT: @AmoBailar: ¡A mí también! ¿Cuál es su paso de baile favorito? RT @PiesFelices: me encanta bailar y me hace muy feliz.

Ejemplo de una MT:

Tuit Original: @AmanteHamburguesa: Los mejores ingredientes adicionales de hamburguesa de todos los tiempos son huevos fritos, aguacate, tocino, queso, preferiblemente gouda ahumado. #hamburguesa #alimentame
Tuit de MT: @CarneyPan: ¡Se le olvidaron los pepinillos, cebolla salteada! MT@ AmanteHamburguesa: Los mejores ingredientes adicionales de hamburguesa de todos los tiempos son huevos fritos, aguacate, tocino, queso.

¿Hay maneras de hacerle seguimiento al éxito de mis chats?

Sí, hay varios servicios gratuitos como: Topsy, Tweetchup y Buffer. También hay otros servicios de análisis que son por suscripción, como SimplyMeasured, Crowdbooster y Twitonomy. Si utiliza un acortador de URL como Bit.ly, también podrá hacerle seguimiento a cuántos clics recibieron sus tuits con bit.ly mediante la revisión de su cuenta.

¿Qué otras mejores prácticas debo conocer?

No dude en re-tuit (RT) las respuestas que le gusten de otros participantes. Y añada una etiqueta de almohadilla (#) a palabras clave comunes, ya que les permitirá localizarlas en Twitter y permitirán una mayor visibilidad.

Ejemplos de guiones de chats de Twitter

Guión#1: Chat de Twitter Seguridad en línea en el hogar

La información simulada, que incluye las preguntas del moderador y las respuestas de un panelista, está en azul.

Chat de Twitter Seguridad en línea en el hogar #ChatCiberSeguro [INSERTAR FECHA, HORA, ETC.]			
Marca	**Organizaciones**	**Usuarios de Twitter**	**Páginas web de la organización**
Tema/Etiquetas de almohadilla	Seguridad general en línea Únase a _____ mientras discutimos _____. Aprenda ____, _____ y ____ en este chat.		
Panelistas	Moderador: @Moderador Panelistas: @Panelista1		

Tuits promocionales para enviar antes y durante el chat	
Twitter	Únase __, _____, ____ para un chat de #Twitter ___en ___. ¡Utilice #___ para unirse!
	Aprenda _____ en nuestra _____ chat de #Twitter en _____ en __. ¡Utilice #____ para unirse!
Marca en Facebook	Denos un Me gusta en #Facebook para más:
Marca en Twitter	Manténgase conectado después de nuestro chat de #Twitter siguiendo _____, _____, _____
Info adicional	Manténgase informado y obtenga consejos _____ aquí:

Tuits de bienvenida y presentación	
2:50 p.m. ET	¡Solo 10 minutos hasta que comience nuestro _____ chat de #Twitter! ¡Esperamos que se conecte a nosotros! ¡Utilice _____ para conectarse!
3:00 p.m. ET PRESENTACIÓN	@Moderador: ¡Bienvenido a nuestro chat #seguridadenlinea de #Twitter! #ChatCiberSeguro

3:00 p.m. ET
PRESENTACIÓN

@Moderador: Hoy hablaremos acerca de las maneras en que usted y su familia pueden estar seguros #enlinea. #ChatCiberSeguro

@Moderador: Nuestros invitados son _____ #ChatCiberSeguro

@Moderador: ¡Pidámosles que se presenten! #ChatCiberSeguro

@Panelista1: ¡Hola! Somos _____ y nuestra misión es _____.#ChatCiberSeguro

@Panelista1: Estamos encantados de ser parte de esta serie en este chat de #Twitter y estamos listos a ayudar a empoderar a las personas con recursos para mantenerse más seguros en línea. #ChatCiberSeguro

(Permita que otros panelistas se presenten.)

@Moderador: ¡Excelente! Comencemos. Daremos inicio con una pregunta amplia, pero importante hoy. #ChatCiberSeguro

(Moderador debe reconocer y darle la bienvenida a las personas que respondan a este tuit.)

3:05 p.m. ET
PREGUNTA 1

@Moderador: ¡Excelente! Comencemos. Daremos inicio con una pregunta amplia, pero importante hoy. #ChatCiberSeguro

@Moderador: P1: ¿Cuáles son 3 cosas simples que podemos hacer para mantenernos #seguros en línea todos los días? #ChatCiberSeguro

@Panelista1: R1 1) Asegúrese de que todos los dispositivos tengan el último #software, sistema operativo, antivirus, navegadores web y aplicaciones. #ChatCiberSeguro

@Panelista1: R1 2) No haga clic en el URL o correos electrónicos sospechosos En caso de duda, ¡bótelos a la basura! #ChatCiberSeguro

@Panelista1: R1 3) Tenga cuidado al usar #WiFi público, no asegurado. No tenga actividad en bancos, tiendas, o introduzca información personal #Enlinea. #ChatCiberSeguro

(Espere unos 3 minutos para que la gente responda y el moderador/panelistas puedan re-tuitear las mejores respuestas/llamar la atención sobre buenas respuestas de los participantes)

3:10 p.m. ET
PREGUNTA 2

@Moderador: ¡Vaya! ¡Estas fueron unas respuestas fantásticas! Gracias a todos por compartir estos grandes consejos. #ChatCiberSeguro

@Moderador: @Panelista1 y otros mencionaron un buen punto sobre hacer clic en enlaces sospechosos. #ChatCiberSeguro

@Moderador: P2 ¿Cuáles son algunas maneras de detectar fraudes y posibles ataques #phishing? #ChatCiberSeguro

@Panelista1: R2: Tenga cuidado con los correos electrónicos que soliciten información personal o le piden que actúe con rapidez. Faltas de ortografía y errores tipográficos son pistas, también. #ChatCiberSeguro

@Panelista1: R2: Recuerde, si algo suena demasiado bueno para ser verdad, ¡probablemente lo es! #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:14 p.m. ET
PREGUNTA 3

@Moderador: Cambiemos la marcha un poco y pasemos a otro aspecto importante: #seguridadenlinea y familias. #ChatCiberSeguro

@Moderador: Muchos niños tienen sus propios dispositivos y computadoras #moviles, de modo que el concepto de un computador en la habitación familiar puede no ser válido. #ChatCiberSeguro

@Moderador: P3: ¿Hay cosas importantes que los #padres deban hacer cumplir cuando sus #niños están #enlinea? #ChatCiberSeguro

@Panelista1: R3 Ayude a los niños a identificar sitios creíbles y seguros y sean cautos al hacer clic, descargar y publicar contenido. #ChatCiberSeguro

@Panelista1: R3 Conozca las características de protección y #privacidad de sus #dispositivos y los sitios web y #apps que sus hijos utilizan. Su PSI puede ayudar, también. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:18 p.m. ET
PREGUNTA 4

@Moderador: Hablando de estar #enlinea en casa - nuestra siguiente pregunta puede parecer básica, pero aún así ¡es bueno que todo el mundo la conozca! #ChatCiberSeguro

@Moderador: P4: ¿Cómo puede asegurarse de que su red #WiFi en casa es segura? #ChatCiberSeguro

@Panelista1: R4: Asegúrese de que el router es WPA2 o WPA-PSAK, que tienen autenticación/cifrado más fuerte. WEP no es tan seguro. #ChatCiberSeguro

@Panelista1: R4: Cambie el SSID (nombre) en el router pero no utilice nombres personales, como el "WIFI de Ann." Use una mezcla de números/letras. #ChatCiberSeguro

@Panelista1: R4: Cambie la contraseña y hágala fuerte y larga - utilizando una combinación de letras mayúsculas/minúsculas y números y símbolos. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:22 p.m. ET
PREGUNTA 5

@Moderador: Bueno, es hora de cambiar un poco las cosas. La siguiente pregunta es "verdadero o falso" #ChatCiberSeguro

@Moderador: P5: ¿Verdadero o falso: Todos #dispositivos habilitados para #Internet necesitan una protección anti-virus? #ChatCiberSeguro

@Panelista1: R5: ¡Verdadero! Los teléfonos móviles, tabletas y otros dispositivos son vulnerables a las amenazas. Usted debe protegerlos como lo haría con su computadora. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:26 p.m. ET
PREGUNTA 6

@Moderador: P6: ¿Qué es lo más importante a recordar para mantenerse seguros en línea en dispositivos #móviles? #ChatCiberSeguro

@Panelista1: R6: ¡Lea la política de #privacidad y conozca qué información recoge una aplicación (contactos, fotos, ubicación) antes de descargarla! #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:30 p.m. ET
PREGUNTA 7

@Moderador: Pasemos a otro tema básico, pero muy importante: #contraseñas. #ChatCiberSeguro

@Moderador: P7: ¿Cuáles son los elementos de una buena #contraseña y hay otras tecnologías que hacen que sea más seguro? #ChatCiberSeguro

@Panelista1: R7: Los elementos de una buena contraseña: Larga y fuerte con una mezcla de letras mayúsculas/minúsculas, números y símbolos #ChatCiberSeguro

@Panelista1: R7: Ejemplo: @$!llygRAY3l3ph@^t es más seguro que "asillygrayelephant". #ChatCiberSeguro

@Panelista1: R7: Muchos sitios web ofrecen una protección más allá de la contraseña, como una autenticación de 2 pasos - una mejor manera de proteger las cuentas #enlinea. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:34 p.m. ET
PREGUNTA 8

@Moderador: Hemos mencionado esto antes, pero revisemos la noción de usar #WiFi pública de forma segura. #ChatCiberSeguro

@Moderador: P8: ¿Cómo detecta usted una #WiFi no segura y cuáles sitios web debe evitar mientras la usa?

@Panelista1: R8: #WiFi no asegurada no requiere que escriba una contraseña antes de acceder a ella. #ChatCiberSeguro

@Panelista1: R8: #WiFi gratuito en cafeterías, aeropuertos, hoteles, etc. por lo general no es segura. #ChatCiberSeguro

@Panelista1: R8: Si está usando #WiFi no seguro, no debe visitar sitios web que requieren que usted escriba su nombre de usuario y contraseña. #ChatCiberSeguro

@Panelista1: R8: Ejemplos de esto son el correo electrónico, redes sociales, sitios web de viajes. Y nunca ingrese información de la tarjeta de crédito o financiera. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:38 p.m. ET
PREGUNTA 9

@Moderador: La siguiente pregunta se trata de algo que preocupa a la mayoría de las personas: #ciberdelito #ChatCiberSeguro

@Moderador: P9: Si usted descubre que es víctima de #ciberdelito, ¿dónde debe denunciarlo y pedir ayuda? #ChatCiberSeguro

@Panelista1: P9: Notifique a su agencia de policía local y el Centro de Quejas de Delitos en #Internet: http://www.ic3.gov/default.aspx. #ChatCiberSeguro

@Panelista1: P9: Si usted es una víctima de #robodeidentidad, notifique a sus instituciones financieras de inmediato y póngase en contacto con las agencias de crédito. #ChatCiberSeguro

@Panelista1: P9: Recoja y mantenga cualquier tipo de pruebas (extractos de la tarjeta de crédito, correos electrónicos, etc.), cambie contraseñas y actualice sus dispositivos. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:42 p.m. ET
PREGUNTA 10

@Moderador: Tenemos tiempo para una última pregunta antes de abrirlo a nuestro público... #ChatCiberSeguro

@Moderador: P10: ¿Qué recursos #seguridadenlinea recomienda usted para personas que quieren #Protegerse y a sus familias? #ChatCiberSeguro

@Panelista1 R10: El sitio web para consumidores de la FTC, On-GuardOnline.gov tiene grandes recursos. #ChatCiberSeguro

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:45 p.m. ET

@Moderador: Ahora es el turno de nuestros invitados: ¿Alguien tiene una pregunta de #seguridadenlinea que les gustaría hacer? #cybersafetalk

@Panelista1: ¡Asegúrese de visitar nuestro sitio web _____ para obtener más información útil! #ChatCiberSeguro

3:55 p.m. ET
CIERRE

@Moderador: ¡Parece que eso es todo el tiempo que tenemos para hoy! ¿Nuestros panelistas tienen algo más que añadir? #ChatCiberSeguro

@Moderador: Gracias por acompañarnos en nuestro _____ chat de Twitter! #ChatCiberSeguro

@Moderador: Síganos en _____ para nuestro próximo chat de #Twitter en _____ # ChatCiberSeguro.

Ejemplos de guiones de chats de Twitter
Guión #2: Seguridad en línea para pequeñas empresas
La información simulada, que incluye las preguntas del moderador y las respuestas de un panelista, está en azul.

Chat de Twitter Mantener su pequeña empresa segura en linea #chatpequeñaempresa [INSERTAR FECHA, HORA.]			
Marca	**Organizaciones**	**Facebook**	**Twitter**
Tema / Etiquetas de almohadilla	Pequeñas empresas y seguridad en línea Únase a _____ mientras discutimos _____ . Aprenda ____, _____ y ____ en este chat. #_____		
Panelistas	Moderador: @Moderador Panelistas: @Panelistas		

Tuits promocionales para enviar Antes y durante el chat

Twitter	Únase __, _____, ____ para un chat de #Twitter ___ en ___. ¡Utilice #___ a unirse!
	Aprenda _____ en nuestra _____ chat de #Twitter _____ en __. ¡Utilice #____ a unirse!
Marca en Facebook	Denos un Me gusta en #Facebook para más:___ #chatpequeñaempresa
Marca en Twitter	Manténgase conectado después de nuestro chat en #Twitter siguiendo _____, _____, _____ #chatpequeñaempresa
Info. adicional	Manténgase informado y obtenga consejos #seguridadenlínea para su pequeño negocio aquí: ((URL a nuestros sitios web)) #chatpequeñaempresa

Tuits de bienvenida y presentación

2:50 p.m. ET	¡Solo 10 minutos hasta que comience el chat de Twitter #seguridadenlinea #pequeñaempresa! Utilice #chatpequeñaempresa para unirse!
3:00 p.m. ET	@Moderador: ¡Bienvenido a nuestro chat de #Twitter #seguridadenlinea #pequeñaempresa! #chatpequeñaempresa
	@Moderador: Hoy hablaremos sobre maneras de mantener su seguridad en línea de la pequeña empresa. #chatpequeñaempresa
	@Moderador: Nuestros invitados son _____ #chatpequeñaempresa

@Moderador: ¡Pidámosles que se presenten! #chatpequeñaempresa

@Panelista1: ¡Hola! Somos _____ y nuestra misión es _____. #chatpequeñaempresa

@Panelista1: Estamos encantados de ser parte de este chat de #Twitter y estamos listos a ayudar a empoderar a las personas con recursos para mantenerse seguros en línea. #chatpequeñaempresa

(Permita que otros panelistas se presenten.)

@Moderador: ¡Fantástico! ¿Quién más se ha unido a nuestro #ChatCiberSeguro hoy?

(El Moderador debe reconocer y darle la bienvenida a las personas que respondan a este tuit.)

3:05 p.m. ET
PREGUNTA 1

@Moderador: ¡Comencemos! Aquí está nuestra primera pregunta... #chatpequeñaempresa

@Moderador: P1: ¿Qué es lo mejor que los propietarios #pequeñaempresa pueden hacer para proteger a la empresa/empleados/clientes de las amenazas #enlinea? #chatpequeñaempresa

@Panelista1: R1: Asegúrese de que todos los dispositivos tengan los últimos sistemas operativos, software, antivirus, aplicaciones y navegadores web. ¡Actualice regularmente! #chatpequeñaempresa

(Espere unos 3 minutos para que la gente responda y re-tuitee las mejores respuestas/llame la atención sobre buenas respuestas de los participantes)

3:10 p.m. ET
PREGUNTA 2

@Moderador: ¡Vaya! Estas fueron unas respuestas fantásticas!

@Moderador: Aquí está la P2: ¿Cómo más puede mantenerse una #pequeñaempresa segura en línea? #chatpequeñaempresa

@Panelista1: R2: #Pequeñaempresa debe evaluar sus riesgos, crear un plan de #ciberseguridad y capacitar a los empleados para tener buenas prácticas en línea. #chatpequeñaempresa

@Panelista1: R2: Los empleados son el eslabón más débil: educar sobre seguridad en Internet, capacitar a tener cuidado con los archivos adjuntos de correo electrónico y enlaces de fuentes desconocidas. #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:14 p.m. ET
PREGUNTA 3

@Moderador: P3: Protección de los clientes y ganarse la confianza es fundamental para #pequeñaempresa. @Panelista1 ¿Cómo se logra? #chatpequeñaempresa

@Panelista1: R3: Tener una política de #privacidad, saber qué información personal tiene, cómo lo almacena y quién tiene acceso a ella. #chatpequeñaempresa

@Panelista1: R3: También, elimine datos que no necesita y mantenga información personal segura. #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:18 p.m. ET
PREGUNTA 4

@Moderador: P4: Muchas veces, los dueños de #pequeñaempresa piensan que son demasiado pequeños para ser un objetivo para #ciberdelincuentes. ¿Deben creer esto? #chatpequeñaempresa

@Panelista1: R4: Es importante que todo el mundo entienda - incluyendo #pequeñaempresa - que podrían ser blanco de un ataque #ciber. #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:21 p.m. ET
PREGUNTA 5

@Moderador: P5: Si los propietarios de #pequeñaempresa sí encuentran una violación o se convierten en una víctima de #ciberdelito, dónde deben denunciar el incidente? #chatpequeñaempresa

@Panelista1: R5: Denuncie los incidentes al Equipo de Respuesta a Emergencias de Computación de los EE.UU. (@USCERT_gov) en: https://forms.us-cert.gov/report/ #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:25 p.m. ET
PREGUNTA 6

@Moderador: Como mencionamos antes, es una buena idea que #pequeñaempresa cree un plan #ciberseguridad. #chatpequeñaempresa

@Moderador: P6: Panelistas, pueden darnos algunos elementos de un plan #ciberseguridad? #chatpequeñaempresa

@Panelista1: R6: Un plan #ciberseguridad integral se centra en 3 áreas clave: Prevención, resolución y restitución #chatpequeñaempresa

@Panelista1: R6: El @FCC tiene un Planeador #Ciber #pequeñaempresa que puede ayudar: http://www.fcc.gov/cyberplanner #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:29 p.m. ET
PREGUNTA 7

@Moderador: Regresemos a hablar de los empleados. #chatpequeñaempresa

@Moderador: P7: ¿Qué pueden hacer los propietarios #pequeñaempresa para concienciar sobre #seguridadenlinea en su oficina? #chatpequeñaempresa

@Panelista1: R7: Capacite a sus empleados y enséñeles buenos hábitos #seguridadenlinea. #chatpequeñaempresa

@Panelista1: R7: Usted también debe alentar a los empleados a hablar si notan algo mal. #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:33 p.m. ET
PREGUNTA 8

@Moderador: Traiga su propio #dispositivo es cada vez más popular en el lugar de trabajo. #chatpequeñaempresa

@Moderador: P8: ¿Qué necesitan saber los propietarios #pequeñaempresa sobre traer su propio dispositivo (BYOD)? #chatpequeñaempresa

@Panelista1: R8: Independientemente de #BYOD, es una buena idea tener una política de seguridad formal por escrito #Internet para los empleados. #chatpequeñaempresa

@Panelista1: R8: Dispositivos de los empleados deben tener siempre las últimas actualizaciones de software, sistemas operativos, navegadores web, protección antivirus, navegadores y aplicaciones web. #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:36 p.m. ET
PREGUNTA 9

@Moderador: #Phishing y la ingeniería social son herramientas comunes que utilizan #ciberdelincuentes

@Moderador: P9: ¿Cuáles son algunas maneras de #phishing y qué deberían hacer los propietarios #pequeñaempresa para denunciarlo? #chatpequeñaempresa

@Panelista1: R9: Errores tipográficos y faltas de ortografía son signos comunes de #phishing. #chatpequeñaempresa

@Panelista11: R9: Nunca haga clic en una URL sospechoso. En su lugar, escriba la dirección URL en su navegador o use un motor de búsqueda para encontrar la página web. #chatpequeñaempresa

@Panelista1: R9: Usted puede denunciar el #phishing remitiendo el #email a: spam@uce.gov #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:39 p.m. ET
PREGUNTA 10

@Moderador: P10: ¿Qué otros recursos #seguridadenlinea recomiendan para #pequeñaempresa? #chatpequeñaempresa

@Panelista1: R10: La Cámara de Comercio de Estados Unidos (@CommerceGov) tiene este kit de herramientas para #pequeñaempresa: https://www.uschamber.com/issue-brief/Internet-security-essentials-business-20 #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:42 p.m. ET

@Moderador: Ahora es el turno de nuestros invitados: ¿Alguien tiene una pregunta que les gustaría hacerles a nuestro panelistas? #chatpequeñaempresa

(Re-tuitee las mejores respuestas/llame la atención a las buenas respuestas de los participantes)

3:55 p.m. ET
CIERRE

@Moderador: ¡Parece que eso es todo el tiempo que tenemos para hoy! @_____, @_____, @_____ algo que añadir? #chatpequeñaempresa

@Panelista: ¡Gracias por recibirnos y por moderar un chat maravilloso, @Moderador! #chatpequeñaempresa

@Moderador: ¡Gracias por acompañarnos en un Chat de Twitter #seguridadenlinea para #pequeñaempresa! #chatpequeñaempresa

@Moderador: Síganos en _____ para nuestro próximo chat de #Twitter en _____. #chatpequeñaempresa.

Recursos de chat de Twitter

Plataformas Twitter

Usted por supuesto puede acceder a su(s) cuenta(s) de Twitter en Twitter.com, pero aquí hay una lista de clientes de Twitter disponibles para su descarga. Todos ellos son gratuitos, con características adicionales que están disponibles por un costo:

Buffer
https://bufferapp.com/

Hootsuite
https://hootsuite.com/

Janetter
http://janetter.net/

Sobees
(solo para dispositivos Windows)
http://www.sobees.com/social-media-clients

Tweetdeck (propiedad de Twitter):
https://about.twitter.com/products/tweetdeck

Twitterrific
(solo para dispositivos Apple)
http://twitterrific.com/

Herramientas para crear salas virtuales de chat

Muchas de ellas requieren de iniciar sesión y/u obtener acceso a su cuenta de Twitter. La mayoría contiene un acortador de URL automática y añadirá automáticamente la etiqueta de almohadilla designada en sus tuits:

Nurph:
http://nurph.com/

Tchat.io:
http://www.tchat.io/

Tweetchat:
http://tweetchat.com

Twubs:
http://twubs.com/

Analytics Tools

Muchos de estos servicios son gratuitos u ofrecen pruebas gratuitas, pero tienen características adicionales que vienen con una suscripción:

Buffer:
https://bufferapp.com/

Crowdbooster:
http://crowdbooster.com/

Simply Measured:
http://simplymeasured.com/

Topsy:
http://topsy.com/

Tweetchip:
http://tweetchup.com/

Twitter (Must advertise with Twitter or install code within your website):
https://analytics.twitter.com/about

Twitonomy:
http://www.twitonomy.com/

URL Shorteners

Estos servicios también ofrecen análisis, de modo que se puede ver cuántas personas han visitado una URL específica que usted promovió durante un chat de Twitter.

Bitly:
https://bitly.com/

Google:
https://goo.gl/w

J

Infografías

Las infografías son una gran manera de contar una historia utilizando una compleja red de datos y son mucho más interesantes y atractivas a la vista que los gráficos tradicionales. Debido a su encanto visual son un excelente contenido de medios sociales que se comparten una y otra vez.
Estas infografías son buenos ejemplos de cómo utilizar datos para contar la historia de seguridad cibernética a diferentes públicos.

Público En General

Hábitos de navegación y preocupaciones en línea/móvil de Canadá (McAfee)
(Canadian Online/Mobile Surfing Habits and Concerns)
http://www.computerdealernews.com/news/mcafee-adds-applock-to-mobile-security-offering/11243

Es la época que tener cuidado: Evite las 12 estafas de los días de fiesta (McAfee)
('Tis the Season to Be Careful: Avoid the 12 Scams of the Holidays)
http://promos.mcafee.com/offer.aspx?id=565846&cid=131941

Juventud y Familia

La vida de seguridad cibernética de la generación del milenio (National Cyber Security Alliance)
(The Cybersecurity Lives of Millenials)
http://staysafeonline.org/stay-safe-online/resources/the-cybersecurity-lives-of-millennials-infographic

Control parental: Una experiencia en línea segura para sus hijos (Kaspersky)
(Parental Control: A Safe and Secure online experience for your kids)
http://usa.kaspersky.com/internet-security-center/infographics/kids-online

Educación

Estado de la educación cibernética de Estados Unidos (National Cyber Security Alliance)
(State of U.S. Cyber Education)
Http://staysafeonline.org/stay-safe-online/resources/

Negocios

¿Cómo se preparan las empresas de tecnología para ataques cibernéticos (Silicon Valley Bank)
(How Tech Companies Prepare for Cyber Attacks)
http://www.svb.com/cybersecurity-report-infographic/

Seguridad de tecnología de la información (DELL)
(IT Security)
http://www.infographicsarchive.com/tech-and-gadgets/it-security/#prettyphoto

¿Cuánto Cuestan Mis Datos? (Symantec)
http://www.symantec.com/connect/es/blogs/cuanto-cuestan-los-datos-robados-y-servicios-de-ataque-en-el-mercado-clandestino

Negocio Riesgoso: Las amenazas de malware de software sin licencia (Business Software Alliance)
(Risky Business: Malware Threats from Unlicensed Software)
http://globalstudy.bsa.org/2013/malware/ig_malware_en.pdf
http://globalstudy.bsa.org/2013/malware/ig_malware_es.pdf

K

Recursos

Público en General

PARA. PIENSA. CONÉCTATE.

www.stopthinkconnect.org

PARA. PIENSA. CONÉCTATE. Ofrece sugerencias y consejos para los padres sobre la seguridad en Internet, el acoso cibernético, los dispositivos móviles y los videojuegos. Además de los materiales en idioma inglés, hay recursos limitados disponibles en español, portugués, francés, japonés y ruso.
http://stopthinkconnect.org/resources/

SAFE INTERNET DAY

http://www.saferinternet.org/safer-internet-day

Día del Internet Segura (DIS) es organizado por Insafe en febrero de cada año a fin de promover un uso más seguro y responsable de la tecnología y de los móviles en línea, especialmente entre los niños y jóvenes de todo el mundo.

Español
http://www.saferinternet.org/resources

Francés
http://www.saferinternet.org/resources

Portugués
http://www.saferinternet.org/resources

MICROSOFT

http://www.microsoft.com/security/default.aspx

Microsoft es el líder de la industria en materia de seguridad en línea y la educación del consumidor en seguridad. Han desarrollado una completa gama de materiales y recursos que incluyen información para padres y niños y niñas sobre la seguridad en Internet, protección en Internet y la privacidad digital. Los recursos incluyen contenidos en línea y descargable, PowerPoint, libros electrónicos (para adolescentes) y vídeos. Los materiales están disponibles en numerosos idiomas, incluyendo:

Español
http://www.microsoft.com/es-xl/security/default.aspx

Francés
http://www.microsoft.com/fr-fr/security/default.aspx

Portugués
http://www.microsoft.com/pt-pt/security/default.aspx

FACEBOOK

https://www.facebook.com/safety

Facebook se ha comprometido con contribuir a la seguridad en línea para los jóvenes. Una variedad de herramientas y recursos están disponibles para ayudar a los padres a navegar la configuración de la cuenta y de privacidad, ayudar a los padres a entender los medios sociales y cómo ayudar a sus hijos adolescentes a evitar las trampas de los medios sociales y la gestión de una vida digital.

NORTON POR SYMANTEC

http://us.norton.com/family-resources/

El centro de recursos de la familia de Norton tiene consejos para padres, adolescentes y niños y niñas. Norton también tiene una Guía de seguridad en línea para la familia descargable disponible en varios idiomas.

Inglés
http://us.norton.com/online-safety-guide

Español
http://now.symassets.com/now/en/pu/images/promotions/onlinesafetyguide/br-00386-sl_familyonlinesafetyguide_3rded.pdf

Francés
http://www.symantec.com/content/en/us/home_homeoffice/media/theme/parentresources/fosg-french.pdf

MCAFEE

http://www.thinkbeforeyoulinkinschool.com/family

GOOGLE

https://www.google.com/safetycenter/

El centro de seguridad de Google cuenta con herramientas y recursos para las familias que cubren la seguridad en línea. Además de la seguridad en línea y guía de seguridad básica, el centro de recursos tiene información sobre cómo configurar filtros de búsqueda amigables a la familia, utilizar las calificaciones de las aplicaciones, y la forma de controlar el acceso a los juegos y aplicaciones aprobadas.

Jóvenes, Padres y Educadores

Los siguientes recursos tienen excelentes materiales para padres y jóvenes. Excepto donde se indique, todos los recursos que están disponibles de forma gratuita (todos los recursos corporativos incluidos en esta lista son gratis). Estos recursos están en inglés; algunos están disponibles en otros idiomas, incluyendo español, francés y portugués.

INTERNET WATCH FOUNDATION

www.iwf.org.uk

Internet Watch Foundation (IWF) se enfoca específicamente en la lucha contra el abuso de menores y de imágenes criminalmente obscenas alojadas en el Reino Unido y alrededor del mundo. IWF trabaja en asociación con la industria en línea, la policía, el gobierno y los socios internacionales. Es una obra de caridad y una entidad de autorregulación, con más de 100 miembros de la industria en línea.

Español
www.iwf.org.uk

CHILDNET INTERNATIONAL

www.childnet.com

Childnet International es una organización sin fines de lucro que trabaja en colaboración con otros alrededor del mundo para ayudar a hacer de Internet un lugar excelente y seguro para los niños. El sitio web aloja un número de recursos recomendados para jóvenes, padres, cuidadores y profesores.

PROTECIONONLINE.COM

http://www.protecciononline.com

Protección Online es un emprendimiento realizado por un equipo humano con amplios conocimientos en el campo de recursos, herramientas, navegación y protección en la Web que nace con el objetivo de brindar las mejores recomendaciones para que el uso de las nuevas tecnologías sean más agradable y segura a través de la promoción de buenos hábitos de conducta, prácticas de cyberciudadanía y acciones que minimicen el peligro en la Red.

INSTITUTO DE SEGURIDAD DE FAMILIA EN LÍNEA (FOSI)

(Family Online Safety Institute)
www.fosi.org

FOSI es una organización no gubernamental, con sede en Estados Unidos y el Reino Unido, que se centra en la seguridad de los niños, niñas y las familias. Tienen una gran cantidad de recursos para que los padres aprendan sobre la seguridad en línea, la privacidad y la crianza de niños y niñas digitales. Además del desarrollo de recursos educativos, FOSI también desarrolla informes sobre políticas y lleva a cabo investigaciones.

IKEEPSAFE

iKeepsafe es una ONG con sede en Estados Unidos centrada en la seguridad en línea, la ciudadanía digital y la privacidad de los niños y niñas. Hay recursos gratuitos disponibles para los padres que incluyen:

Faux Paw, una serie de libros digitales para niños y niñas pequeños
http://www.ikeepsafe.org/parents/fauxpaw/

BEAPRO aplicaciones para Facebook y Android
Esta aplicación les ayuda a los padres a evaluar el comportamiento digital en su hogar, ofrece consejos de expertos y recursos, y consejos sobre cómo pasar información a los niños y niñas.
http://www.ikeepsafe.org/beapro-parent-app/

Guía de medios sociales
http://ikeepcurrent.org/

Videos
http://www.ikeepsafe.org/videos/

COMMON SENSE MEDIA

www.commonsensemedia.org

Common Sense Media es una ONG con sede en Estados Unidos cuya misión de "empoderar a los padres, los maestros y los formuladores de políticas al proporcionar información imparcial, asesoramiento de confianza y herramientas innovadoras para ayudarles a aprovechar el poder de los medios de comu-

nicación y la tecnología como una fuerza positiva en la vida de todos los niños y niñas".

Common Sense Media les proporciona orientación a los padres sobre una variedad de temas digitales, incluyendo una lista de aplicaciones maravillosas apropiadas a la edad, el acoso cibernético, el tiempo de pantalla, la privacidad y la seguridad en Internet y los medios sociales.

Common Sense Media, recursos de la familia:
https://www.commonsensemedia.org/educators/family-tip-sheets

En Español
https://www.commonsensemedia.org/educators/family-tip-sheets

STAYSAFEONLINE.ORG
www.staysafeonline.org

Staysafeonline.org es una página web gestionada por la National Cyber Security Alliance (NCSA), una ONG con sede en Estados Unidos, cuya misión es "educar y, por tanto, empoderar a la sociedad digital a utilizar el Internet de forma segura en el hogar, el trabajo y la escuela, protegiendo la tecnología que utilizan los particulares, las redes a las que se conectan, y nuestros activos digitales compartidos".

Staysafeonline.org tiene una gran cantidad de recursos para padres, incluyendo información sobre ciudadanía digital, el acoso cibernético, el control parental y juegos en línea. Los padres también podrán encontrar recursos sobre las mejores prácticas básicas de seguridad cibernética, robo de identidad, dispositivos móviles y redes sociales.

CENTRO NACIONAL PARA NIÑOS DESAPARECIDOS Y EXPLOTADOS (NCMEC)
(National Center for Missing & Exploited Children)
NetSmartz Workshop
http://www.netsmartz.org/

Netsmartz Workshop, un programa del Centro Nacional para Niños Desaparecidos y Explotados ofrece recursos y materiales para padres, adolescentes, preadolescentes y niños y niñas. Videos, juegos, concursos y consejos en línea cubren una gama de temas, desde el robo de identidad, el acoso cibernético, los dispositivos móviles, las redes sociales, la seguridad cibernética y juegos.

FTC ONGUARDONLINE
www.onguardonline.gov/

Español
www.alertaenlinea.gov/

OnguardOnline.gov es un sitio web de seguridad del consumidor en línea de la Comisión Federal de Comercio de Estados Unidos. Hay una gran cantidad de información y recursos para padres, adolescentes y niños y niñas sobre la seguridad cibernética, la seguridad y privacidad en línea. Los recursos incluyen consejos, juegos y vídeos. OnguardOnline también ha organizado un gran libro descargable para ayudar a los padres a discutir cuestiones de seguridad en línea con sus hijos. (http://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf)

Empresas

PARA. PIENSA. CONÉCTATE.
PARA. PIENSA. CONÉCTATE. ofrece consejos y asesoramiento que las empresas pueden utilizar para empezar a lograr que sus negocios sean más seguros, así como los materiales que, descargados, pueden ser publicados en el lugar de trabajo para educar a los empleados. Además de los materiales de inglés, existen recursos limitados disponibles en español, portugués, francés, japonés y ruso.
http://stopthinkconnect.org/resources/

COMISIÓN FEDERAL DE COMUNICACIONES DE ESTADOS UNIDOS (FCC)
(United States Federal Communications Commission)

La FCC ha desarrollado una herramienta de planeación de seguridad cibernética para las pequeñas empresas. El planificador ayuda a evaluar su preparación para la seguridad cibernética y crear un plan centrado en la prevención, la resolución y la restitución. Además del planeador, tienen una lista de recursos adicionales.
http://www.fcc.gov/cyberforsmallbiz

EQUIPO DE RESPUESTA A EMERGENCIAS DE COMPUTACIÓN DEL DEPARTAMENTO DE SEGURIDAD NACIONAL DE ESTADOS UNIDOS (US-

CERT)
(United States Department of Homeland Security Computer Emergency Readiness Team)

US-CERT es un gran recurso para obtener información detallada sobre todos los tipos de amenazas de seguridad cibernética, información técnica y orientación sobre la forma de proteger sus redes y dispositivos. También tienen una actividad RSS a la que usted puede suscribirse para tener información actualizada sobre cuestiones de seguridad cibernética.
https://www.us-cert.gov/ncas/tips

COMISIÓN FEDERAL DE COMERCIO (FTC)
(Federal Trade Commission)

Mientras que el sitio web de la FTC no está dirigido específicamente a los negocios, gran parte de la información es valiosa para la pequeña empresa.
http://www.onguardonline.gov/topics/secure-your-computer

Español
http://www.alertaenlinea.gov/temas/proteja-su-computadora

CENTRO DE SEGURIDAD EN INTERNET (CIS)
(Center for Internet Security)

El CIS cuenta con recursos que los negocios pueden utilizar para aprender algunos conceptos básicos de seguridad cibernética (asegurar credenciales de inicio de sesión, cuentas de redes sociales, seguridad de banca en línea). El CIS está conectado con el Centro de Intercambio de Información y Análisis Multi-Estado (MSISAC) que tiene consejos diarios, un boletín de noticias y enlaces para liberar recursos de formación.
https://www.cisecurity.org/
http://msisac.cisecurity.org/

LA ALIANZA NACIONAL DE SEGURIDAD CIBERNÉTICA (NCSA)
(National Cyber Security Alliance)

NCSA tiene buenos recursos para las pequeñas empresas que buscan educarse sobre cómo mantenerse seguras en línea.
http://staysafeonline.org/business-safe-online/

MICROSOFT
Microsoft tiene una gran cantidad de información para el lugar de trabajo.
http://www.microsoft.com/security/default.aspx

Español
http://www.microsoft.com/es-xl/security/default.aspx

Francés
http://www.microsoft.com/fr-fr/security/default.aspx

Portugués
http://www.microsoft.com/pt-pt/security/default.aspx

Ejemplos de Investigación y Encuestas

ALIANZA NACIONAL DE SEGURIDAD CIBERNÉTICA (NCSA)
La NCSA ha llevado a cabo una serie de encuestas de pequeñas empresas en una variedad de temas en los últimos años.

https://www.staysafeonline.org/business-safe-online/resources

PWC
Encuesta del Estado Mundial sobre la Seguridad de Información 2015

http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

EY
Encuesta Global de Seguridad de la Información 2014

http://www.ey.com/publication/vwluassets/ey-global-information-security-survey-2014/$file/ey-global-information-security-survey-2014.pdf

CRIANZA/FAMILIA
FOSI: PAUTAS DE CRIANZA EN LA ERA DIGITAL 2014
(FOSI: Parenting in the Digital Age 2014)
https://www.fosi.org/policy-research/parenting-digital-age/

IKEEPSAFE: INFORME DEL ÍNDICE DE SEGURIDAD DE LOS PADRES 2013

http://storage.googleapis.com/ikeepsafe/beapro%20parent/beapro_parent_index_report.pdf

MICROSOFT

http://www.microsoft.com/security/resources/research-studies.aspx

Microsoft ha encargado numerosos estudios de investigación en temas como el uso de móvil, la educación en seguridad cibernética, la intimidación en línea, juegos en línea y la gestión de la reputación en línea.

PROYECTO DE INTERNET DE INVESTIGACIÓN PEW

Adolescentes, Medios Sociales, y Privacidad
http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

NEGOCIO RIESGOSO: LAS AMENAZAS DE MALWARE POR SOFTWARE SIN LICENCIA (BUSINESS SOFTWARE ALLIANCE)

http://globalstudy.bsa.org/2013/index.html

Español
http://globalstudy.bsa.org/2013/malware/study_malware_esmx.pdf

L

PARA.PIENSA.CONÉCTATE

PARA. PIENSA. CONÉCTATE.™ es la campaña mundial de sensibilización de seguridad cibernética para ayudar a todos los ciudadanos digitales a estar más seguros en línea.

PARA. PIENSA. CONÉCTATE. Fue desarrollado por una coalición de empresas privadas, sin fines de lucro y organizaciones gubernamentales bajo la orientación del Grupo de Trabajo Anti-Phishing (APWG, por sus siglas en inglés) y de la Alianza Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés). Una amplia investigación se llevó a cabo para aportarle información a la campaña sobre mensajes que no solo aumentarían la sensibilidad sobre la seguridad cibernética, sino también inspirarían a la personas a cambiar su comportamiento. En octubre de 2010 la campaña fue lanzada por la Messaging Convention PARA. PIENSA. CONÉCTATE. en asociación con el gobierno de Estados Unidos, incluida la Casa Blanca. La campaña es supervisada por el APWG y NCSA. Desde el lanzamiento inicial en EE.UU., la campaña ha ganado fuerza global. Canadá, Japón, Malasia, Panamá, Paraguay y Uruguay se han unido a la campaña. La Organización de los Estados Americanos ha firmado un memorando de entendimiento para adoptar y apoyar la campaña.

Metas y Objetivos de PARA. PIENSA. CONÉCTATE.

"Animaremos a todos los usuarios de Internet a estar más pendientes de la práctica de hábitos seguros en línea; nos aseguraremos de que la seguridad en Internet sea percibida como una responsabilidad compartida en el hogar, en el lugar de trabajo y a lo largo de nuestras comunidades; y transformaremos la manera en que los sectores público y privado y el gobierno federal de Estados Unidos colaboran para que la seguridad cibernética sea una realidad.

Nuestro objetivo es ayudarle a la gente a entender no solo los riesgos que vienen con el uso de Internet, sino también la importancia de practicar un comportamiento seguro en línea.

Nuestros objetivos son:

• Aumentar y reforzar la conciencia de seguridad cibernética, incluyendo los riesgos y amenazas asociados, y proveer soluciones para aumentar la seguridad cibernética.
•Comunicar los enfoques y estrategias para que el público y sus familias y sus comunidades estén más seguras en línea.
•Cambiar la percepción de seguridad cibernética entre el público americano de la evitación de lo desconocido al reconocimiento de la responsabilidad compartida.
•Involucrar al público, el sector privado y los gobiernos estatales y locales en los esfuerzos de nuestra nación para mejorar la seguridad cibernética.
•Aumentar el número de interesados nacionales y organizaciones comunitarias dedicadas a educar al público sobre la seguridad cibernética y lo que la gente puede hacer para protegerse en línea".

La campaña PARA. PIENSA. CONÉCTATE. está abierta para todas las personas sin ningún costo. Todos los materiales que se encuentran en www.stopthinkconnect.org están disponibles para que cualquiera que desee utilizarlos. Las empresas, las ONG y los particulares que deseen utilizar el logotipo en sus sitios web, crear materiales únicos o modificar los materiales de la campaña ya creadas deberán firmar una licencia. La licencia no tiene ningún costo; es simplemente un acuerdo de que los lineamientos de la campaña serán seguidos y serán utilizados en forma para la que están destinados. Para revisar la licencia y los lineamientos de estilo editorial que la acompaña, véase el Apéndice A y B. Se les pide a los gobiernos que quieran unirse a la campaña firmar un Memorando de Entendimiento. El memorando de entendimiento es un acuerdo con la Convención de mensajería PARA. PIENSA. CONÉCTATE. Declarando la intención de la campaña y del gobierno. Para obtener más información acerca de las alianzas internacionales de campaña póngase en contacto con Peter Cassidy en Peter@apwg.org.

Mensajes

PARA. PIENSA. CONÉCTATE.

Estos son los mensajes relacionados con la campaña PARA. PIENSE.CONÉCTATE. Fueron desarrollados sobre la base de las investigaciones utilizadas para informar a la campaña. Todos estos mensajes fueron creados cuidadosamente para ser positivos y orientados a la acción. Cada mensaje principal es seguido por una serie de sub-mensajes que están destinados a ser positivos y orientados a la acción. Todos los mensajes principales se pueden utilizar con cualquier tipo de público, mientras que los sub-mensajes pueden ser apropiados para un público más específico. Todos estos mensajes principales son los puntos iniciales de una campaña; los mensajes pueden ser editados o agregados, según se necesite, para un público en particular.

Mantenga su equipo limpio.

- Mantenga actualizado el software de seguridad: tener el último software de seguridad, navegador web y sistema operativo son las mejores defensas contra los virus, malware y otras amenazas en línea.
- Automatice las actualizaciones de software: Muchos programas de software se conectarán y actualizarán automáticamente para defenderse de los riesgos conocidos. Active las actualizaciones automáticas si eso es una opción disponible.
- Proteja todos los dispositivos que se conectan a Internet: Junto con las computadoras, teléfonos inteligentes, sistemas de juegos y otros dispositivos habilitados para Internet también necesitan protección contra virus y malware.
- Enchufe y escanee: Los USB y otros dispositivos externos pueden ser infectados por virus y malware. Utilice su software de seguridad para escanearlos.

Proteja su información personal.

- Asegure sus cuentas: Solicite protección más allá de las contraseñas. Muchos proveedores de cuentas ahora ofrecen formas adicionales para verificar su identidad antes de realizar negocios en ese sitio.
- Cree contraseñas largas y fuertes: Combine letras mayúsculas y minúsculas con números y símbolos para crear una contraseña más segura.
- Cuenta única, contraseña única: contraseñas diferentes para cada cuenta ayudan a frustrar a los delincuentes cibernéticos.
- Anótelo y manténgalo a salvo: Todo el mundo puede olvidar una contraseña. Lleve una lista que esté guardada en un lugar seguro lejos de su computadora.
- Sea dueño/a de su presencia en línea: Establezca la configuración de privacidad y de seguridad en los sitios web a su nivel de comodidad de intercambio de información. Está bien limitar cómo y con quién se comparte la información.

Conecte con cuidado.

- En caso de duda, tírelo a la basura: Los enlaces en el correo electrónico, tuits, mensajes y la publicidad en línea son a menudo la forma que utilizan los delincuentes cibernéticos para comprometer su equipo. Si parece sospechoso, incluso si usted conoce la fuente, es mejor eliminarlo o en su caso, marcarlo como correo basura.
- Sea inteligente con los puntos de acceso Wi-Fi: Limite el tipo de negocio que realiza y ajuste la configuración de seguridad de su dispositivo para limitar quién puede acceder a su equipo.
- Proteja su $$: Cuando esté utilizando la banca y haciendo compras, verifique que los sitios están habilitados en seguridad. Busque direcciones web con “https://”, que significa que el sitio toma medidas adicionales para ayudar a proteger su información. “Http://” no es seguro.

Sea sabio en la Web

- Manténgase al día. Manténgase actualizado/a con las nuevas maneras de mantenerse seguro en línea. Visite los sitios web de confianza para tener la información más reciente, y comparta con amigos, familiares y colegas y anímelos a ser sabios en la web.
- Piense antes de actuar: Tenga cuidado con las comunicaciones que le imploran que actúe de inmediato, ofrezcan algo que suene demasiado bueno para ser verdad, o soliciten información personal.
- Haga una copia de seguridad: Proteja su valioso trabajo, música, fotos y otra información digital al hacer una copia electrónica y almacenar de forma segura.

Sea un buen ciudadano en línea

- Más seguro para mí, más seguro para todos: Lo que haga usted en línea tiene el potencial de afectar a todos, en casa, en el trabajo y en todo el mundo. Practicar buenos hábitos en línea beneficia a la comunidad digital mundial.
- Publique sobre los demás solo lo que usted quisiera que ellos publiquen acerca de usted.
- Ayude a las autoridades a combatir la delincuencia informática: Denuncie sobre robos a las finanzas, las identidades y los delitos cibernéticos en [inserte información de la agencia local de denuncias] ser apropiados para un público más específico.

Secretario General
Luis Almagro Lemes

Secretario General Adjunto
Nestor Mendez

Kit de Herramientas para la Campaña de Concientización sobre Seguridad Cibernética

Secretario Ejecutivo del Comité Interamericano contra el Terrorismo
Alfred Schandlbauer

Desarrollado por
Aimee Larsen Kirkpatrick

Editores
Pablo Martinez
Belisario Contreras
Kerry-Ann Barrett
Barbara Marchiori de Assis

Colaboradores
Peter Cassidy
Emily Eckland
Diego Subero
Gonzalo García-Belenguer
Emmanuelle Pelletier
Francisco Javier Villa
Robert Fain
Catalina Lillo

Organización de los Estados Americanos | Más derechos para más gente

17th Street and Constitution Ave., NW
Washington, D.C., 20006-4499
United States of America

www.oas.org