



Trasfondo:

Con el propósito de reconocer la importancia de la seguridad cibernética, el Presidente Obama designó el mes de octubre como Mes Nacional de la Concienciación en Seguridad Cibernética (NCSAM, por sus siglas en inglés). Ya en su 13º año, el Mes Nacional de la Concienciación en Seguridad Cibernética es un esfuerzo de colaboración entre el Departamento de Seguridad Nacional de Estados Unidos (DHS, por sus siglas en inglés) y sus colaboradores de los sectores público y privado, lo que incluye la Alianza Nacional de Seguridad Cibernética (National Cyber Security Alliance), con el objetivo de generar conciencia sobre la importancia de la seguridad cibernética y la pureza cibernética.



National Cyber Security
Awareness Month

Temas semanales del NCSAM 2016:

Cada semana de octubre está dedicada a un tema y mensaje correspondiente relacionado a la seguridad cibernética. Los temas aquí listados ofrecen una oportunidad para que el gobierno y la industria estén involucrados y apoyen con actividades que consideren relevantes. Para fomentar la participación de todos los estadounidenses, se coordinarán eventos clave en diversos lugares del país. Le invitamos a coordinar sus planes para el Mes Nacional de la Concienciación en Seguridad Cibernética a partir de los siguientes temas semanales:

1. Semana 1: 3-7 de octubre de 2016 – Tema: Pasos de cada día para reforzar la seguridad en línea con la campaña “Para.Piensa.Conéctate” (Stop.Think.Connect.™).
La seguridad cibernética forma parte de todos los aspectos de nuestra vida, ya sea en el hogar, en el trabajo, en los estudios o mientras viajamos. Sin importar sus capacidades técnicas ni su formación, existen medidas simples que cualquier persona puede adoptar para reforzar la seguridad informática en su vida digital. La semana 1 da inicio al Mes Nacional de la Concienciación en Seguridad Cibernética 2016 y busca consolidar consejos básicos para que el público tenga mayor seguridad en línea, lo que incluye cuentas más seguras mediante pasos de autenticación más sólidos y manteniéndose al día con las actualizaciones de seguridad.
2. Semana 2: 10-14 de octubre de 2016 – Tema: La informática desde la sala de descanso a la sala de reuniones
Todos somos responsables de proteger tanto nuestros datos personales como los de la organización en la que trabajamos. Desde el CEO hasta el empleado más novato, la política de ciberseguridad de toda organización se basa en prácticas de vigilancia y concienciación compartidas. La semana 2 contempla cómo todos los empleados pueden fomentar una cultura de ciberseguridad en el trabajo.
3. Semana 3: 17-21 de octubre de 2016 – Tema: Reconocer y combatir los delitos cibernéticos
A medida que la tecnología avanza, el impacto de los delitos cibernéticos incrementa en costo y frecuencia. El gobierno, las fuerzas policiales, la industria y los ciudadanos, jugamos todos un papel crucial en la mitigación de sus efectos negativos en nuestras escuelas, comunidades y en nuestro bienestar personal. Estos incidentes se perpetúan a diario mediante correos electrónicos fraudulentos (phishing) disfrazados como provenientes de fuentes de confianza, en sitios web infectados que obtienen información personal que ingresamos y en forma de enlaces persuasivos con programas de extorsión (ransomware) que bloquean archivos en nuestros dispositivos hasta que se pague un dinero como ‘rescate’. La semana 3 se enfoca en los indicios de intención criminal por medio de la tecnología y en lo que cada persona puede hacer para detectar y prevenir los delitos cibernéticos.
4. Semana 4: 24-28 de octubre de 2016 – Tema: Nuestras vidas siempre conectadas: ¿cuál es tu “app”-titud?
Con el crecimiento de tecnologías conectadas en autos, electrodomésticos, productos financieros, el área de la salud y otras que cada vez se controlan más desde dispositivos “inteligentes”, nos encontramos ante la necesidad de estar siempre al tanto de los últimos dispositivos e innovaciones y pendientes de cómo asegurarlos. La semana 4 da una mirada al futuro y analiza cómo se incluye la seguridad cibernética en tecnologías avanzadas para permitir una vida segura en nuestra sociedad digital.
5. Semana 5: 31 de octubre de 2016 – Tema: Construyendo resistencia para la infraestructura crítica
La unión entre la seguridad cibernética y la seguridad física es esencial para la resistencia de la infraestructura crítica tanto a nivel local como nacional. La resistencia de los sistemas y bienes esenciales, desde la red energética hasta sistemas bancarios, es vital para la seguridad, economía y salud pública de nuestro país. La semana 5 se concentra en el sostenimiento de la infraestructura crítica del país y facilita la transición al Mes Nacional de la Resistencia y la Seguridad de la Infraestructura Crítica (CISR, en inglés).

El hashtag para el Mes Nacional de la Concienciación en Seguridad Cibernética será #CyberAware. Le invitamos a usar este hashtag antes y durante el mes de octubre para mostrar su apoyo y el de su organización para generar conciencia sobre la seguridad cibernética.

Para más información, póngase en contacto con la campaña Para.Piensa.Conéctate.™ a través de stopthinkconnect@dhs.gov.