MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2021 KIT D'OUTILS

Messages clés, articles, médias sociaux et plus encore pour promouvoir le Mois de la sensibilisation à la cybersécurité 2021

TABLE DES MATIERES

BIENVENUE AU MOIS DE LA SENSIBILISATION A LA CYBERSECURITE 2021

Organisé chaque année en octobre, le Mois de la sensibilisation à la cybersécurité est un effort de collaboration entre le gouvernement et l'industrie pour garantir que chaque Américain dispose des ressources dont il a besoin pour rester en sécurité en ligne tout en augmentant la résilience de la nation contre les cybermenaces.

L'agence de la cybersécurité et de la sécurité de l'infrastructure (CISA) et l'alliance de la cybersécurité nationale (NCSA) sont co-responsable du Mois de la sensibilisation à la cybersécurité.

Nous vous remercions de participer au Mois de la sensibilisation à la cybersécurité. Pour vous aider dans vos efforts et votre participation, ce document comprend une mine de ressources pour vous et votre organisation, quelle que soit leur taille ou leur secteur d'activité, afin de vous engager et promouvoir le thème central et les messages critiques avant et pendant le mois d'octobre.

THEMES ET MESSAGES CLES POUR OCTOBRE 2021

Le Mois de la sensibilisation à la cybersécurité a un thème général que nous vous demandons d'utiliser dans vos propres initiatives d'octobre. Cette année, sous le thème « Faites votre part. #BeCyberSmart. », la campagne mettra l'accent sur le rôle que chaque individu joue dans la sécurité en ligne et soulignera l'importance de prendre des mesures proactives pour améliorer la cybersécurité à la maison et sur le lieu de travail.

THEME GENERAL 2021

Faites votre part #BeCyberSmart.

MESSAGES CLES DE 2021

Pour aider à cadrer les conversations, concevoir des ressources et organiser des événements avec les parties prenantes internes et externes, nous décomposons le thème général en quatre messages hebdomadaires. Les messages clés ci-dessous seront présentés tout au long du mois pour aider à générer des événements, des ressources et des activités exécutés par CISA et NCSA, et nous avons inclus des sujets potentiels pour vous aider à démarrer vos propres efforts pour le Mois de la sensibilisation à la cybersécurité.

- **SEMAINE 1 : Soyez Cyber Smart**
  Prenez des mesures simples pour protéger nos vies numériques.
- **SEMAINE 2 : Combattez le Phish !**
  Découvrez comment repérer et signaler les tentatives d'hameçonnage pour empêcher les ransomwares et autres attaques de logiciels malveillants.
- **SEMAINE 3 : Découvrez. Expérimentez Partagez.**
  Commémorez la Semaine de sensibilisation aux carrières en cybersécurité de l'initiative nationale pour l'éducation à la cybersécurité (NICE) Cybersecurity Career Awareness Week et la main-d'œuvre mondiale en matière de cybersécurité.
- **SEMAINE 4 : La cybersécurité en premier.**
  Explorez comment la cybersécurité et la sécurité en ligne sont de plus en plus importantes alors que nous continuons à fonctionner virtuellement dans notre travail et notre vie personnelle.

COMMENT S'ENGAGER

Cette section fournit des conseils pour diffuser des messages de sensibilisation à la cybersécurité afin de garantir que votre campagne du Mois de la sensibilisation à la cybersécurité atteigne votre public cible. L'objectif de la campagne 2021 est de promouvoir la responsabilité personnelle et des changements de comportement positifs en matière de cybersécurité. Pour assurer le succès en octobre, gardez cet objectif à l'esprit lorsque vous créez des ressources, développez des activités et planifiez des événements.

IDEES D'ENGAGEMENT

- Apportez votre voix et vos ressources aux conversations sur les médias sociaux en utilisant les hashtags #BeCyberSmart and #CybersecurityAwarenessMonth
- Inclure un message sur l'importance de la cybersécurité dans les bulletins d'information, les envois postaux et sites Web en octobre
- Organiser un événement ou une réunion pour discuter des questions de cybersécurité locales et pertinentes
- Organiser, fournir ou promouvoir des possibilités de formation et d'exercices en cybersécurité pour vos activités internes et intervenants externes
- Participez à une formation ou à un exercice local ou virtuel pour améliorer la cybersécurité et la résilience au sein de votre organisation
- Utilisez les fiches conseils disponibles sur cisa.gov/cybersecurity-awareness-month pour lire sur divers sujets de cybersécurité
    - Que ce soit au travail ou à la maison, ces fiches conseils ont quelque chose d'utile pour tout le monde
- Devenez un ami du STOP. THINK. CONNECT. ™ Campagne en visitant cisa.gov/stopthinkconnect
- Les professionnels de la cybersécurité peuvent s'engager à aider les communautés vulnérables #SecureTogether et les aider à améliorer leur posture de cybersécurité grâce à des actions clés à www.cybercrimesupport.org

LES MEILLEURS CONSEILS A PARTAGER PENDANT LE MOIS DE LA SENSIBILISATION A LA CYBERSECURITE

- **Doublez votre protection de connexion.** Activez l'authentification multifactorielle (MFA) pour vous assurer que la seule personne ayant accès à votre compte est vous-même. Utilisez-le pour les e-mails, les opérations bancaires, les réseaux sociaux et tout autre service nécessitant une connexion. Si MFA est une option, activez-la en utilisant un appareil mobile de confiance, tel que votre smartphone, une application d'authentification ou un jeton sécurisé—un petit dispositif physique qui peut s'accrocher à votre trousseau de clés. Lisez le Multi-Factor Authentication (MFA) How-to-Guide pour plus d'information.

- **Changez votre protocole de mot de passe.** Selon les directives de l'Institut national des normes et de la technologie (NIST), vous devriez envisager d'utiliser le mot de passe ou la phrase de passe le plus long possible. Soyez créatif et personnalisez votre mot de passe standard pour différents sites, ce qui peut empêcher les cybercriminels d'accéder à ces comptes et vous protéger en cas de violation. Utilisez des gestionnaires de mots de passe pour créer et retenir des mots de passe différents et complexes pour chacun de vos comptes. Lisez le Creating a Password Tip Sheet pour en savoir plus.

- **Si vous vous connectez, vous devez protéger.** Qu'il s'agisse de votre ordinateur, de votre smartphone, de votre console de jeux ou d'autres périphériques réseau, la meilleure défense contre les virus et les logiciels malveillants consiste à mettre à jour les logiciels de sécurité, le navigateur web et les systèmes d'exploitation les plus récents. Inscrivez-vous aux mises à jour automatiques, si vous le pouvez, et protégez vos appareils à l'aide de un logiciel anti-virus. Lisez le Phishing Tip Sheet pour en savoir plus.
- **Jouez la carte de la difficulté avec les inconnus.** Les cybercriminels utilisent des tactiques de phishing, dans l'espoir de tromper leurs victimes. Si vous n'êtes pas sûr de l'identité de l'expéditeur d'un courriel - même si les détails semblent exacts - ou si le courriel semble "bidon", ne répondez pas et ne cliquez pas sur les liens ou les pièces jointes qu'il contient. Lorsqu'elle est disponible, utilisez l'option "signaler un hameçon" ou "signaler" pour aider votre organisation ou votre fournisseur de messagerie à bloquer d'autres courriels suspects avant qu'ils n'arrivent dans votre boîte de réception.
- **Ne jamais cliquer et raconter.** Limitez les informations que vous publiez sur les médias sociaux - des adresses personnelles à l'endroit où vous aimez prendre un café. Ce que beaucoup de gens ne réalisent pas, c'est que ces détails apparemment aléatoires sont tout ce que les criminels ont besoin de savoir pour vous cibler, vous, vos proches et vos biens matériels - en ligne et dans le monde réel. Gardez secrets les numéros de sécurité sociale, les numéros de compte et les mots de passe, ainsi que les informations spécifiques vous concernant, telles que votre nom complet, votre adresse, votre date d'anniversaire et même vos projets de vacances. Désactivez les services de localisation qui permettent à quiconque de voir où vous êtes - et où vous n'êtes pas - à tout moment. Lisez le Social Media Cybersecurity Tip Sheet pour en savoir plus.
- **Gardez un œil sur vos applications.** La plupart des appareils, jouets et dispositifs connectés sont pris en charge par une application mobile. Votre appareil mobile pourrait être rempli d'applications suspectes fonctionnant en arrière-plan ou utilisant des autorisations par défaut que vous n'avez jamais réalisé que vous aviez approuvées. Ces applications recueillent vos informations personnelles à votre insu et mettent votre identité et votre vie privée en danger. Vérifiez les autorisations de vos applications et utilisez la "règle du moindre privilège" pour supprimer ce dont vous n'avez pas besoin ou que vous n'utilisez plus. Apprenez à dire simplement "non" aux demandes de privilèges qui n'ont pas de sens. Ne téléchargez que des applications provenant de fournisseurs et de sources fiables.
- **Restez protégé tout en étant connecté.** Avant de vous connecter à un point d'accès public sans fil, par exemple dans un aéroport, un hôtel ou un café, assurez-vous de confirmer le nom du réseau et les procédures de connexion exactes auprès du personnel concerné pour vous assurer que le réseau est légitime. Si vous utilisez un point d'accès public non sécurisé, adoptez une bonne hygiène Internet en évitant les activités sensibles (par exemple, les opérations bancaires) qui nécessitent des mots de passe ou des cartes de crédit. Votre hotspot personnel est souvent une alternative plus sûre au Wi-Fi gratuit. N'utilisez que les sites commençant par "https://" pour vos achats ou vos opérations bancaires en ligne.

RESSOURCES DE CYBERSECURITE

Vous trouverez ci-dessous des ressources utiles pour améliorer et promouvoir la sensibilisation à la cybersécurité en octobre et tout au long de l'année. Explorez ces sites pour trouver du contenu à utiliser dans des blogs, des articles et des messages au sein de vos organisations et auprès de publics externes.

- L'Alliance nationale pour la cybersécurité (NCSA) établit des partenariats publics/privés solides pour créer et mettre en œuvre des efforts d'éducation et de sensibilisation de grande envergure afin de donner aux utilisateurs, à la maison, au travail et à l'école, les informations dont ils ont besoin pour assurer leur propre sécurité, celle de leurs organisations, de leurs systèmes et de leurs informations sensibles en ligne et pour encourager une culture de la cybersécurité. Pour les événements recommandés par le NCSA, cliquez : https://staysafeonline.org
- Propulsé par le ministère américain de la sécurité intérieure, le programme "Be Cyber Smart" campaign est conçu pour inciter la jeune génération d'américains à assumer la responsabilité de leur propre cybersécurité. Découvrez les bases de la cybersécurité, les escroqueries courantes et comment signaler les incidents de cybersécurité en visitant la campagne en ligne.
- Vous cherchez des informations sur un poste ou un cours particulier en matière de cybersécurité ? The National Initiative for Cybersecurity Careers and Studies (NICCS) est une ressource nationale pour l'éducation, la formation et le développement de la main-d'œuvre en matière de cybersécurité. Le NICCS propose des outils et des informations aux professionnels actuels et futurs de la cybersécurité, qu'il s'agisse d'étudiants et d'enseignants de la maternelle à la terminale, d'employés fédéraux, de vétérans ou de personnes en réorientation professionnelle. Ces outils et

ressources sont à la disposition de toute personne souhaitant obtenir plus d'informations sur le domaine de la cybersécurité, sur la manière de faire progresser une carrière dans ce domaine, etc.

CANAUX DE COMMUNICATION

Les hashtags officiels du Mois de la sensibilisation à la cybersécurité 2021 sont #BeCyberSmart et #CybersecurityAwarenessMonth. Donnez de la visibilité à votre participation et à celle de votre organisation en utilisant ces hashtags avant et pendant le mois d'octobre pour promouvoir et participer aux activités et événements de la campagne.

EXEMPLE DE CALENDRIER DE COMMUNICATION

Utilisez le calendrier de communication suivant pour vous aider à planifier vos efforts de sensibilisation et d'exécution avant et pendant le Mois de la sensibilisation à la cybersécurité. Il s'agit uniquement d'un guide et non d'une restriction ou d'une limitation de vos activités.

AOUT

- Début de la planification du mois de sensibilisation à la cybersécurité entre le marketing et la direction sur les activités et la participation d'octobre, y compris les communications, les nouvelles et les recherches potentielles de l'entreprise qui pourraient être publiées au cours du mois.
- **Le 19 août :** Order bulk cybersecurity awareness materials de la Commission fédérale du commerce (FTC) à distribuer au cours du mois d'octobre.
- **Le 27 août :** Cette date est le dernier jour pour inviter un représentant de la CISA ou des agences fédérales locales à parler à vos employés sur la sécurité en ligne. Demandez des conférenciers CISA en visitant la section « Demander un conférencier CISA » à l'adresse http://www.cisa.gov/contact-us

SEPTEMBRE

- **Le 1er septembre :** Créer un calendrier de communication numérique pour les messages sociaux, les blogs et les courriels de l'entreprise et de la direction, ainsi que pour les autres promotions du Mois de sensibilisation à la cybersécurité tout au long du mois.
- **Le 20 septembre :** Lancez un compte à rebours de deux semaines pour le Mois de la sensibilisation à la cybersécurité sur les canaux de médias sociaux.
- **Le 21 septembre :** Envoyez un courriel aux employés pour leur annoncer votre participation à la campagne et leur expliquer comment votre entreprise s'impliquera avant et pendant le Mois de la sensibilisation à la cybersécurité.
- **Le 30 septembre :** Affichez les graphiques du Mois de la sensibilisation à la cybersécurité dans votre entreprise, dans des endroits très fréquentés, ou sur le(s) site(s) Web de votre organisation.
- **Le 30 septembre :** Organisez un déjeuner pour les employés afin de discuter des politiques de votre entreprise en matière de cybersécurité et d'utilisation acceptable et partagez la présentation du mois de sensibilisation à la cybersécurité avec les employés.

OCTOBRE

- **Le 1er octobre :** Travaillez avec vos dirigeants pour publier une proclamation officielle de l'entreprise en faveur du #CyberMonth et de leur engagement à Faire votre part. #BeCyberSmart
- **Le 1er octobre :** Envoyez une lettre à vos clients pour souligner la participation de votre entreprise au Mois de la sensibilisation à la cybersécurité et leur donner des conseils utiles pour qu'ils soient #BeCyberSmart.
- **Le 1er octobre :** Envoyez/programmez la première série de conseils quotidiens ou hebdomadaires aux médias sociaux/employés sur la façon de rester en sécurité en ligne.
- **Le 4 octobre :** Publier un communiqué de presse de l'entreprise en rapport avec le mois (mises à jour de produits ou d'offres, victoires de clients, etc.)
- **Le 11 octobre :** Envoyez/programmez une seconde série de conseils quotidiens ou hebdomadaires aux médias sociaux/employés sur la façon de rester en sécurité en ligne.
- **Le 18 octobre :** Envoyez/programmez la troisième série de conseils quotidiens ou hebdomadaires aux médias sociaux/employés sur la façon de rester en sécurité en ligne.
- **Le 19 octobre :** Effectuez une simulation d'hameçonnage avec vos employés en utilisant les outils suivants CISA's Cyber Hygiene Services

- **Le 25 octobre :** Envoyez/programmez la quatrième de conseils quotidiens ou hebdomadaires aux médias sociaux/employés sur la façon de rester en sécurité en ligne.
- **Le 26 octobre :** Organisez un événement partenaire du Mois de la sensibilisation à la cybersécurité pour les employés et/ou votre entreprise communité locale
- **Le 28 octobre :** Envoyer une distribution finale de matériel de sécurité en ligne soulignant l'importance d'être cyberintelligent toute l'année.
- **Le 29 octobre :** Envoyez aux employés un courriel récapitulant les informations qu'ils ont apprises tout au long du mois - envisagez d'offrir de petits prix à ceux qui ont obtenu de bons résultats lors des activités ou qui se sont engagés.

COMMUNICATION SUR LES RESEAUX SOCIAUX

Vous trouverez ci-dessous des exemples de messages sur les médias sociaux pour promouvoir le mois de sensibilisation à la cybersécurité dans votre organisation. Le CISA et le NCSA vous encouragent vivement à publier des messages sur vos canaux de communication en ligne avant et pendant le mois d'octobre.

TWITTER :

Semaine du coup d'envoi :

#CyberMonth est de retour en octobre pour sa 18e année afin d'éduquer la nation sur la cybersécurité et sur la façon dont tous les Américains peuvent être plus en sécurité en ligne. Découvrez comment vous pouvez Faire votre part #BeCyberSmart en vous rendant sur le site cisa.gov/cybersecurity-awareness-month

Semaine 1 – Soyez Cyber Smart :

Faire votre part #BeCyberSmart! Cette première semaine du Mois de la sensibilisation à la cybersécurité, nous allons explorer les principes fondamentaux de la cybersécurité, en vous apprenant comment mieux sécuriser votre vie numérique et améliorer la sécurité de vos appareils. #CyberMonth #cybersecurity #InformationSecurity

Semaine 2 - Combattez le Phish ! :

Combattez le Phish ! Cette semaine, le Mois de la sensibilisation à la cybersécurité mettra l'accent sur la manière dont les particuliers peuvent repérer les tentatives d'hameçonnage. L'hameçonnage peut souvent conduire à des vulnérabilités qui peuvent déboucher sur des ransomwares ou d'autres types de logiciels malveillants. #FightThePhish #Phishing #Ransomware #BeCyberSmart #CyberMonth

Semaine 3 – Découvrez. Expérimentez. Partagez :

Rejoignez la CISA et L'initiative nationale pour l'éducation à la cybersécurité (NICE) cette semaine pour célébrer la semaine de sensibilisation aux carrières dans le domaine de la cybersécurité. Cette semaine, nous présenterons leurs contributions et leurs innovations. La formation d'une main-d'œuvre spécialisée dans la cybersécurité renforcera la sécurité. #CyberMonth #CyberCareer

Semaine 4 - La cybersécurité d'abord :

C'est la dernière semaine du Mois de la sensibilisation à la cybersécurité, vous devez continuer à faire votre part et #BeCyberSmart! Les actions d'aujourd'hui affectent notre avenir. La cybersécurité fait l'objet d'un effort tout au long de l'année et est devenue une préoccupation majeure dans notre façon de travailler, d'apprendre et de vivre. #CyberMonth #CybersecurityFirst

FACEBOOK :

Semaine du coup d'envoi :

Le Mois de la sensibilisation à la cybersécurité revient pour la 18e année en octobre 2021. Cybersecurity Awareness Month Site web (cisa.gov/cybersecurity-awareness-month) souligne la nécessité d'éduquer les individus et les organisations sur l'importance de la cybersécurité, en veillant à ce que tous les Américains disposent des ressources nécessaires pour être plus sûrs et sécurisés en ligne.

- **SEMAINE 1 : Soyez Cyber Smart**
- **SEMAINE 2 : Combattez le Phish !**
- **SEMAINE 3 : Découvrez. Expérimentez. Partagez. – Semaine de sensibilisation aux carrières en cybersécurité**
- **SEMAINE 4 : La cybersécurité en premier.**

#BeCyberSmart #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 1 – Soyez Cyber Smart:

Faites votre part #BeCyberSmart! Le premier thème hebdomadaire du Mois de la sensibilisation à la cybersécurité explorera les principes fondamentaux de la cybersécurité, en apprenant à l'Amérique comment faire sa part et #BeCyberSmart ! Des gestes simples peuvent contribuer à sécuriser votre vie numérique et à améliorer la sécurité des appareils connectés à l'internet.

Au programme de cette semaine : ____, ____, et ____. Pour plus d'information, visitez le Cybersecurity Awareness Month Site web : cisa.gov/cybersecurity-awareness-month.

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 2 - Combattez le Phish ! :

Combattez le Phish ! Cette semaine, le Mois de la sensibilisation à la cybersécurité mettra l'accent sur la manière dont les particuliers peuvent repérer les tentatives d'hameçonnage potentielles. L'hameçonnage peut souvent conduire à des vulnérabilités qui peuvent déboucher sur des ransomwares ou d'autres types de logiciels malveillants. Réduisez vos risques d'être victime d'une attaque de phishing.

Au programme de cette semaine : ____, ____, et ____. Pour plus d'information, sur le phishing visitez le Cybersecurity Awareness Month Site web : cisa.gov/cybersecurity-awareness-month.

#Phishing #Ransomware #Malware #respond #recover

Semaine 3 – Découvrez. Expérimentez. Partagez :

Rejoignez la CISA et L'initiative nationale pour l'éducation à la cybersécurité (NICE) cette semaine pour célébrer la semaine de sensibilisation aux carrières dans le domaine de la cybersécurité. Les professionnels de la cybersécurité jouent un rôle essentiel dans la société et la sécurité mondiales. Cette semaine, nous présenterons leurs contributions et leurs innovations. La constitution d'une main-d'œuvre mondiale en matière de cybersécurité renforce la sécurité de chaque nation, nous pouvons expliquer comment.

#ExploreExperienceShare #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 4 - La cybersécurité d'abord :

C'est la dernière semaine du Mois de la sensibilisation à la cybersécurité, mais vous devriez toujours essayer de faire votre part et #BeCyberSmart. Ce que nous faisons aujourd'hui peut influencer l'avenir de la cybersécurité des particuliers, des consommateurs et des entreprises. La cybersécurité est de plus en plus prise en compte dans notre façon de travailler, d'apprendre et de jouer. La cybersécurité est un travail de toute une année et devrait être l'une de nos premières considérations lorsque nous créons ou achetons de nouveaux appareils et services connectés.

Participez à la conversation sur le Mois de la sensibilisation à la cybersécurité en utilisant le hashtag #BeCyberSmart.

#BeCyberSmart #CybersecurityFirst #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

INSTAGRAM :

Semaine du coup d'envoi :

Le Mois de la sensibilisation à la cybersécurité revient en octobre pour la 18e année consécutive afin de sensibiliser la nation à la cybersécurité et à la manière dont tous les Américains peuvent être plus en sécurité en ligne. Découvrez comment vous pouvez Faire votre part #BeCyberSmart en vous rendant sur le site cisa.gov/cybersecurity-awareness-month.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 1 – Soyez Cyber Smart :

Faites votre part #Be CyberSmart! Cette première semaine du Mois de la sensibilisation à la cybersécurité, nous allons explorer les principes fondamentaux de la cybersécurité, en vous apprenant comment mieux sécuriser votre vie numérique et améliorer la sécurité de vos appareils. #CyberMonth #cybersecurity #InformationSecurity

Participez à la conversation sur le Mois de la sensibilisation à la cybersécurité. Vous pouvez contribuer à la conversation en utilisant le hashtag #BeCyberSmart.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 2 - Combattez le Phish ! :

Combattez le Phish ! Cette semaine, le Mois de la sensibilisation à la cybersécurité mettra l'accent sur la manière dont les particuliers peuvent repérer les tentatives d'hameçonnage. L'hameçonnage peut souvent conduire à des vulnérabilités qui peuvent déboucher sur des ransomwares ou d'autres types de logiciels malveillants.

Participez à la conversation sur le Mois de la sensibilisation à la cybersécurité en utilisant le hashtag #BeCyberSmart.

-
-
-

#FightThePhish #Phishing #Ransomware #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 3 - Découvrez Expérimentez Partagez :

Rejoignez la CISA et L'initiative nationale pour l'éducation à la cybersécurité (NICE) cette semaine pour célébrer la semaine de sensibilisation aux carrières dans le domaine de la cybersécurité. Cette semaine, nous présenterons leurs contributions et leurs innovations. La formation d'une main-d'œuvre spécialisée dans la cybersécurité renforcera la sécurité.

-
-
-

#CyberCareers #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 4 - La cybersécurité d'abord :

C'est la dernière semaine du Mois de la sensibilisation à la cybersécurité, vous devez continuer à faire votre part et #BeCyberSmart! Les actions d'aujourd'hui affectent notre avenir. La cybersécurité fait l'objet d'un effort tout au long de l'année et est devenue une préoccupation majeure dans notre façon de travailler, d'apprendre et de vivre.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

LINKEDIN :

Semaine du coup d'envoi :

Le mois d'octobre, qui en est à sa 18e édition, est le Mois de la sensibilisation à la cybersécurité. Chaque année, la campagne vise à sensibiliser la nation à l'importance de la cybersécurité, en veillant à ce que tous les Américains disposent des ressources nécessaires pour être plus sûrs et sécurisés en ligne.

Les particuliers et les entreprises peuvent participer au Mois de la sensibilisation à la cybersécurité en utilisant les ressources du CISA pour créer leurs propres campagnes de sensibilisation ! Les partenaires peuvent créer leurs propres campagnes de sensibilisation en utilisant les thèmes hebdomadaires de cette année :

- **SEMAINE 1 : Soyez Cyber Smart**
- **SEMAINE 2 : Combattez le Phish !**
- **SEMAINE 3 : Découvrez. Expérimentez Partagez. – Semaine de sensibilisation aux carrières en cybersécurité**
- **SEMAINE 4 : La cybersécurité en premier.**

Pour en savoir plus sur la campagne, consultez le site cisa.gov/cybersecurity-awareness-month !

Semaine 1 – Soyez Cyber Smart :

#BeCyberSmart est le premier thème hebdomadaire du Mois de la sensibilisation à la cybersécurité. Il explorera les principes fondamentaux de la cybersécurité et expliquera aux organisations comment faire leur part et #BeCyberSmart ! Des gestes simples peuvent contribuer à sécuriser votre vie numérique et à améliorer la sécurité des appareils connectés à l'internet.

Au programme de cette semaine : ____, ____, et ____. Pour plus d'information, visitez le Cybersecurity Awareness Month Site web : cisa.gov/cybersecurity-awareness-month.

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semaine 2 - Combattez le Phish ! :

Combattez le Phish ! Cette semaine, le Mois de la sensibilisation à la cybersécurité mettra l'accent sur la manière dont les particuliers peuvent repérer les tentatives d'hameçonnage potentielles. L'hameçonnage peut souvent conduire à des vulnérabilités qui peuvent déboucher sur des ransomwares ou d'autres types de logiciels malveillants. Réduisez les risques que votre entreprise ou votre organisation soit victime d'attaques de phishing.

Au programme de cette semaine : ____, ____, et ____. Pour plus d'information, sur le phishing visitez le Cybersecurity Awareness Month Site web : cisa.gov/cybersecurity-awareness-month.

Semaine 3 – Découvrez. Expérimentez. Partagez :

Rejoignez la CISA et L'initiative nationale pour l'éducation à la cybersécurité (NICE) cette semaine pour célébrer la semaine de sensibilisation aux carrières dans le domaine de la cybersécurité. Les professionnels de la cybersécurité jouent un rôle essentiel dans la société et la sécurité mondiales. Cette semaine, nous présenterons leurs contributions et leurs innovations. La constitution d'une main-d'œuvre mondiale en matière de cybersécurité renforce la sécurité de chaque nation, rejoignez-nous pour apprendre pourquoi.

Semaine 4 - La cybersécurité d'abord :

C'est la dernière semaine du Mois de la sensibilisation à la cybersécurité, mais vous devriez toujours essayer de faire votre part et #BeCyberSmart. Ce que nous faisons aujourd'hui peut influencer l'avenir de la cybersécurité des particuliers, des consommateurs et des entreprises. La cybersécurité est de plus en plus prise en compte dans notre façon de travailler, d'apprendre et de jouer. La cybersécurité est un travail de toute une année et devrait être l'une de nos premières considérations lorsque nous créons ou achetons de nouveaux appareils et services connectés.

Au programme de cette semaine : ____, ____, et ____. Pour plus d'information, sur le phishing visitez le Cybersecurity Awareness Month Site web : cisa.gov/cybersecurity-awareness-month.

MODELE DE BILLET DE BLOG

CAMPAGNE DU MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2021

Maintenant dans sa 18e année, le Mois de la sensibilisation à la cybersécurité continue de sensibiliser le public à l'importance de la cybersécurité dans notre pays. Organisé chaque année en octobre, le Mois de la sensibilisation à la cybersécurité est un effort de collaboration entre le gouvernement et l'industrie pour s'assurer que tous les Américains disposent des ressources dont ils ont besoin pour être plus sûrs et plus sécurisés en ligne.

FAITES VOTRE PART. #BECYBERSMART.

Chaque année, sous l'impulsion de la Cybersecurity and Infrastructure Security Agency (CISA) et la National Cyber Security Alliance (NCSA), Mois de la sensibilisation à la cybersécurité transmet un message clair sur l'importance du partenariat entre le gouvernement et l'industrie, de la Maison Blanche à l'individu.

Le thème éternel—**Faites votre part. #BeCyberSmart.** Ce thème encourage les individus et les organisations à assumer leur rôle dans la protection de leur partie du cyberespace, en mettant l'accent sur la responsabilité personnelle et l'importance de prendre des mesures proactives pour améliorer la cybersécurité.

MESSAGES HEBDOMADAIRES

Pour vous aider, vous et vos organisations, à créer une campagne efficace de sensibilisation à la cybersécurité, CISA et NCSA ont créé quatre thèmes hebdomadaires sur lesquels se concentrer pendant le mois de sensibilisation à la cybersécurité :

- **SEMAINE 1 : Soyez Cyber Smart**
  La première semaine explore les principes fondamentaux de la cybersécurité : comment des actions simples peuvent contribuer à sécuriser vos vies numériques, à améliorer la sécurité des appareils intelligents et connectés à l'internet, et comment d'autres principes fondamentaux peuvent contribuer à réduire les cyberrisques.
- **SEMAINE 2 : Combattez le Phish !**
  La deuxième semaine sera consacrée à la manière dont les particuliers peuvent repérer les tentatives d'hameçonnage potentielles, qui conduisent souvent à des vulnérabilités pouvant déboucher sur des ransomware ou d'autres types de logiciels malveillants. Elle offrira des conseils sur la manière dont les particuliers peuvent réduire leurs risques d'être victimes d'attaques de phishing - en signalant ou en supprimant les activités suspectes - ainsi que sur la manière d'y répondre et de s'en remettre.
- **SEMAINE 3 : Découvrez. Expérimentez. Partagez.**
  En partenariat avec l'initiative nationale pour l'éducation à la cybersécurité (NICE), la troisième semaine célèbre la semaine de sensibilisation aux carrières dans le domaine de la cybersécurité. Cette semaine illustrera le rôle

essentiel que jouent les professionnels de la cybersécurité dans la société et la sécurité mondiales et attirera l'attention sur leurs contributions et leurs innovations. Cette semaine montre également comment la constitution d'une main-d'œuvre mondiale en matière de cybersécurité renforce la sécurité de chaque nation et favorise la prospérité économique.

- **SEMAINE 4 : La cybersécurité d'abord**
  La dernière semaine soulignera que la cybersécurité doit être une priorité et non une réflexion après coup et examinera comment ce que nous faisons aujourd'hui peut affecter l'avenir de la cybersécurité des particuliers, des consommateurs et des entreprises. Cette semaine mettra également en évidence le fait que la cybersécurité est un effort à mener tout au long de l'année et qu'elle devrait être la première préoccupation d'un individu ou d'une organisation lorsqu'ils créent ou achètent de nouveaux appareils et services connectés.

Ce mois-ci en particulier, nous vous demandons de ne pas traiter la cybersécurité comme un sujet tabou : parlez aux autres de la façon d'être « Cyber Smart » et assurez-vous de partager les ressources du Mois de la sensibilisation à la cybersécurité dans toute votre communauté, avec vos amis, votre famille et vos collègues. Ce faisant, nous pouvons tous faire d'énormes progrès dans la protection de nos appareils.

Utilisez le hashtag du Mois de la sensibilisation à la cybersécurité **#BeCyberSmart**, pour aider à promouvoir la sensibilisation à la cybersécurité. Assurez-vous également site web pour en savoir plus sur les efforts à venir du Mois de la sensibilisation à la cybersécurité en octobre.

EXEMPLE D'EMAIL AUX CLIENTS ET AU PERSONNEL

Vous trouverez ci-dessous un exemple d'email que vous et votre organisation pouvez utiliser pour annoncer et promouvoir le mois de sensibilisation à la cybersécurité auprès de votre clientèle et au sein de votre organisation. Le CISA et la NCSA vous encouragent vivement à communiquer avec vos propres parties prenantes et votre organisation avant et pendant le mois d'octobre.

Exemple d'email aux clients :

Chers <clients ou groupe de parties prenantes>,

[INSÉRER LE NOM DE L'ORGANISATION] se joint à la campagne du mois de sensibilisation à la cybersécurité.

Chaque octobre, Cybersecurity Awareness Month continue de sensibiliser à l'importance de la cybersécurité dans notre pays. Dirigé par la Cybersecurity and Infrastructure Security Agency (CISA) et la National Cybersecurity Alliance (NCSA), Le Mois de la sensibilisation à la cybersécurité partage des messages et des thèmes hebdomadaires sur l'importance de rester en sécurité en ligne. Le thème éternel- **Faites votre part. #BeCyberSmart. –** encourage les individus et les organisations à assumer leur rôle dans la protection de leur partie du cyberespace, en insistant sur la responsabilité personnelle et l'importance de prendre des mesures proactives pour améliorer la cybersécurité.

Au cours de l'année et demie écoulée, notre monde déjà virtuel a dépendu encore davantage de l'internet. Des organisations comme [INSÉRER LE NOM DE L'ORGANISATION] et des individus comme vous se déplacent plus que jamais en ligne - pour se rencontrer, pour faire des affaires, et pour simplement s'amuser.

Si une présence accrue en ligne peut être positive, le Mois de la sensibilisation à la cybersécurité encourage chacun à à s'approprier une activité en ligne accrue et les importantes pratiques de sécurité qui l'accompagnent. La sécurité virtuelle de notre communauté et, en définitive, de notre nation, dépend de nos pratiques personnelles en matière de sécurité en ligne.

La cybersécurité est importante pour [INSÉRER LE NOM DE L'ORGANISATION] et nous nous sommes engagés à aider nos clients à devenir plus résilients. Tout au long du mois d'octobre, vous apprendrez à :

- **Soyez Cyber Smart**

  Prenez des mesures simples pour protéger nos vies numériques.

- **Combattez le Phish !**

  Nous mettrons en évidence les dangers des tentatives de phishing, qui peuvent conduire à des attaques de ransomware ou d'autres logiciels malveillants, et comment signaler les emails suspects.

- **Découvrez. Expérimentez Partagez.**

  Célébrez l'initiative nationale pour l'éducation à la cybersécurité (NICE) Cybersecurity Career Awareness Week et la main-d'œuvre mondiale en matière de cybersécurité, et mettre en évidence la façon dont les individus peuvent apprendre à devenir un professionnel de la cybersécurité.

- **Priorité à la cybersécurité**

  Explorez comment la cybersécurité et la sécurité en ligne sont de plus en plus importantes alors que nous continuons à fonctionner virtuellement dans notre travail et notre vie personnelle.

Nous devrions tous aborder la cybersécurité avec soin en possédant, sécurisant et protégeant tous nos comptes et informations en ligne. [INSÉRER LE NOM DE L'ORGANISATION] vous propose ces ressources que vous pouvez utiliser pour assurer votre sécurité en ligne :

- Site Web du Mois de la sensibilisation à la cybersécurité de CISA : cisa.gov/cybersecurity-awareness-month
- Les Cyber Essentiels de CISA - les meilleures pratiques de base en matière de cybersécurité pour les chefs d'entreprise : cisa.gov/cyber-essentials
- En savoir plus sur les carrières dans le cyber avec l'initiative nationale pour les carrières et les études en cybersécurité : niccs.cisa.gov

Si vous avez d'autres questions sur la façon dont [INSÉRER LE NOM DE L'ORGANISATION] s'implique dans l'email de la campagne du Mois de la sensibilisation à la cybersécurité de cette année [INSÉRER L'E-MAIL POC DE LA CAMPAGNE ORANIZATION'S CYBERSECURITY MONTH].

<Signature>

Exemple d'email au personnel :

Cher <nom de l'organisation>,

Cybersecurity Awareness Month aura lieu en octobre 2021 ! [INSÉRER LE NOM DE L'ORGANISATION] a rejoint la campagne annuelle menée par la Cybersecurity and Infrastructure Security Agency (CISA) et la National Cybersecurity Alliance (NCSA). La campagne montre comment les secteurs public et privé peuvent travailler ensemble et faire leur part pour construire un monde en ligne sécurisé. notre part individuelle dans la construction d'un monde en ligne sécurisé. Cette année, nous continuons à utiliser le thème général « **Faites votre part, #BeCyberSmart.** »

De nombreux cyberprofessionnels sont conscients des risques et des enjeux de notre monde de plus en plus virtuel. À [INSÉRER LE NOM DE L'ORGANISATION] nous voulons que vous nous aidiez à améliorer notre position en matière de cybersécurité et que vous utilisiez les connaissances acquises au travail pour aider les autres à adopter une approche sûre et consciente de la cybersécurité.

Tout au long du mois d'octobre, vous prendrez connaissance de quatre messages hebdomadaires :

- **SEMAINE 1 : Soyez Cyber Smart**
  Comment vous pouvez prendre des mesures simples pour assurer la sécurité de nos vies numériques.
- **SEMAINE 2 : Combattez le Phish !**
  Nous mettrons en évidence les dangers des tentatives de phishing, qui peuvent conduire à des attaques de ransomware ou d'autres logiciels malveillants, et comment signaler les emails suspects.
- **SEMAINE 3 : Découvrez. Expérimentez. Partagez.**
  Ensemble, nous célébrerons l'initiative nationale pour l'éducation à la cybersécurité (NICE) Cybersecurity Career Awareness Week et la main-d'œuvre mondiale en cybersécurité, organise notre propre salon de recrutement en cybersécurité et met en évidence les divers outils pédagogiques dont dispose la CISA.
- **SEMAINE 4 : La cybersécurité en premier.**
  Explorez comment la cybersécurité et la sécurité en ligne sont de plus en plus importantes alors que nous continuons à fonctionner virtuellement dans notre travail et notre vie personnelle.

Chacun de nous peut s'impliquer en octobre pour nous aider tous à être plus sûrs et sécurisés en ligne. Faites votre part.

#BeCyberSmart en utilisant les ressources suivantes :

Site Web du Mois de la sensibilisation à la cybersécurité de CISA : cisa.gov/cybersecurity-awareness-month

Les Cyber Essentiels de CISA - les meilleures pratiques de base en matière de cybersécurité pour les chefs d'entreprise : cisa.gov/cyber-essentials

En savoir plus sur les carrières dans le cyber avec l'initiative nationale pour les carrières et les études en cybersécurité : niccs.cisa.gov

Si vous avez d'autres questions sur la façon dont [INSÉRER LE NOM DE L'ORGANISATION] s'implique dans l'e-mail de la campagne du Mois de la sensibilisation à la cybersécurité de cette année [INSÉRER L'E-MAIL POC DE LA CAMPAGNE ORANIZATION'S CYBERSECURITY MONTH] ou si vous souhaitez signaler des activités suspectes à l'e-mail informatique [INSÉRER L'ADRESSE ÉMAIL LA PLUS PERTINENTE].

<Signature>