SOYEZ CYBER SMART

#CyberMonth

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2021

Qu’est-ce que le Mois de la sensibilisation à la cybersécurité?

Le Mois de la sensibilisation à la cybersécurité sensibilise à l’importance de la cybersécurité dans l’ensemble de notre pays.

Cybersécurité « Et alors ? »

Le saviez-vous?

Un logiciel antivirus est disponible pour les appareils mobiles, qui sont une cible facile et courante pour les pirates et autres acteurs malveillants.

Cybersécurité Bon sens

- Être en sécurité en ligne n'est pas si différent d'être en sécurité dans le monde physique!
- Restez calme et faites confiance à votre instinct!

Termes couramment utilisés

- Mauvais acteur
- Hacker
- Cyberattaque

Faites votre part.
#BeCyberSmart.

La cybersécurité commence par VOUS et est la responsabilité de **tous**.

Il existe actuellement une estimation
5,2 milliards d'internautes ou
63% de la population mondiale.

CYBERCRIMINALITÉ

Qu'est-ce que c'est ?

La cybercriminalité est tout crime commis par voie électronique.

Cela peut inclure...

- Le vol
- La fraude
- Parfois même le meurtre

Exemples

- Vol d'identité
- Matériel d'abus sexuel d'enfants
- Vol financier
- Violations de la propriété intellectuelle
- Malware
- Ingénierie sociale malveillante

Pourquoi devriez-vous vous en soucier ?

- Le crime est un danger hors ligne et en ligne !
- Les bases de la cyberdéfense peuvent contribuer grandement à vous garder, vous et vos données, hors des mains de mauvais acteurs.

MALWARE

Qu’est-ce que c’est ?

Tout logiciel destiné à…

- endommager
- désactiver
- Ou autorisez une personne non autorisée à accéder à votre ordinateur ou à un autre appareil connecté à Internet

Exemples

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Virus
- Vers

Pourquoi devriez-vous vous en soucier ?

- La plupart des cybercrimes commencent par une sorte de malware. Vous, votre famille et vos renseignements personnels est certainement à risque si les logiciels malveillants trouve son chemin sur votre ordinateur ou vos appareils.

RANSOMWARE

Qu’est-ce que c’est ?

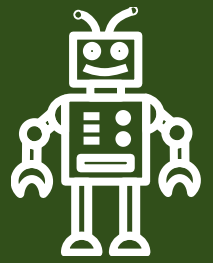
Malware conçu pour rendre les données ou le matériel inaccessibles à la victime jusqu'à ce qu'une rançon soit payée.

Exemples

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

Pourquoi devriez-vous vous en soucier ?

- Souvent téléchargé sous forme de liens de courrier électronique malveillants
- Atteinte à la fois à la stabilité financière et à la réputation
- Aucune garantie que vous récupérerez vos données, même si vous payez
- Souvent utilisé comme leurre pour d'autres activités malveillantes



BOTS

Qu’est-ce que c’est ?

Les bots sont un type de programme utilisé pour automatiser des tâches sur Internet.

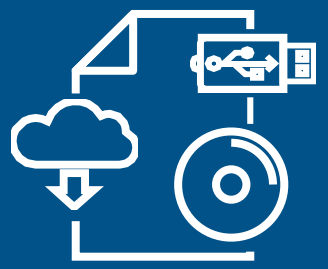
Le saviez-vous?

Tous les bots ne sont pas mauvais. Lorsque vous utilisez un moteur de recherche, ces résultats sont rendus possibles par l'aide de bots qui "explorent" l'internet et indexent le contenu. Les chatbots comme Siri et Alexa sont un autre type courant de "bon" bot.

Pourquoi devriez-vous vous en soucier ?

Les bots malveillants le peuvent :

- Recueillir les mots de passe
- Enregistrer les frappes de clavier
- Obtenir des informations financières
- Détourner des comptes de médias sociaux
- Utiliser votre e-mail pour envoyer des spams
- Ouvrir des portes dérobées sur le dispositif infecté



CYBERATTAQUES PHYSIQUES

Qu’est-ce que c’est ?

Les cyberattaques physiques utilisent du matériel, des dispositifs de stockage externes ou d'autres vecteurs d'attaque physiques pour infecter, endommager ou compromettre les systèmes numériques. Cela peut inclure...

- Dispositifs de stockage USB
- CD/DVD
- Internet des objets (IoT)

Pourquoi devriez-vous vous en soucier ?

- Facile à négliger
- Difficile à identifier et à détecter
- Extrêmement difficile à enlever
- Ils peuvent tout faire, de l'installation d'un ransomware à l'envoi de copies ou à la modification de systèmes d'information, en passant par le démantèlement de réseaux.

Le saviez-vous?

Tout ce qui est connecté à l'internet est potentiellement vulnérable, des scooters électriques aux ordinateurs portables en passant par les cargos.

L'INGÉNIERIE SOCIALE

Qu'est-ce que c'est ?

- Les cybercriminels peuvent profiter de vous en utilisant des informations communément disponibles par...
- Plateformes de médias sociaux
- Partage de l'emplacement
- Conversations en personne

Exemples

- Phishing
- Pretexting
- Baiting
- Quid pro quo
- Tailgating
- Inside job
- Swatting

Pourquoi devriez-vous vous en soucier ?

- Votre vie privée n'est pas seulement un luxe - c'est une mesure de sécurité
- Les attaques peuvent être réussies avec peu ou pas de connaissances ou de capacités de programmation.
- Les mesures de sécurité technologiques ne peuvent que vous protéger dans une certaine mesure - vous êtes votre meilleure défense.

PHISHING

Qu’est-ce que c’est ?

Faux messages provenant d'une source apparemment fiable ou réputée et destinés à vous convaincre de…

- Révéler des informations
- Donner un accès non autorisé à un système
- Cliquer sur un lien
- Vous engager dans une transaction financière

Exemples

- Courriels
- Messages texte
- Appels téléphoniques
- Messages et posts sur les médias sociaux
- Liens hypertextes suspects

Pourquoi devriez-vous vous en soucier ?

- Extrêmement courant
- Peut avoir de graves conséquences
- Le diable est dans les détails

Cet email vous tromperait-il ?

Nouveau message

De Legitimate-Looking-Source@notquiteyourworkemail.com

Sujet Mise à jour informatique urgente : Vulnérabilité des logiciels

Mise à jour du logiciel

Bon après-midi, Tom,

Une vulnérabalité a été identifiée dans "Big Name Software" qui permet à un attaquant d'enregistrer des appels et des vidéos depuis votre ordinateur à votre ins. Veuillez installer la mise à jour attaquée avant la fin de la journée ou votre poste de travail sera verrouillé.

Nous avons également créé une application pour tous les employés afin de détermin s'ils ont été affectés par cette vulnérabilité. **Cliquez** ici pour lancer l'application.

www.fakewebsite.com/gotcha.exe
Cliquez ou tapez pour suivre le lien.

Cordialement,
BossMann
Le département informatique de votre entreprise

RÉPONSE

SWATTING

Qu’est-ce que c’est ?

Une attaque centrée sur le partage de la localisation dans laquelle les mauvais acteurs appellent la police en prétendant que la victime a commis un crime...

- Alerte à la bombe
- Intrus armé
- Incident violent

Pourquoi devriez-vous vous en soucier ?

- Conséquences physiques et immédiates
- Parfois était simplement conçu comme une farce
- Une arrestation et des blessures graves peuvent en résulter
- Réduisez les risques en partageant votre position uniquement avec des personnes de confiance et ne partagez vos photos de vacances qu'une fois que vous êtes rentré sain et sauf chez vous

Exemples

Votre position est intégrée sous forme de métadonnées dans chaque photo que vous prenez avec votre téléphone. Désactivez les services de localisation lorsque vous ne les utilisez pas afin qu'il soit plus difficile pour les personnes mal intentionnées de consulter ces informations.

D'AUTRES VOIES D'ATTAQUE

Qu'est-ce que c'est ?

- Internet de tout
- Tout appareil connecté à votre réseau
- Collecte d'informations
- Accès à distance
- Bluetooth
- Ports ouverts

Exemples

- Appareils intelligents
- Téléphone portable
- Thermostat
- Véhicules
- Consoles de jeux
- Imprimantes
- Équipement médical
- Systèmes industriels

Pourquoi devriez-vous vous en soucier ?

- Votre réseau peut être utilisé pour attaquer quelqu'un d'autre
- Tout appareil qui stocke des informations ou qui est connecté à Internet peut être une vulnérabilité
- Supposez que vous êtes vulnérable et prenez des mesures pour comprendre et atténuer les risques
- Ne soyez pas le « fruit à portée de main »

Comment mieux se protéger en ligne ?

Sécurisez vos réseaux.

Les routeurs sans fil sont un moyen pour les cybercriminels d'accéder aux appareils en ligne.

Si vous le connectez, protégez-le.

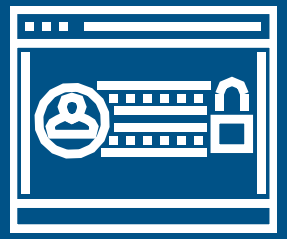
Une défense éprouvée contre les intrusions est la mise à jour vers le dernier logiciel de protection antivirus.

Restez à jour.

Gardez le logiciel à jour avec les dernières versions et configurez le logiciel de sécurité pour exécuter des analyses régulières.

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.



Conseils sur les mots de passe

Le saviez-vous?

Le bourrage de mot de passe ou de justificatif est une cyberattaque qui tente de "bourrer" des noms d'utilisateur et des mots de passe déjà compris d'un site vers un autre site dans l'espoir que l'utilisateur utilise les mêmes informations de connexion sur toutes les plateformes.

- ****** Utilisez des mots de passe différents sur différents systèmes et comptes
- ****** Utilisez le mot de passe le plus long autorisé
- ****** Utilisez un mélange de lettres majuscules et minuscules, de chiffres et de symboles.
- ****** Réinitialisez votre mot de passe tous les deux mois
- ****** Utilisez un gestionnaire de mots de passe

Thème du mois de la sensibilisation à la cybersécurité

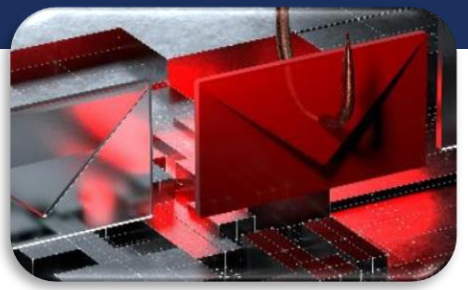
Thème :

- **Faites votre part. #BeCyberSmart.**

Programme du mois de la sensibilisation à la cybersécurité 2021

1er octobre :
Coup d'envoi officiel

SEMAINE 1 :
Semaine du 4 octobre
SOYEZ Cyber Smart.

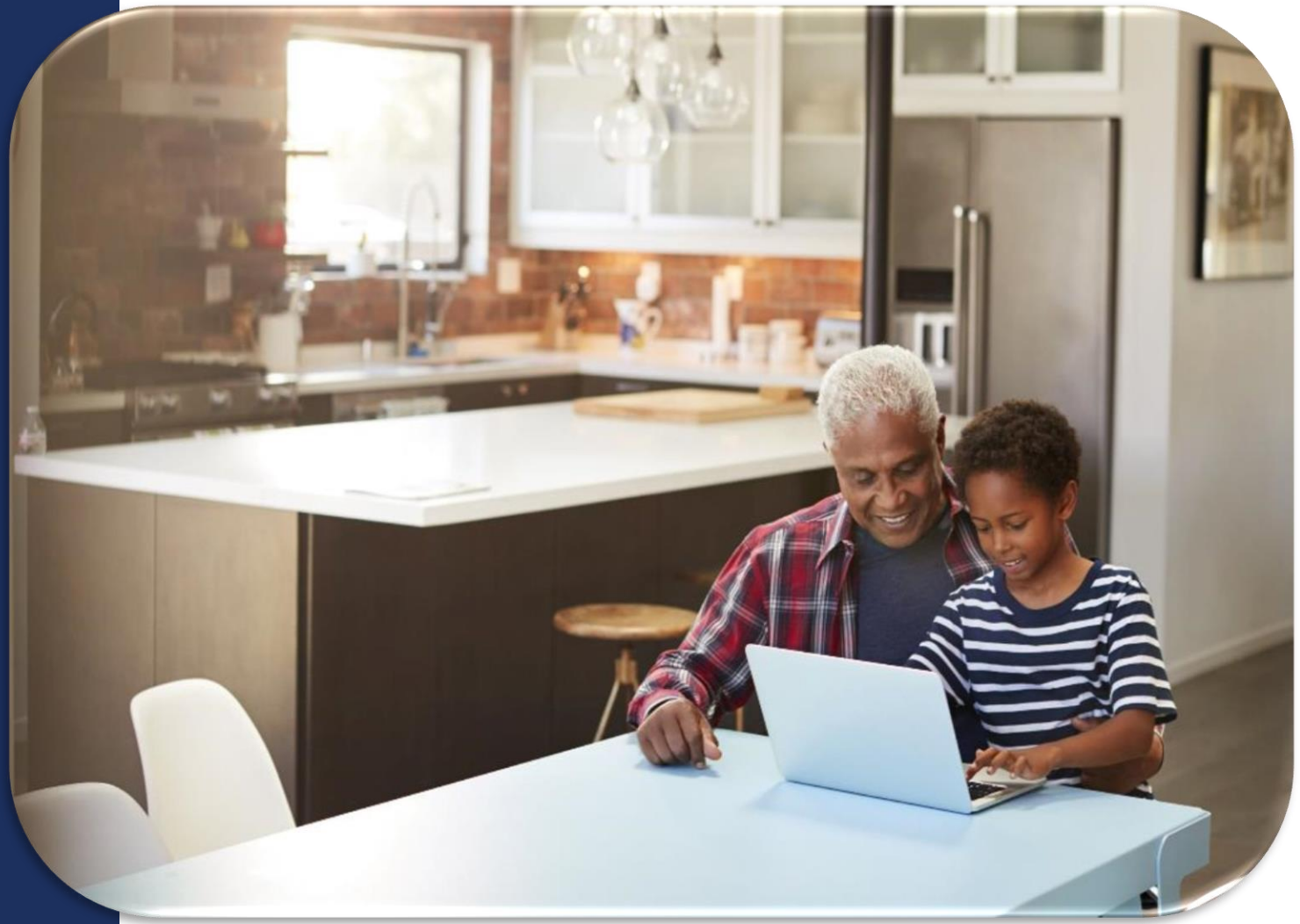


SEMAINE 2 :
Semaine du 11 octobre
Combattez le Phish !

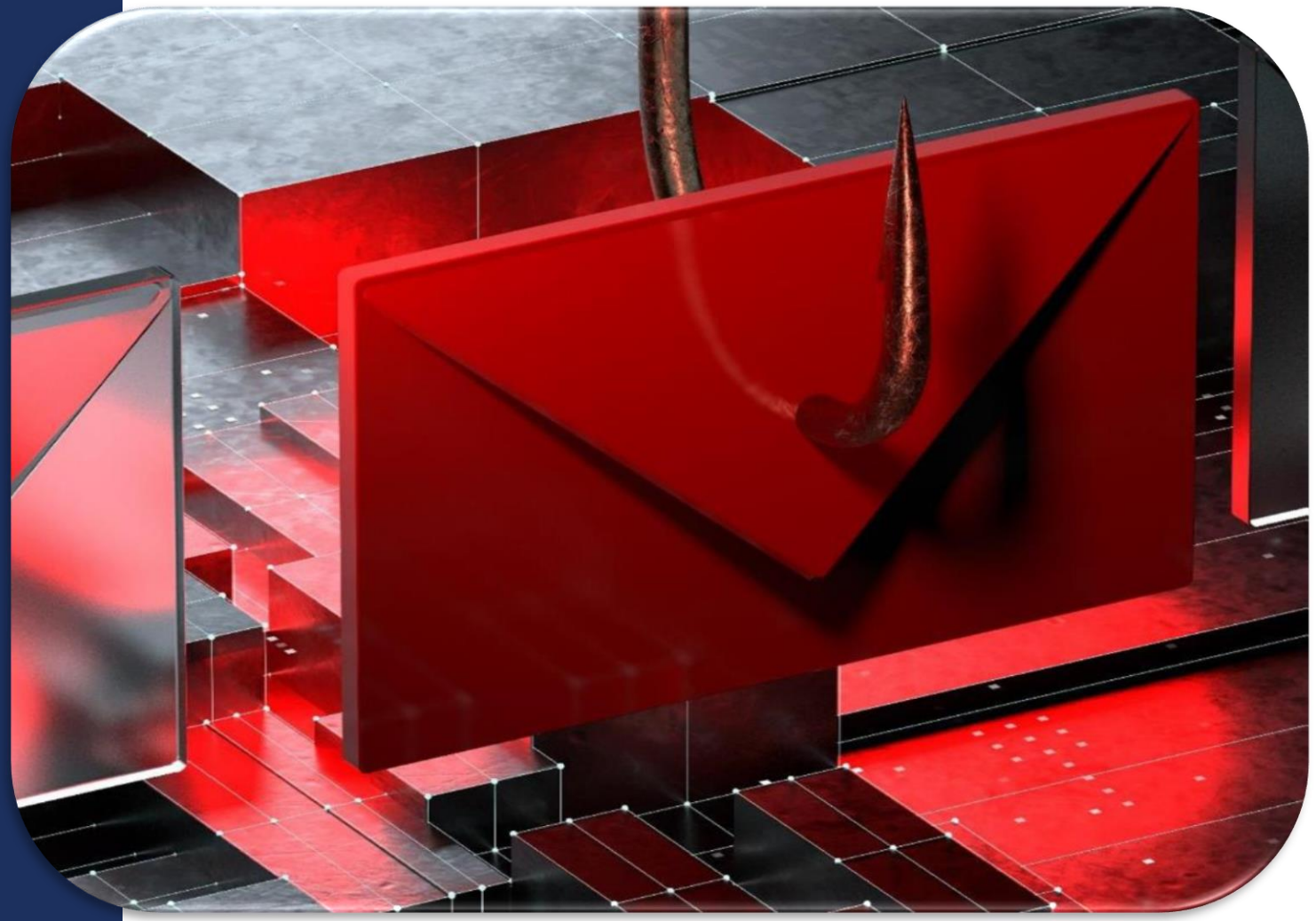
SEMAINE 3 :
Semaine du 18 octobre
Découvrez. Expérimentez. Partagez. (Semaine de sensibilisation aux carrières en cybersécurité)

SEMAINE 4 :
Semaine du 25 octobre
La cybersécurité en premier.

SEMAINE 1 :
Soyez Cyber Smart.



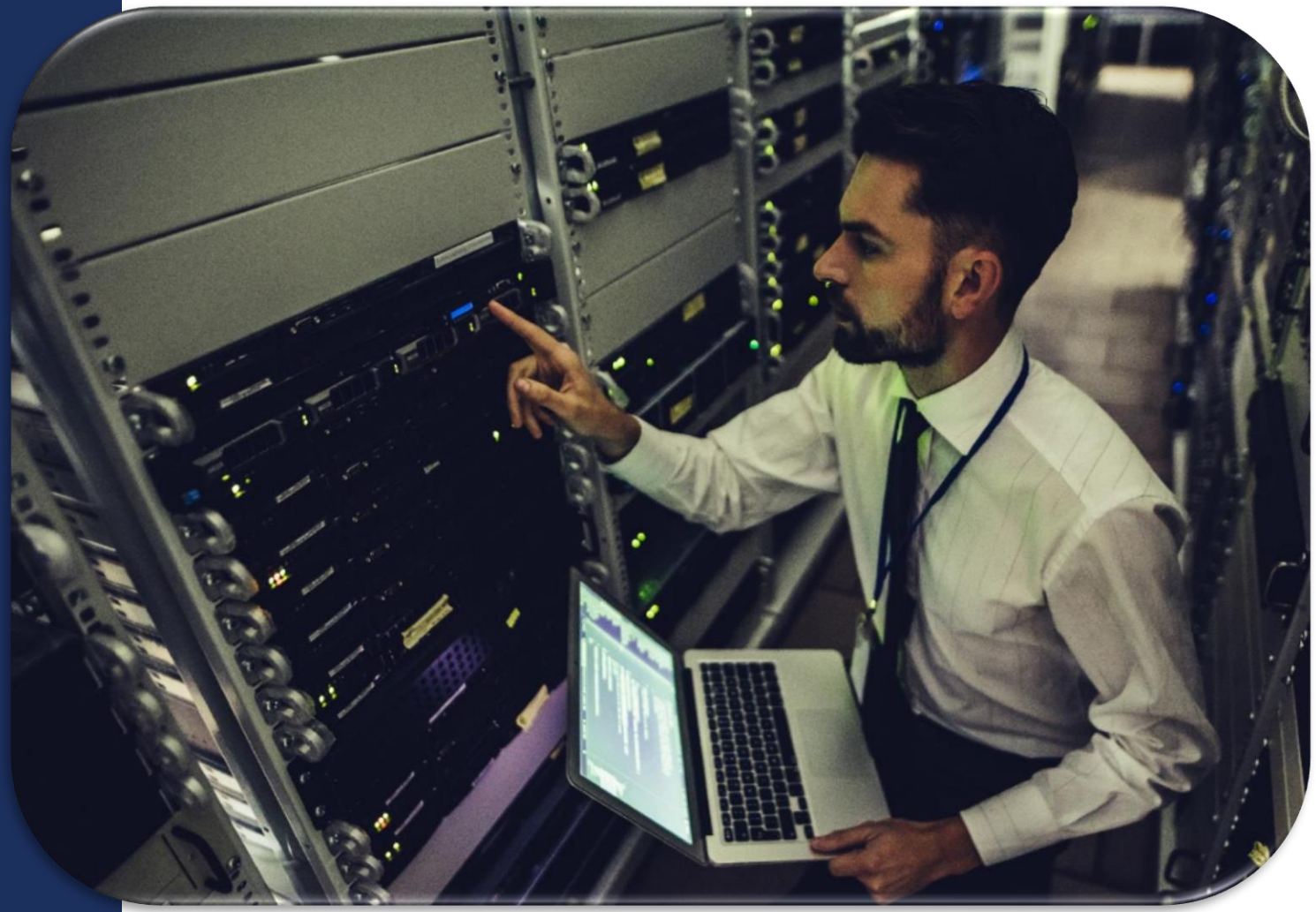
SEMAINE 2 :
Combattez le Phish !



SEMAINE 3 :

Découvrez.
Expérimentez.
Partagez.

Semaine de sensibilisation aux carrières en cybersécurité



SEMAINE 4 :
La cybersécurité en premier.

Sensibilisez et impliquez-vous

- Devenez un champion du mois de la cybersécurité
- Promouvoir le mois de sensibilisation à la cybersécurité sur les médias sociaux ; utiliser le #BeCyberSmart hashtag
- Se porter volontaire pour prendre la parole lors des engagements du mois de sensibilisation à la cybersécurité
- Transmettez des conseils de cybersécurité à vos amis, votre famille et vos collègues de travail.

Pour plus d'information, contactez le CyberAwareness@cisa.dhs.gov

Visitez cisa.gov/cybersecurity-awareness-month ou staysafeonline.org/cybersecurity-awareness-month/ pour plus de ressources.