TERRANOVA SECURITY

La sensibilisation à la cybersécurité est l'affaire de tous

Pourquoi et comment faire de la sensibilisation à la cybersécurité

Theo Zafirakos
CISO et coach en sensibilisation à la sécurité
Terranova Security

À propos de Terranova

Terranova est un chef de file mondial en matière de sensibilisation à la cybersécurité, reconnu par Gartner, cumulant plus de 1000 programmes de simulation d'hameçonnage et de sensibilisation à la cybersécurité pour plus de 6 millions d'utilisateurs.

TERRANOVA SECURITY

Objectifs

Obtenir des astuces et des recommandations sur comment réussir la mise en œuvre d'un programme de sensibilisation à la sécurité de l'information.

Pourquoi les organisations ont-elles besoin de programmes de sensibilisation à la cybersécurité?

L’hameçonnage, la plus grande menace pour les utilisateurs et les organisations

Rançongiciel

Utilisé pour détruire les données

Fraude

Utilisé pour commettre des fraudes financières

Mots de passe

Utilisé pour voler des mots de passe

Logiciel Malveillant

Utilisé pour transmettre des logiciels malveillants

Information

Utilisé pour voler des informations sensibles

L’hameçonnage en chiffres

- Combien de temps prend une attaque par hameçonnage pour compromettre sa première victime?
- Combien de jours, en moyenne, un fraudeur peut-il rester dans un système sans que l’intrusion soit détectée?
- Quel pourcentage d’utilisateurs cliquent sur un lien provenant d’une source inconnue ?
- Quel pourcentage d’utilisateurs croient automatiquement à la légitimité d’un courriel, lorsque le message provient d’une source connue ?
- Quel est le pourcentage d’utilisateurs qui réutilisent leurs mots de passe ?

- **80 secondes** (WIRED)
- **99 jours** (FireEye)
- **50 %** (TechRepublic)
- **70 %** (Terranova Security)
- **73 %** (Entrepreneur)

Pourquoi faire de la sensibilisation (page 1 de 2)

- **Maintenir la conformité**

Respecter diverses réglementations en matière de protection des données, de confidentialité et de gouvernance informatique à l'aide d'un programme de formation.

- **Rester opérationnel**

Comme les employés sont souvent la première ligne de défense, on a besoin d'un programme de sensibilisation comme mécanisme de défense pour minimiser la fréquence des attaques qui ont un impact sur votre organisation.

- **Réduire les dépenses**

Minimiser les coûts associés aux incidents qui pourraient entraîner une interruption de vos services, une perte de productivité, une fuite de données ou le mécontentement des clients.

Pourquoi faire de la sensibilisation (page 2 de 2)

- **Clarifier les responsabilités**

Clarifier et communiquer les responsabilités liées à la gestion des ressources informatiques et technologiques. La sécurité de l'information est la responsabilité de tous.

- **Maintenir la crédibilité**

Utiliser le programme de sensibilisation pour maintenir ou accroître la crédibilité et la confiance auprès des clients, des parties prenantes internes et externes et des auditeurs.

- **Instaurer une culture de sensibilisation**

Promouvoir la compréhension des risques liés à l'information et à la technologie, réduisant ainsi le risque global pour votre organisation.

Créer une culture consciente de la sécurité - Les défis

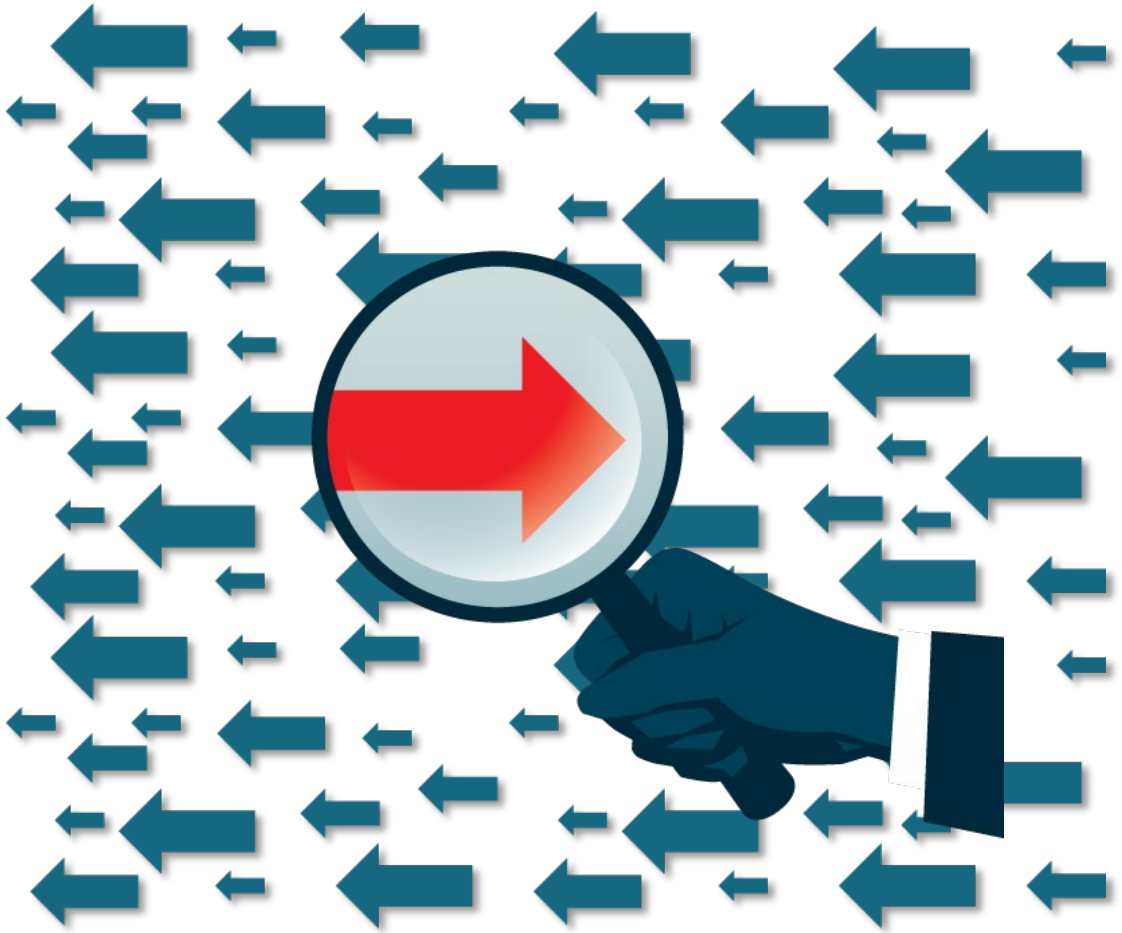
- La culture de sécurité ne consiste pas simplement à appliquer les meilleures pratiques.
- Les utilisateurs pensent que leurs actions ne font aucune différence.
- Souvent, les entreprises ne donnent pas aux utilisateurs les outils nécessaires pour prendre les bonnes décisions.
- La relation directe entre les cybermenaces et l'impact sur les services d’affaires n'est pas démontrée.
- Nécessité de défaire les perceptions négatives de la cybersécurité.

Comment sensibiliser les utilisateurs aux cyber menaces et aux meilleures pratiques en matière de cybersécurité?

Tout le monde doit participer à la solution

Dans l'environnement numérique actuel, les criminels tentent de plus en plus d'infiltrer des réseaux personnels ou commerciaux.

Il est important que **nous comprenions tous comment identifier une menace,** ainsi que les mesures à mettre en place pour empêcher l'accès non autorisé à vos systèmes informatiques afin de protéger nos renseignements.



Les composantes d'un programme complet

1. Une approche éprouvée pour établir un programme efficace
2. Du matériel de formation et des outils de renforcement
3. Un calendrier de communication
4. Des outils de mesure et des rapports
5. Une équipe de gestion du programme
6. Un budget

Les étapes d'un programme de sensibilisation efficace

Analyse

Précisez vos objectifs de programme et de campagne, puis identifiez votre public cible.

Planification

Établissez le plan de déploiement de votre feuille de route, votre plan de projet et votre plan de communication.

Déploiement

Déployez vos campagnes, entretenez une communication constante avec votre public cible et insistez sur les messages clés.

Mesure

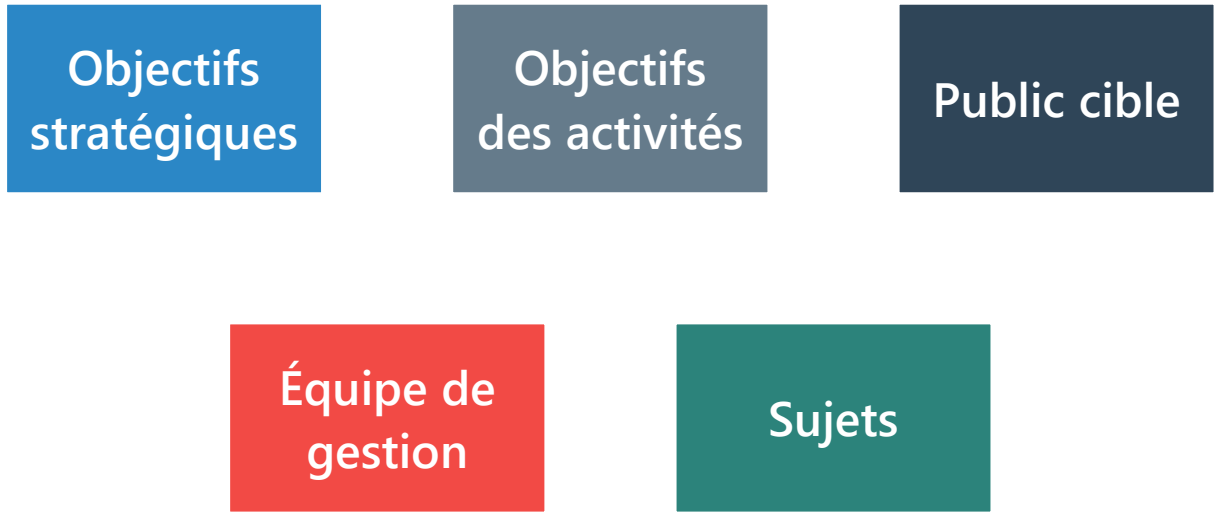
Utilisez des indicateurs pour évaluer le succès de votre programme et déterminer si vous atteignez vos objectifs.

Optimisation

Comparez vos objectifs avec les résultats et identifiez de nouveaux objectifs. Effectuez la mise à jour de votre programme de sensibilisation au moins une fois par année.

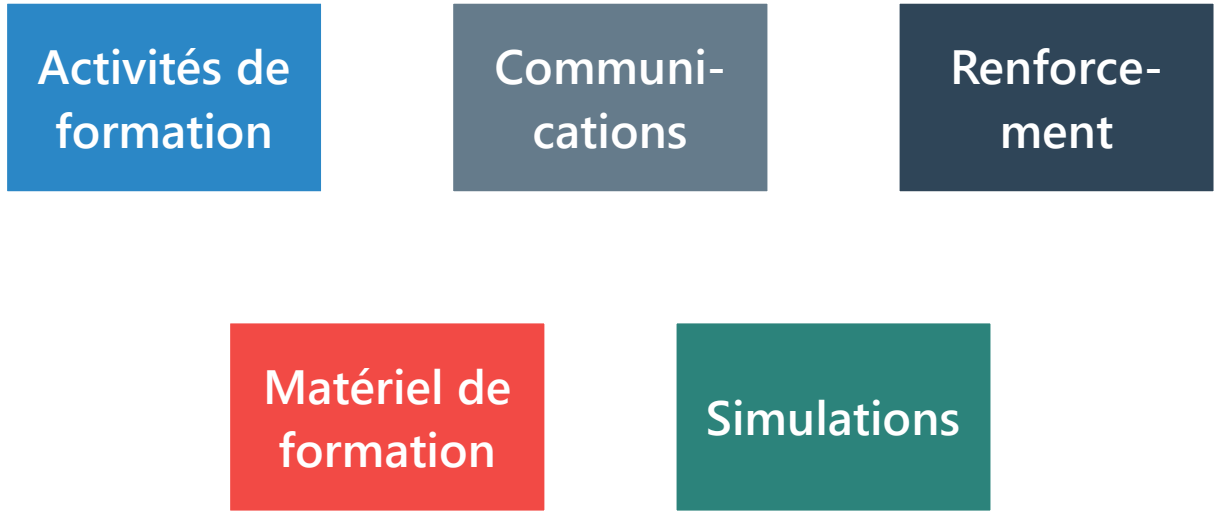
Analyse des besoins

Les objectifs doivent soutenir la vision stratégique du programme de sensibilisation et aident à justifier les raisons pour lesquelles le programme est en place.



Planification

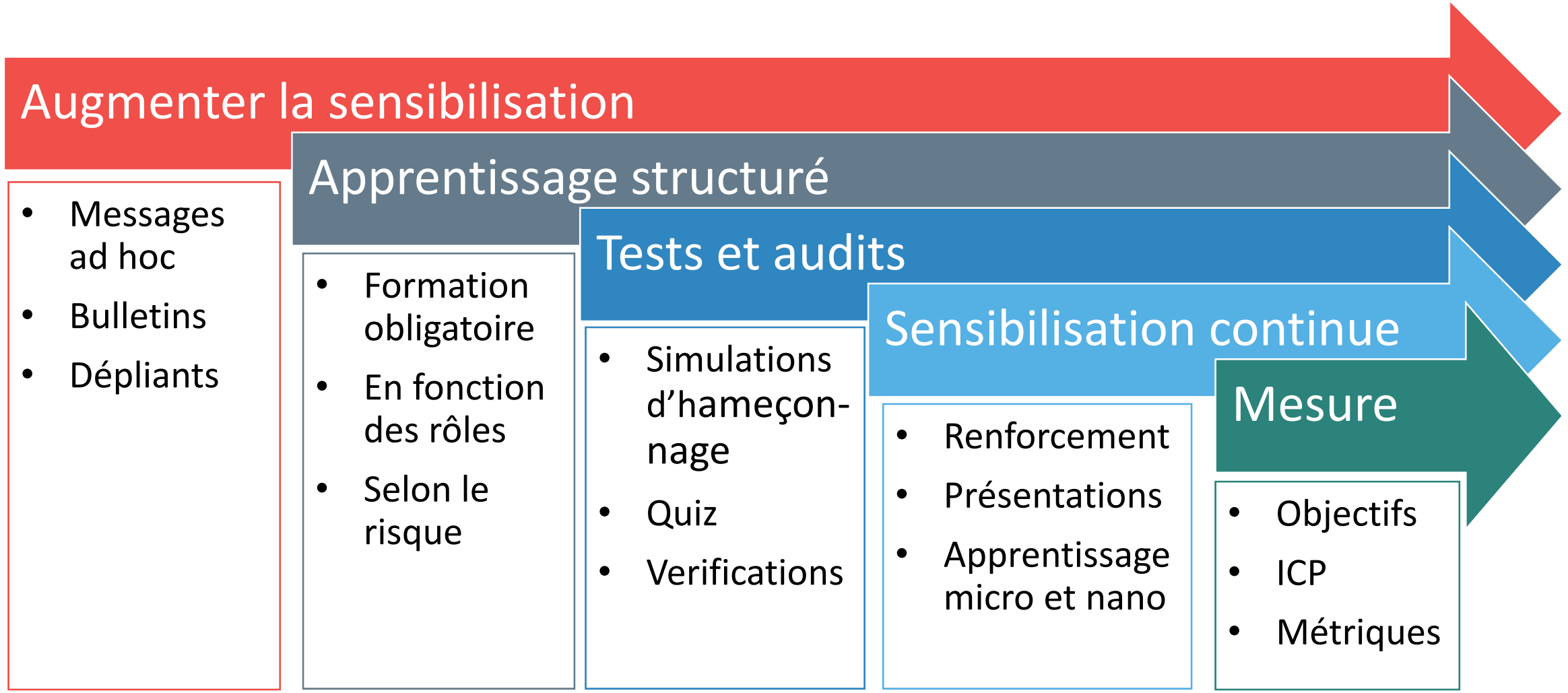
Sur la base des résultats de l'analyse, préparez une stratégie de sensibilisation et un plan qui répondra aux exigences.



Produits d’un programme de sensibilisation

1. Plateforme de sensibilisation, quiz et simulations
2. Contenu de sensibilisation à la sécurité de l’information et cours en ligne
3. Activités de renforcement (micro- ou nano- activités d’apprentissage)
4. Matériel de communication (affiches, bulletins, fonds d’écran)

Mise en œuvre d'un programme de sensibilisation



Quelles sont les principales cyber menaces aux quelles les organisations doivent faire attention?

Sujets clés pour la sensibilisation à la sécurité

Mots de passe

Courriel & Internet

Principe du « bureau propre »

Hameçonnage

Réseaux sociaux

Protection des données

Messages clés pour les utilisateurs

- Ne faites pas confiance aux messages inhabituels ou inattendus, particulièrement ceux venant d'expéditeurs inconnus.
- N'ouvrez pas de pièces jointes douteuses et n'activez pas les macros de documents Office.
- Ne visitez pas de liens Web inconnus ou suspects.
- Tapez vos mots de passe seulement aux écrans de connexion que vous reconnaissez et ne les partagez jamais avec quiconque.
- Traitez vos renseignements personnels et commerciaux avec soin et gardez-les confidentiels.
- Respectez les politiques et directives d'entreprise.

Menace interne non intentionnelle
Comportements à risque

1. Contourner les contrôles de sécurité
2. Ignorer les politiques et procédures de sécurité
3. Laisser un appareil sans protection et sans surveillance
4. Jeter des documents sensibles dans des bacs de recyclage non sécurisés
5. Installer des applications non approuvées
6. Visiter des sites Web à haut risque

Menace interne intentionnelle
Que pouvons-nous faire?

- Surveiller les employés mécontents qui peuvent utiliser leur position pour se venger et causer des dommages graves à votre entreprise.
- Surveillez les employés qui travaillent à des heures inhabituelles ou qui apportent beaucoup d'informations à la maison.
- Changements de l'état financier. Une personne en difficulté financière peut vendre des informations sensibles.
- Vérifiez les activités des 90 derniers jours de tout employé ayant accès aux données sensibles et qui ont quitté l'entreprise.

Prochaines étapes

- Attribuer à quelqu'un la responsabilité de préparer et de gérer le programme
- Déterminer les exigences de sensibilisation
- Déterminer les capacités internes de préparer et gérer le programme
- Sélectionner le contenu du programme (développer en interne ou acheter)
- Sélectionnez une plate-forme pour héberger votre programme (interne ou externe)
- Annoncez votre programme (idéalement par la haute direction)
- Déployer vos activités, suivre les performances, ajuster le programme

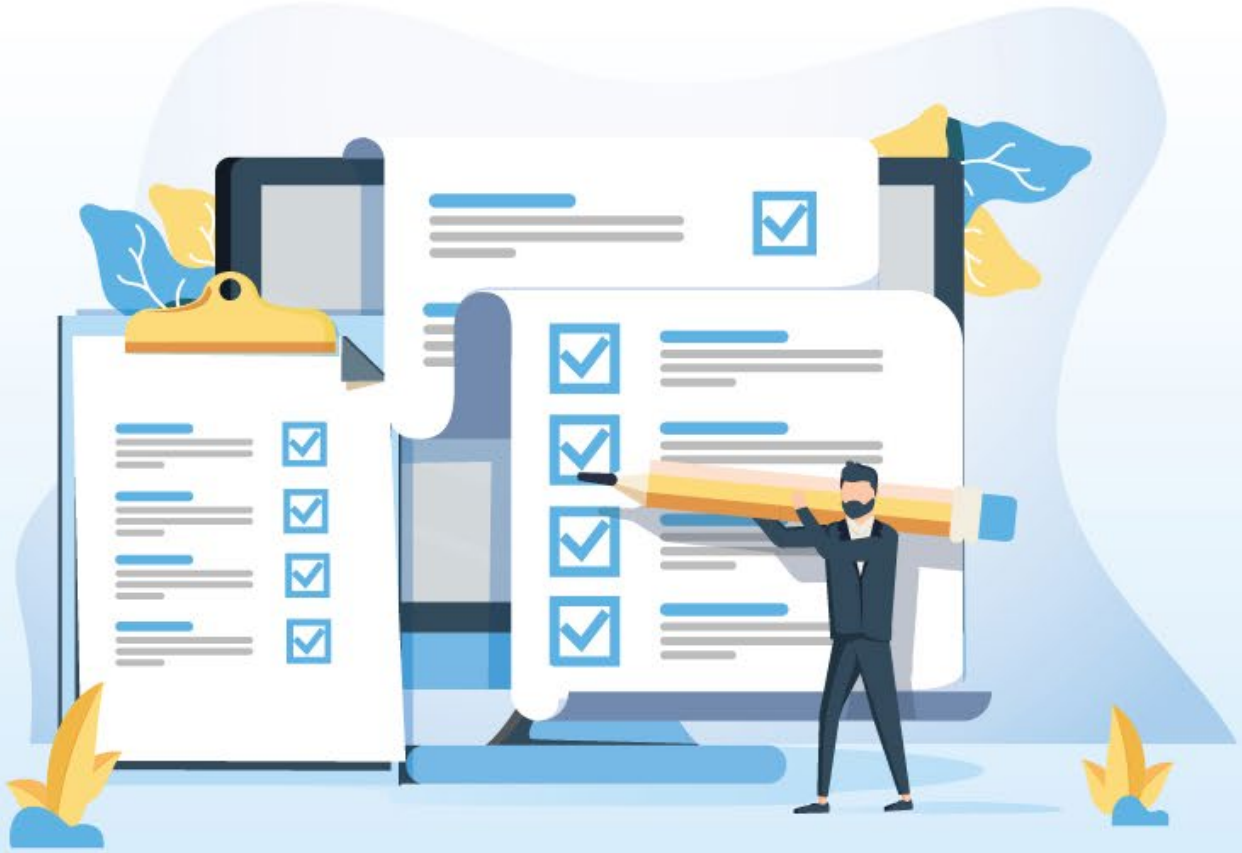
Trousse de protection pour votre ordinateur à la maison

Un cours interactif et des ressources pour la maison dans le cadre du Mois national de la sensibilisation à la cybersécurité!

Nous vous invitons à partager cette trousse avec les employés, les collègues, la famille et les amis pour les aider à mieux se protéger contre les cyber menaces tant au travail qu'à la maison.

Obtenir ma trousse

Terranovasecurity.com/fr/ncsam-kit-2019/



Autres ressources

Terranova Security

- Fiche d'évaluation de votre programme (en anglais seulement)

https://terranovasecurity.com/fr/evaluation-cyber-securite/

- Blogue de sensibilisation à la cybersécurité et autres ressources

https://terranovasecurity.com/fr/blogue/

Autres

- Pensez cybersécurité (Gouvernement du Canada)

https://www.pensezcybersecurite.gc.ca/index-fr.aspx

- Protéger votre entreprise contre les cyberattaques (Desjardins)

https://www.desjardins.com/proteger-entreprise-contre-cyberattaques/

Continuons la discussion!

Un membre de notre équipe est à votre disposition pour vous fournir des informations sur nos outils de simulation d'hameçonnage et de sensibilisation à la cybersécurité.

- 1-514-489-5806
- Sans frais: 1-866-889-5806
- info@terranovasecurity.com
- www.terranovasecurity.com