

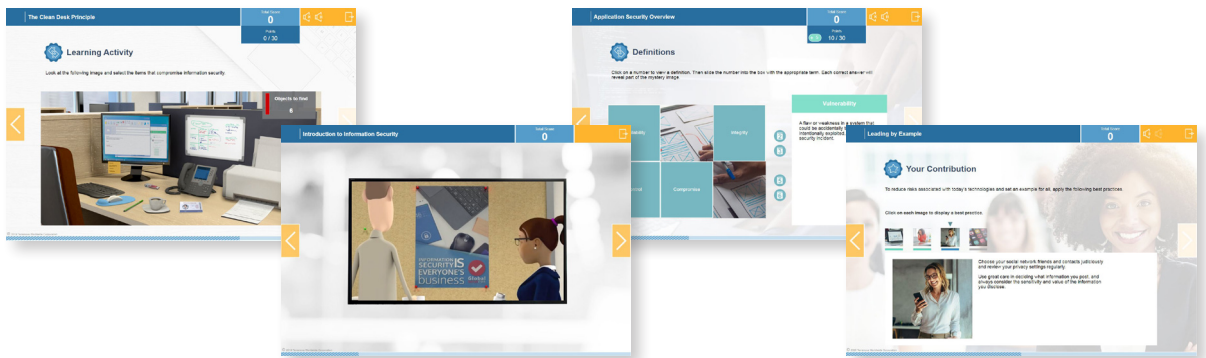
Programme de sensibilisation à la sécurité - Cliquez et lancez !

Des campagnes prêtes à l'emploi, faciles à déployer

Bénéficiez d'une exceptionnelle expérience de sensibilisation à la sécurité prête à l'emploi, facile à utiliser et à déployer. Lancez des campagnes de formation et des simulations de phishing en quelques clics seulement et réalisez rapidement un solide retour sur investissement en transformant les utilisateurs en cyberhéros !



EN SAVOIR PLUS !



Sécurisez vos informations sensibles

Créez facilement un programme efficace de formation en cybersécurité, aussi simple à mettre en place qu'à gérer. En proposant un contenu préconfiguré qui met à profit plus de 20 ans d'expertise en matière de cybersécurité, Terranova Security vous permet d'offrir une incroyable expérience d'apprentissage immersive qui répond à vos besoins et à vos objectifs.



**Cours informatifs
prédéfinis**



**Simulations de phishing
tirées du monde réel**



**Formats de formation
variés et attrayants**



**Interface utilisateur
intuitive, facile à utiliser**



**Format adapté à
l'apprentissage mobile**



**Approche d'apprentissage
inclusive**

Sélectionnez votre programme de formation en cybersécurité *Cliquez et Lancez* pour former vos cyberhéros

NOMBRE TOTAL DE CAMPAGNES DE SENSIBILISATION À LA SÉCURITÉ PAR AN

FRÉQUENCE DE DÉPLOIEMENT

SUJETS INCLUS

Appareils mobiles

Courrier électronique

Cycle de vie de l'information

Fuite de données

Hameçonnage

Ingénierie sociale

Introduction à la sécurité de l'information

Logiciels malveillants

Menace interne non intentionnelle

Mots de passe

Signalement des incidents

Télétravail

OUTILS DE COMMUNICATION ET DE RENFORCEMENT

Bulletins, affiches, fonds d'écran et bannières web

SIMULATION DE PHISHING

FORMATION DE RENFORCEMENT POUR LES UTILISATEURS QUI ONT CLIQUÉ SUR UNE SIMULATION DE PHISHING

Micro-learning Topics

- Compromission de courriers électroniques professionnels
- Rançongiciel
- Hameçonnage ciblé
- Hameçonnage Web

Nanolearning Topics

- Usurpation d'identité - Exemple d'attaque
- Hameçonnage - Six indices qui devraient soulever des doutes
- Rançongiciel
- Harponnage - La fraude au président

COURS COMPLÉMENTAIRES FACULTATIFS

Basé sur le rôle - Sensibilisation à la sécurité de l'information pour :

- Administrateurs TI
- Développeurs TI
- Finances
- Managers
- Ressources humaines

Serious Game:

- Télétravail: Mot de passe robuste

CHAMPION



1

Annuel

6



6 sujets

2 comportements par trimestre

2 sujets par trimestre



Ajout sur demande

ÉTOILE



4

Trimestriel

12



12 sujets

2 comportements par trimestre

2 sujets par trimestre



Ajout sur demande

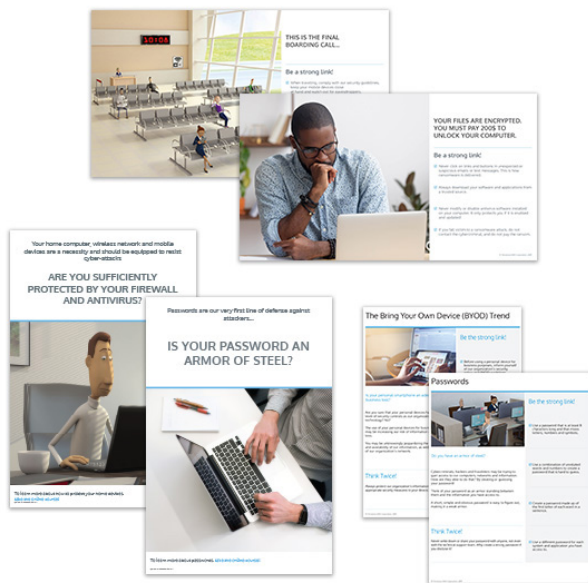
Plan pour les campagnes de niveau Champion

	T1	T2	T3	T4
<p>Étape 1</p> <p>Déployer une simulation initiale de phishing de référence</p> <p>Déployer un questionnaire de référence en guise de suivi</p>	<p>Clic sur un lien et divulgation du mot de passe</p> <p>(12 questions prédéfinies)</p>			
<p>Étape 2</p> <p>Annoncer et déployer votre campagne de formation annuelle</p>	<p>Connaissance générale SSI (30 minutes)</p> <ul style="list-style-type: none"> • Introduction à la sécurité de l'information • Mots de passe • Hameçonnage • Logiciels malveillants • Fuite de données • Signalement des incidents 			
<p>Étape 3</p> <p>Distribuer des outils de renforcement (Bulletins, affiches, fonds d'écran et bannières web)</p>	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2
<p>Étape 4</p> <p>Déployer une simulation de phishing tirée du monde réel, ciblant les comportements des utilisateurs</p>	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Divulgation des données relatives au mot de passe 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un bouton • Ouverture d'une pièce jointe malveillante 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Fourniture des données PII 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Fourniture des données PFI
<p>Étape 5</p> <p>Déployer une formation de renforcement pour les utilisateurs qui ont cliqué sur une simulation de phishing</p> <ul style="list-style-type: none"> • 1 Micro-learning (ML) • 1 Nano-learning (NL) 	<p>(ML)</p> <ul style="list-style-type: none"> • Hameçonnage Web <p>(NL)</p> <ul style="list-style-type: none"> • Hameçonnage - Six indices qui devraient soulever des doutes 	<p>(ML)</p> <ul style="list-style-type: none"> • Rançongiciel <p>(NL)</p> <ul style="list-style-type: none"> • Rançongiciel 	<p>(ML)</p> <ul style="list-style-type: none"> • Hameçonnage ciblé <p>(NL)</p> <ul style="list-style-type: none"> • Usurpation d'identité - Exemple d'attaque 	<p>(ML)</p> <ul style="list-style-type: none"> • Compromission de courriers électroniques professionnels <p>(NL)</p> <ul style="list-style-type: none"> • Harponnage - La fraude au président

Plan pour les campagnes de niveau Étoile

	Campagne #1 T1	Campagne #2 T2	Campagne #3 T3	Campagne #4 T4
<p>Étape 1</p> <p>Déployer une simulation initiale de phishing de référence</p> <p>Déployer un questionnaire de référence en guise de suivi</p>	<p>Clic sur un lien et divulgation du mot de passe</p> <p>(12 questions prédéfinies)</p>			
<p>Étape 2</p> <p>Annoncer et déployer votre campagne de formation trimestrielle</p>	<p>Sujets:</p> <ul style="list-style-type: none"> • Introduction à la sécurité de l'information • Ingénierie sociale • Mots de passe 	<p>Sujets:</p> <ul style="list-style-type: none"> • Hameçonnage • Logiciels malveillants • Signalement des incidents 	<p>Sujets:</p> <ul style="list-style-type: none"> • Courrier électronique • Appareils mobiles • Télétravail 	<p>Sujets:</p> <ul style="list-style-type: none"> • Cycle de vie de l'information • Menace interne non intentionnelle • Fuite de données
<p>Étape 3</p> <p>Distribuer des outils de renforcement (Bulletins, affiches, fonds d'écran et bannières web)</p>	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2	Partager des outils de renforcement alignés sur les sujets de l'étape 2
<p>Étape 4</p> <p>Déployer une simulation de phishing tirée du monde réel, ciblant les comportements des utilisateurs</p>	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Divulgation des données relatives au mot de passe 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un bouton • Ouverture d'une pièce jointe malveillante 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Fourniture des données PII 	<p>Comportements:</p> <ul style="list-style-type: none"> • Clic sur un lien • Fourniture des données PFI
<p>Étape 5</p> <p>Déployer une formation de renforcement pour les utilisateurs qui ont cliqué sur une simulation de phishing</p> <ul style="list-style-type: none"> • 1 Micro-learning (ML) • 1 Nano-learning (NL) 	<p>(ML)</p> <ul style="list-style-type: none"> • Hameçonnage Web <p>(NL)</p> <ul style="list-style-type: none"> • Hameçonnage - Six indices qui devraient soulever des doutes 	<p>(ML)</p> <ul style="list-style-type: none"> • Rançongiciel <p>(NL)</p> <ul style="list-style-type: none"> • Rançongiciel 	<p>(ML)</p> <ul style="list-style-type: none"> • Hameçonnage ciblé <p>(NL)</p> <ul style="list-style-type: none"> • Usurpation d'identité - Exemple d'attaque 	<p>(ML)</p> <ul style="list-style-type: none"> • Compromission de courriers électroniques professionnels <p>(NL)</p> <ul style="list-style-type: none"> • Harponnage - La fraude au président

Outils de communication et de renforcement



Renforcez l'engagement des employés avec une gamme diversifiée d'outils de communication, enrichie régulièrement

Affiches

Mettez en valeur votre programme de formation avec des visuels adaptables à votre marque.

Bulletins

Des mises à jour sur votre formation et la mise en valeur des bonnes pratiques en sécurité envoyées directement à vos utilisateurs.

Fonds d'écran et bannières web

Renforcez la participation à votre programme avec des messages numériques percutants et inspirants.

Formation de sensibilisation à la sécurité multilingue

La formation de champions de la cybersécurité est une tendance mondiale, ce qui fait de la langue une composante essentielle. Donnez à vos employés la possibilité de suivre la formation de sensibilisation à la sécurité dans la langue de leur choix.

EN	Anglais	JA	Japonais
EN-GB	Anglais (Royaume-Uni)	PT	Portugais (Brésil)
FR	Français (Canada)	RU	Russe
FR-FR	Français (France)	ZH-HK	Chinois (Hong Kong) (script traditionnel; narration cantonnais)
ES	Espagnol (Amérique Latine)	ZH-CN	Chinois (RPC*) (script simplifié; narration mandarin)
ES-ES	Espagnol (Espagne)		
DE	Allemand		
IT	Italien		

Des langues supplémentaires sont disponibles sur demande.

*RPC : République Populaire de Chine

Terranova Security et Microsoft :

Offrir aux utilisateurs le meilleur contenu de sensibilisation à la sécurité

Terranova Security est le partenaire de choix de Microsoft pour aider les organisations du monde entier à tirer profit d'un contenu de grande qualité pour renforcer la protection de leurs données. Le matériel de formation de Terranova Security s'appuie également sur les informations en temps réel de Microsoft concernant le phishing pour illustrer les cybermenaces les plus récentes et aider les utilisateurs à sécuriser tous les types d'informations.

Distinctions de l'industrie

Gartner



Reconnaissance par Gartner dans son Market Guide 2021 comme fournisseur représentatif pour :

Sensibilisation à la sécurité – formation assistée par ordinateur

L'excellence du service à la clientèle est une force directrice et une valeur fondamentale pour toute l'équipe de Terranova Security.

Cette distinction est la confirmation par nos clients que nous faisons une différence et que nous les soutenons dans leur démarche de sensibilisation à la sécurité.

Rapport du quadrant des données de sensibilisation à la sécurité et de l'information 2021.

Gagnant Or - Sensibilisation à la sécurité de l'information

Contenu engageant et informatif pour tous les utilisateurs

Accédez à un contenu sur la sécurité de l'information éducatif, amusant, et facilement partageable avec la nouvelle ressource gratuite de Terranova Security : le Hub de Cybersécurité!



Parmi les sujets traités dans le Hub (il y en a plusieurs autres!) :

- Phishing
- Social Engineering
- Télétravail
- Mots de passe robustes

ACCÉDER AU HUB

* Le Hub est mis à jour régulièrement, aussi consultez-le souvent pour profiter des plus récentes vidéos, infographies, et plus.