TERRANOVA SECURITY

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 données

Créez facilement un programme efficace de formation en cybersécurité , aussi simple à mettre en place qu'à gérer. 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 puissante 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* et formez vos cyberhéros

	CHAMPION	ÉTOILE
NOMBRE TOTAL DE CAMPAGNES DE SENSIBILISATION À LA SÉCURITÉ PAR AN	1	4
FRÉQUENCE DE DÉPLOIEMENT	Annuel	Trimestriel
SUJETS INCLUS	6	12
Appareils mobiles		✓
Courrier électronique		✓
Cycle de vie de l'information		✓
Fuite de données	✓	✓
Phishing	✓	✓
Ingénierie sociale		✓
Introduction à la sécurité de l'information	✓	✓
Malwares	✓	✓
Menace interne non intentionnelle		✓
Mots de passe	✓	✓
Signalement des incidents	✓	✓
Travail à distance		✓
OUTILS DE COMMUNICATION ET DE RENFORCEMENT Bulletins, affiches, fonds d'écran et plus !	6 sujets	12 sujets
SIMULATION DE PHISHING	1 simulation par trimestre	2 simulations par trimestre
FORMATION DE CONSOLIDATION PONCTUELLE POUR LES UTILISATEURS QUI ONT CLIQUÉ SUR UNE SIMULATION DE PHISHING **Microlearning Topics** • Compromission de courriers électroniques professionnels • Ransomware • Phishing ciblé (spear phishing) • Phishing sur le Web **Nanolearning Topics** • Usurpation d'identité - Exemple d'attaque • Phishing - Six indices qui devraient soulever des doutes • Ransomware • Harponnage - La fraude au président	2 sujets par trimestre	2 sujets par trimestre
COURS COMPLÉMENTAIRES FACULTATIFS **Basé sur le rôle - Sensibilisation à la sécurité de l'information pour :** • Administrateurs IT • Cadres • Développeurs IT • Finances • Managers • Ressources humaines **Cyber Game:** • Serious Game • Cyber Challenge	+ Ajout sur demande	+ Ajout sur demande

Plan pour les campagnes de niveau Champion

	T1	T2	T3	T4
Étape 1				
Déployer une simulation initiale de phishing de référence **Déployer un questionnaire de référence en guise de suivi**	Clic sur un lien et divulgation du mot de passe (12 questions prédéfinies)			
Étape 2	**Connaissance générale SSI (30 minutes)**			
Annoncer et déployer votre **campagne de formation annuelle**	• Introduction à la sécurité de l'information • Mots de passe • Phishing • Malwares • Fuite de données • Signalement des incidents			
Étape 3				
Distribuer des outils de **renforcement** (Bulletins, affiches, fonds d'écran et plus !)	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer
Étape 4	**Comportements:**			
Déployer une **simulation de phishing** basée sur des exemples réels, ciblant les comportements des utilisateurs	• Clic sur un lien • Divulgation des données relatives au mot de passe	• Clic sur un bouton • Ouverture d'une pièce jointe malveillante	• Clic sur un lien • Fourniture des données PII	• Clic sur un lien • Fourniture des données PFI
Étape 5				
Déployer une **formation ponctuelle** pour les utilisateurs qui ont cliqué sur une simulation de phishing • 1 Micro-learning (ML) • 1 Nano-learning (NL)	(ML) • Hameçonnage Web (NL) • Phishing - Six indices qui devraient soulever des doutes	(ML) • Ransomware (NL) • Ransomware	(ML) • Phishing ciblé (spear phishing) (NL) • Usurpation d'identité - Exemple d'attaque	(ML) • Compromission de courriers électroniques professionnels (NL) • Harponnage - La fraude au président

Plan pour les campagnes de niveau Étoile

	Campagne #1	Campagne #2	Campagne #3	Campagne #4
	T1	T2	T3	T4
Étape 1				
Déployer une simulation initiale de phishing de référence **Déployer un questionnaire de référence en guise de suivi**	Clic sur un lien et divulgation du mot de passe (12 questions prédéfinies)			
Étape 2	**Sujets:**			
Annoncer et déployer votre **campagne de formation trimestrielle**	• Introduction à la sécurité de l'information • Ingénierie sociale • Mots de passe	• Phishing • Malwares • Signalement des incidents	• Courrier électronique • Appareils mobiles • Travail à distance	• Cycle de vie de l'information • Menace interne non intentionnelle • Fuite de données
Étape 3				
Distribuer des outils de **renforcement** (Bulletins, affiches, fonds d'écran et plus !)	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer	S'aligner sur les sujets de l'étape 2 et les appuyer
Étape 4	**Comportements:**			
Déployer une **simulation de phishing** basée sur des exemples réels, ciblant les comportements des utilisateurs	• Clic sur un lien • Divulgation des données relatives au mot de passe	• Clic sur un bouton • Ouverture d'une pièce jointe malveillante	• Clic sur un lien • Fourniture des données PII	• Clic sur un lien • Fourniture des données PFI
Étape 5				
Déployer une **formation ponctuelle** pour les utilisateurs qui ont cliqué sur une simulation de phishing • 1 Micro-learning (ML) • 1 Nano-learning (NL)	(ML) • Hameçonnage Web (NL) • Phishing - Six indices qui devraient soulever des doutes	(ML) • Ransomware (NL) • Ransomware	(ML) • Phishing ciblé (spear phishing) (NL) • Usurpation d'identité - Exemple d'attaque	(ML) • Compromission de courriers électroniques professionnels (NL) • Harponnage - La fraude au président

Outils de communication et de renforcement

Renforcez la participation de vos collaborateurs avec une gamme d'outils de communication diversifiée et enrichie régulièrement

Affiches

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

Bulletins

Des mises à jour sur votre formation et le partage de bonnes pratiques en cybersécurité envoyées directement à vos utilisateurs.

Fonds d'écran et bannières web

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

Bandes dessinées

Ajoutez un aspect ludique à votre programme de formation grâce à de courtes bandes dessinées illustrant des situations reliées à la sécurité de l'information.

Infographies

Partagez des conseils et de bonnes pratiques en matière de cybersécurité dans un format attrayant et idéal pour les réseaux sociaux et les réseaux internes.

Cyberpedia

Informez-vous sur les principaux sujets liés à la cybersécurité grâce à des articles web informatifs et exhaustifs.

Videos "Qu'est-ce que…"

Prodiguez à vos utilisateurs des conseils et des bonnes pratiques en matière de cybersécurité sous forme de vidéos.

Tous les outils de communication sont actuellement disponibles en EN, FR-CA et FR-FR. Pour un support linguistique supplémentaire, contactez l'équipe du succès client de Terranova Security

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 en sensibilisation à la sécurité dans la langue de leur choix.

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

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 a été choisi par Microsoft pour aider les organisations à travers le monde à renforcer la protection de leurs données grâce à un contenu de grande qualité. Le matériel de formation ainsi que les simulations de phishing de Terranova Security s'appuie également sur des informations, fournies en temps réel par Microsoft, sur les plus récentes cybermenaces.

Distinctions de l’industrie

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
- Travail à distance
- Mots de passe robustes

ACCÈDER AU HUB

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