FORTRA'S
TERRANOVA
SECURITY

Catalogue de formations en sensibilisation à la sécurité de Terranova Security

Profitez de la meilleure expérience de formation en sensibilisation à la sécurité de l'industrie grâce à des cours qui enseignent tout ce que votre organisation doit savoir pour changer le comportement des utilisateurs et protéger vos informations sensibles des cybercriminels.

Cours de sensibilisation à la sécurité

Enrichissez votre programme de formation avec des contenus de sensibilisation à la sécurité ludiques et stimulants, qui soutiennent les responsables de la cybersécurité et leurs initiatives de changement des comportements. Profitez d'un contenu de formation multilingue, accessible et adapté aux mobiles, qui rend la formation de sensibilisation à la sécurité disponible à tous types d'utilisateurs tout en favorisant un climat inclusif.

Quiz

Testez les connaissances acquises par les participants lors de vos formations de sensibilisation à la sécurité, à l'aide de quiz proposés sous différents formats de questionnaires. Puisez dans la banque de questions préformulées ou créez vos propres questions afin que vos utilisateurs reçoivent le matériel d'évaluation et le feedback les plus pertinents possible.

Bibliothèque sur la sensibilisation à la sécurité

CONNAISSANCES GÉNÉRALES

Utilisateur 6 à 10 min

- Appareils mobiles
- BYOD (Bring Your Own Device)
- Classification de l'information
- Compromission de courriers électroniques professionnels
- Confidentialité sur le Web
- Contrôle de l'accès
- Courrier électronique
- Cycle de vie de l'information
- Fuite de données
- Hameçonnage
- Ingénierie sociale
- Introduction à la sécurité de l'information
- Le bon usage d'Internet
- Les smartphones
- Logiciels malveillants
- Menace interne non intentionnelle
- Mots de passe
- Principe du « bureau propre »
- Propriété intellectuelle
- Protection de votre ordinateur à la maison
- Protection des informations personnelles
- Protéger les données des cartes de paiement
- Rançongiciel
- Risques liés aux réseaux Wi-Fi ouverts
- Réseaux sociaux
- Sécurité physique
- Services Cloud
- Signalement des incidents
- Sites Web d'hameçonnage
- Télétravail
- Usurpation d'identité
- Voyager en toute sécurité

CYBER GAME

Serious Game 3 à 8 min

- Compromission de courriers électroniques professionnels
- Mot de passe robuste
- Ransomware
- Sécurisation du bureau à domicile
- ★ Services cloud

Cyber Challenge 3 min

- Phishing
- ★ Courrier électronique

★ **RÉCEMMENT AJOUTÉ**

BASÉ SUR LE RISQUE

Microapprentissage 3 à 4 min

- Ami ou ennemi?
- Le principe du « Clean desk »
- Clé USB à risque
- Compromission de courriers électroniques professionnels
- Comprendre les demandes d'autorisation d'applications
- Conseils de stratégie concernant les informations sensibles
- Contrôle d'accès
- Fraude au président
- Gérer des personnes non identifiées
- Phishing ciblé (spear phishing)
- Phishing
- Phishing téléphonique
- Phishing par SMS
- Phishing par messagerie vocale
- Phishing sur le Web
- Menace interne non intentionnelle
- Message d'information
- Partage d'un ordinateur de l'entreprise
- Partage non sécurisé d'informations sensibles
- Quiz Cybersécurité
- Ransomware
- Sécurisation de l'environnement de bureau à domicile
- Usurpation d'identité d'un haut dirigeant

Nanoapprentissage 2 à 3 min

- Anatomie d'une attaque de spear phishing
- Attaque
- Détection de cyberattaques
- Être conscient de la sécurité
- Phishing - Six indices qui devraient soulever des doutes
- Phishing par SMS
- Phishing par messagerie vocale
- Harponnage - La fraude au président
- Ingénierie sociale
- Ingénierie sociale par courrier électronique
- Menaces internes
- Partage dans le cloud
- Prévention des atteintes à la sécurité
- Protection de l'information sensible - Traitement de l'information
- Qu'est-ce que l'authentification à deux facteurs
- Ransomware
- Réseaux sociaux
- Risques liés aux cyberconférences
- Sécurité Wi-Fi
- Site Web de phishing
- Stegosploit
- Usurpation
- Usurpation d'identité - Exemple d'attaque

Nanovidéos 1 à 2 min

- Cyberfraude
- Exposition des données financières
- Malware
- Ransomware
- URL de site Web malveillant
- Violation des données des employés
- Vol d'identifiants
- Usurpation d'identité

BASÉ SUR LE RÔLE

Sensibilisation à la sécurité de l'information pour : 30 à 40 min

- Administrateurs IT
- Cadres
- Développeurs IT
- Finances
- Utilisateurs privilégiés TI
- Managers
- Ressources humaines

OWASP 15 à 45 min

- « Open Web Application Security Project » (OWASP)

CONFIDENTIALITÉ ET CONFORMITÉ 15 à 45 min

- « CCPA Essentials »
- Ce qu'il faut savoir du RGPD
- « HIPAA/HITECH »
- « Personally Identifiable Information » (PII)
- « Protected Health Information » (PHI)
- Protection des renseignements personnels
- RGPD pour les employés de l'approvisionnement
- Sensibilisation à la norme PCI DSS

CONNAISSANCES GÉNÉRALES

Utilisateur

Conçus pour renforcer l'élément humain de la sécurité de l'information de votre organisation, nos cours destinés aux utilisateurs aident les participants à comprendre les meilleures pratiques concernant une grande variété de sujets en cybersécurité. Chaque module comprend des activités d'apprentissage interactives qui consolident ces messages clés.

CODE	SUJET	DESCRIPTION	DURÉE 6 à 10 minutes
101	Introduction à la sécurité de l'information	• S'initier à la sécurité de l'information et à son importance générale • Comprendre les responsabilités des utilisateurs dans la protection des informations de l'organisation	
102	Classification de l'information	• Comprendre comment et pourquoi les organisations classifient leurs informations • S'exercer à classifier de l'information en fonction du niveau de confidentialité	
103	Cycle de vie de l'information	• Comprendre la valeur des informations appartenant à une organisation • Apprendre à gérer correctement l'information à travers son cycle de vie	
104	Propriété intellectuelle	• Savoir ce qu'est la propriété intellectuelle • Comprendre les comportements et les situations qui peuvent violer les droits de propriété intellectuelle	
105	Mots de passe	• Comprendre l'importance de créer des mots de passe efficaces • Apprendre comment créer des mots de passe solides et faciles à mémoriser	
106	Sécurité physique	• Comprendre pourquoi les organisations doivent sécuriser l'ensemble de leurs locaux et équipements • Apprendre comment protéger les aires de travail communes contre les menaces	
108	Contrôle de l'accès	• Apprendre pourquoi les organisations doivent contrôler l'accès à leurs réseaux et systèmes • Comprendre le processus impliqué pour l'octroi et la surveillance des accès	
201	Courrier électronique	• Reconnaître les menaces courantes liées aux emails et à leur utilisation abusive • Connaître les précautions à prendre avec les emails entrants et sortants	
203	Confidentialité sur le Web	• Comprendre les risques liés à la divulgation involontaire d'information sensible sur le Web • Comprendre et reconnaître les menaces en ligne	
205	Ingénierie sociale	• Comprendre le fonctionnement de l'ingénierie sociale *(social engineering)* et comment elle peut être à l'origine de diverses cybermenaces • Reconnaître les principales tactiques d'ingénierie sociale utilisées par les cybercriminels	
206	Principe du « bureau propre »	• Reconnaître l'importance d'éviter de laisser de l'information sensible sans surveillance dans un espace de travail • Découvrir comment assurer la sécurité de divers documents et appareils mobiles	
207	Protection des informations personnelles	• Connaître les obligations et les droits liés au respect de la vie privée • Identifier les informations qui sont considérées comme des renseignements personnels	
208	Protéger les données des cartes de paiement	• Comprendre les obligations des organisations concernant la protection des données des cartes de paiement • Connaître les menaces liées aux données des cartes de paiement	
210	Hameçonnage	• Connaître les tactiques d'hameçonnage *(phishing)* courantes et savoir comment elles menacent la sécurité de l'information • Reconnaître et identifier les caractéristiques d'un message et d'un site Web d'hameçonnage	

CODE	SUJET	DESCRIPTION	DURÉE 6 à 10 minutes
211	BYOD (Bring Your Own Device)	• Comprendre les enjeux de sécurité liés à l'utilisation d'appareils personnels à des fins professionnelles • Connaître les stratégies adoptées par les organisations pour réduire les risques liés à l'utilisation des appareils personnels	
301	Logiciels malveillants	• Connaître les différents types de logiciels malveillants *(malware)* • Comprendre les comportements humains et les facteurs techniques qui contribuent à prévenir les infections par un logiciel malveillant	
304	Le bon usage d'Internet	• Apprendre comment les organisations peuvent être affectées par une utilisation inappropriée d'Internet. • Comprendre quels comportements peuvent être potentiellement nuisibles sur les appareils ou les comptes de l'entreprise	
306	Usurpation d'identité	• Comprendre les conséquences du vol d'identité sur les victimes et les organisations • Connaître les principales méthodes utilisées pour commettre un vol d'identité	
307	Réseaux sociaux	• Comprendre les questions de confidentialité et de propriété de l'information liées à l'utilisation des réseaux sociaux • Connaître les menaces posées par les fraudeurs et les cybercriminels	
308	Télétravail	• Comprendre la réalité des utilisateurs mobiles et du travail à distance • Comprendre les risques liés à la mobilité des utilisateurs	
321	Appareils mobiles	• Comprendre les vulnérabilités associées aux appareils mobiles • Connaître les moyens de préserver la sécurité et l'intégrité des appareils mobiles	
322	Voyager en toute sécurité	• Savoir comment préserver la sécurité de l'information lors des déplacements et du travail à distance • Connaître les menaces pour l'information et la technologie utilisées par les employés en déplacement	
323	Protection de votre ordinateur à la maison	• Connaître les principales méthodes utilisées par les cybercriminels pour accéder à vos informations • Identifier les vulnérabilités propres au domicile et les activités risquées sur Internet	
324	Rançongiciel	• Connaître les rançongiciels *(ransomware)* et les conséquences négatives qu'ils peuvent avoir sur une organisation • Savoir comment les attaques par rançongiciels sont lancées	
325	Fuite de données	• Comprendre ce qui constitue une fuite de données et ses conséquences sur une organisation • Connaître les causes communes de fuites de données internes et externes	
326	Compromission de courriers électroniques professionnels	• Comprendre ce qu'est la fraude du président et comment cette attaque fonctionne • Connaître les principales stratégies d'hameçonnage utilisées dans ce type d'attaque	
327	Menace interne non intentionnelle	• Comprendre comment les utilisateurs peuvent involontairement mettre la sécurité de l'information en danger • Apprendre quels comportements et actions peuvent entraîner un incident de sécurité	
328	Signalement des incidents	• Comprendre l'importance de détecter et de gérer les incidents de sécurité rapidement • Apprendre à identifier et à signaler différents types d'incidents de sécurité	
329	Sites Web d'hameçonnage	• Comprendre les principales tactiques utilisées par les pirates pour construire des sites Web d'hameçonnage *(phishing)* • Apprendre comment protéger efficacement vos données des sites malveillants	
329	Risques liés aux réseaux Wi-Fi ouverts	• Comprendre les risques de se connecter à un réseau Wi-Fi non sécurisé • Apprendre les meilleures pratiques en matière de partage de l'information sur un réseau à l'extérieur du domicile ou du bureau	

CODE	SUJET	DESCRIPTION	DURÉE 6 à 10 minutes
331	Services Cloud	• Reconnaître les vulnérabilités potentielles liées au stockage, au partage et à l'accès de documents ou de systèmes basés sur le Cloud • Apprendre à utiliser le Cloud de façon sécuritaire grâce à des techniques de collaboration axées sur la cybersécurité	
506	Les smartphones	• Connaître les risques pour la sécurité de l'information liés à l'utilisation du *smartphone* • Apprendre les meilleures pratiques pour protéger l'information stockée sur les *smartphones*	

BASÉ SUR LE RISQUE

Microapprentissage

Destinés aux employés et conçus pour améliorer la rétention des connaissances et favoriser les changements de comportements durables, les modules de microapprentissage proposent du contenu de formation concis. Chaque module cible des risques précis et aide les organisations à atteindre leurs objectifs de productivité.

CODE	SUJET	DESCRIPTION	DURÉE 3 à 4 minutes
3001	Hameçonnage vocal	• Apprendre à identifier les attaques d'hameçonnage *(phishing)* vocal et à protéger les informations confidentielles	
3002	Hameçonnage Web	• Savoir comment vérifier l'identité d'une personne avant de lui donner des informations personnelles, et ce qui constitue une attaque d'hameçonnage *(phishing)* sur le Web	
3003	Hameçonnage de masse	• Comprendre comment identifier une arnaque réelle et protéger ses informations personnelles, par exemple dans le cas d'une fraude par cartes-cadeaux	
3004	Hameçonnage ciblé	• En se glissant dans la peau d'un pirate informatique, comprendre le mode d'opération des cybercriminels et les motifs derrière une attaque potentielle	
3005	Hameçonnage par texto	• Reconnaître les principaux éléments d'une attaque d'hameçonnage *(phishing)* par message texte et savoir comment protéger ses informations	
3006	Whaling	• Comprendre comment l'identité des cadres supérieures peut facilement être compromise par des attaques d'hameçonnage *(phishing)* ciblées, appelées chasse à la baleine	
3007	Usurpation d'identité d'un haut dirigeant par courriel	• Apprendre comment identifier l'usurpation d'identité d'un haut dirigeant par courriel, une attaque ciblée qui profite de l'autorité de l'expéditeur	
3008	Compromission de courriers électroniques professionnels	• Apprendre comment identifier les astuces utilisées par les cybercriminels pour compromettre une boîte mail professionnelle extorquer de l'argent	
3009	Gérer des personnes non identifiées	• Consolider les meilleures pratiques décrites dans le module Signalement des incidents en demandant à l'utilisateur de prendre les bonnes décisions s'il voit un inconnu se promener dans le bureau	
3010	Rançongiciel	• Apprendre comment réagir lors de la réception d'une pièce jointe inattendue et de l'infection d'un ordinateur par un logiciel malveillant *(malware)*	
3011	Menace interne non intentionnelle	• Connaître les bons gestes à poser lors de l'élimination de documents confidentiels en appliquant les meilleures pratiques en matière de sécurité de l'information	
3012	Ami ou ennemi?	• Comprendre quand et comment appliquer les meilleures pratiques en matière de sécurité de l'information lorsqu'un individu tente d'accéder à une zone d'accès réservé	
3013	Contrôle d'accès	• Découvrir les conséquences possibles de prêter son ordinateur à des collègues, ainsi que les meilleures pratiques en lien avec ce scénario	
3014	Le Principe du Bureau Propre	• Connaître les mesures à prendre pour réduire le risque de fuite d'informations sensibles sur un projet confidentiel en combinant les meilleures pratiques liées à différents aspects de la cybersécurité	

CODE	SUJET	DESCRIPTION	DURÉE 3 à 4 minutes
3015	Clé USB à risque	• Connaître les dangers liés au branchement d'un appareil USB inconnu sur un ordinateur, comme l'infection par un logiciel malveillant ou l'installation d'un programme dangereux	
3016	Hameçonnage par téléphone	• Apprendre comment protéger les informations sensibles contre les cybercriminels qui font des tentatives d'hameçonnage *(phishing)* par téléphone	
3017	Quiz Cybersécurité	• Permettre à vos utilisateur de se mesurer à Isa de Terranova Security, dans un jeu interactif qui permet de tester les connaissances générales sur la cybersécurité	
3021	Message d'information	• Comprendre l'importance de signaler un message suspect et les étapes appropriées à suivre dans un tel scénario	
3022	Comprendre les demandes d'autorisation d'applications	• Apprendre les bases des demandes de consentement liées aux applications et les meilleures pratiques à suivre pour s'assurer que les informations sont partagées de façon sécuritaire et uniquement avec les personnes concernées	
3023	Partage non sécurisé d'informations sensibles	• Découvrir les vulnérabilités inhérentes au partage de documents sensibles, et comment modifier, stocker, accéder et partager des informations confidentielles en toute sécurité	
3024	Partage d'un ordinateur de l'entreprise	• Découvrir les problématiques liées au partage d'un ordinateur d'entreprise avec une personne non autorisée et comment s'assurer que les politiques d'utilisation sont respectées à tout moment	
3025	Sécurisation de l'environnement de bureau à domicile	• Apprendre à sécuriser correctement un environnement de bureau à domicile en prenant des précautions concernant son ordinateur et autres appareils, le réseau Wi-Fi, etc.	
3026	Conseils de stratégie concernant les informations sensibles	• Apprendre comment votre organisation peut utiliser ses politiques internes pour délimiter l'information sensible et établir les mesures à prendre en cas de messages restraignant l'information	

BASÉ SUR LE RISQUE

Nanoapprentissage

Les modules de nanoapprentissage permettent aux utilisateurs de bien comprendre les principes fondamentaux spécifiques à la cybersécurité. Adapté à la formation juste-à-temps dans le cadre des simulations d'hameçonnage ou aux opportunités de courts apprentissages, chaque module guide les utilisateurs à travers les risques, les conséquences et les meilleures pratiques liés à un sujet donné.

CODE	SUJET	DESCRIPTION	DURÉE 2 à 3 minutes
2001	Rançongiciel	• Apprendre comment identifier des programmes malveillants (malware) et quoi faire si vous croyez avoir reçu un rançongiciel	
2002	Hameçonnage vocal	• Connaître les meilleures pratiques pour détecter l'hameçonnage (phishing) par téléphone et s'en protéger	
2003	Hameçonnage - Six indices qui devraient soulever des doutes	• Bien comprendre les six principaux indices à surveiller pour identifier une menace d'hameçonnage	
2006	Protection de l'information sensible - Traitement de l'information	• Apprendre à identifier, manipuler et protéger les informations sensibles en toute sécurité	
2007	Détection de cyberattaque	• Approfondir les notions portant sur la détection et la prévention des cyberattaques	
2008	Prévention des atteintes à la sécurité	• Comprendre comment réduire les risques d'atteintes à la sécurité de l'information	
2010	Sécurité Wi-Fi	• Connaître les risques liés à la sécurité du réseau Wi-Fi et les précautions à prendre	
2011	Usurpation d'identité - Exemple d'attaque	• Reconnaître les signes d'une tentative d'usurpation d'identité, et comment l'éviter	
2013	Ingénierie sociale	• Apprendre comment se défendre contre les attaques d'ingénierie sociale *(social engineering)*	
2015	Être conscient de la sécurité	• Savoir quoi faire au quotidien pour protéger votre domicile, vos possessions, vos appareils et vos informations sensibles	
2016	Harponnage - La fraude du PDG	• Connaître le fonctionnement de la fraude du président et comment détecter et éviter ce type de menaces	
2025	Site Web d'hameçonnage	• Apprendre comment identifier un site Web d'hameçonnage et ses principales caractéristiques	
2026	Réseaux sociaux	• Connaître les risques que représentent les cybercriminels sur les réseaux sociaux et comment protéger ses informations personnelles	
2035	Hameçonnage par SMS	• Savoir comment identifier l'hameçonnage (phishing) par texto et s'en protéger	

CODE	SUJET	DESCRIPTION	DURÉE 2 à 3 minutes
2050	Anatomie d'une attaque de harponnage	• Connaître les étapes et les mécanismes utilisés pour concevoir des attaques d'hameçonnage *(phishing)* personnalisées ou ciblées	
2051	Menaces internes	• Découvrir les différents types de menaces internes et les précautions à prendre	
2052	Ingénierie sociale par courrier électronique	• Connaître les étapes et les mécanismes utilisés dans les stratagèmes d'ingénierie sociale *(social engineering)* par courriel	
2053	Usurpation	• Comprendre comment les pirates informatiques peuvent usurper des sites Web populaires et les principaux signes à surveiller	
2054	Attaque d'hameçonnage à deux volets	• Savoir reconnaître les principales tactiques et les signaux d'alarme liés à l'hameçonnage à deux volets	
2055	Stegosploit	• Connaître le rôle clé des images numériques dans les attaques de type stegosploit	
2056	Risques liés aux cyberconférences	• Comprendre les risques et les principales tactiques de piratage associés aux conférences Web	
2057	Partage dans le cloud	• Connaître les vulnérabilités liées aux documents infonuagiques et au partage d'information	
2058	Qu'est-ce que l'authentification à deux facteurs		

BASÉ SUR LE RISQUE

Nanovidéos

Les modules de nanovidéos présentent les risques, les conséquences et les meilleures pratiques relativement à un sujet donné. Ils sont adaptés à la formation juste-à-temps dans le cadre de simulations d'hameçonnage ou comme courtes vidéos indépendantes d'apprentissage en ligne.

CODE	SUJET	DESCRIPTION	DURÉE 1 à 2 minutes
4	Rançongiciel	• Connaître les principaux signaux d'alarme d'une attaque de rançongiciel (ransomware), les conséquences du téléchargement d'un rançongiciel et les meilleures pratiques pour protéger les données contre ce type d'attaque	
5	URL de site Web malveillant	• Comprendre comment repérer et identifier l'URL d'un site Web malveillant en toute sécurité et connaître les techniques utilisées par les cybercriminels pour convaincre les utilisateurs de cliquer	
6	Vol d'identifiants	• Connaître les principaux signaux d'alarme d'une tentative de vol d'identifiant, savoir l'identifier et protéger les données sensibles	
7	Usurpation d'identité	• Savoir quels types de données sont ciblées lors des attaques visant le vol d'identité, comment un vol d'identité réussi affecte la victime et les meilleures pratiques pour aider les utilisateurs à protéger leurs données	
8	Exposition des données financières	• Apprendre comment les cyberattaques peuvent exposer des données financières et comment éviter une potentielle fuite des données lors du partage, du stockage et de l'accès aux informations connexes en appliquant les meilleures pratiques de cybersécurité	
9	Cyberfraude	• Connaître les principales tactiques utilisées par les cybercriminels pour commettre des cyberfraudes, les signaux d'alarme que les utilisateurs devraient surveiller et les meilleures pratiques	
10	Violation des données des employés	• Découvrir comment les employés peuvent être la cible d'une violation de données, les caractéristiques des messages utilisés par les pirates pour inciter les destinataires à divulguer des informations et les meilleures pratiques pour protéger les données	
11	Logiciels malveillants	• Comprendre comment les logiciels malveillants *(malware)* peuvent compromettre un ordinateur ou un appareil mobile, les conséquences d'une infection et comment protéger les données des maliciels	

BASÉ SUR LE RÔLE

Sensibilisation à la sécurité de l'information pour :

Chaque module basé sur le rôle est construit de façon à aborder les meilleures pratiques en sensibilisation à la sécurité spécifiques au contexte des différentes fonctions au sein d'une organisation. Terranova Security offre des cours adaptés aux rôles et responsabilités des professionnels œuvrant dans le domaine des finances et des ressources humaines, aux gestionnaires, et bien plus.

CODE	SUJET	DESCRIPTION	DURÉE 30 à 40 minutes
FIN	Finances	• Découvrir les types d'attaques auxquelles les professionnels du secteur des finances doivent régulièrement faire face, les conséquences d'une attaque réussie sur une organisation et comment se protéger contre les cybercriminels	
GEST	Gestionnaires	• Apprendre comment les gestionnaires peuvent être la cible de cybermenaces complexes et sophistiquées, les meilleures pratiques pour protéger les données et le rôle qui peut être joué par la direction pour favoriser une culture de sensibilisation à la cybersécurité	
HR	Ressources humaines	• Comprendre les règles et les règlements qui régissent le traitement des données des utilisateurs à des fins de RH, les types de tactiques utilisées par les pirates pour tenter de voler les données et comment protéger les informations	
TIA	Administrateurs TI	• Connaître les principales cybermenaces associées aux administrateurs des TI, et les meilleures pratiques pour protéger les informations sensibles, les réseaux et les systèmes	
TID	Développeurs TI	• Comprendre les bases d'un développement informatique sécurisé, comment les cybercriminels peuvent exploiter les différentes vulnérabilités et comment les développeurs peuvent détecter et éviter les attaques	
PRIT	IT Privileged Users		

BASÉ SUR LE RÔLE

OWASP

CODE	SUJET	DESCRIPTION	DURÉE 15 à 45 minutes
OWASP	« Open Web Application Security Project » (OWASP)	• Connaître les menaces de sécurité et les meilleures pratiques liées à l'OWASP et à ses processus	

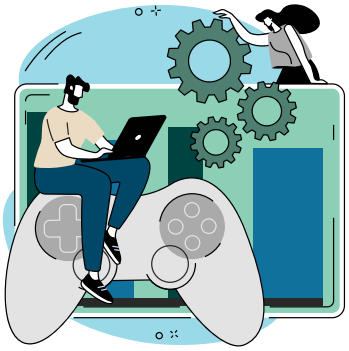
Confidentialité et conformité

Ces cours offrent du contenu de formation de qualité supérieure et des activités explorant les tendances clés en matière de protection des données. Ils permettent aux organisations de comprendre les différents règlements liés à la protection des données et de s'y conformer.

CODE	SUJET	DESCRIPTION	DURÉE 15 à 45 minutes
801	« Personally Identifiable Information » (PII)	• Apprenez tout ce qu'il faut savoir sur la PII	
803	« Protected Health Information » (PHI)	• Apprenez tout ce que vous devez savoir sur la PHI et comment les organisations peuvent s'y conformer	
814	RGPD pour les employés de l'approvisionnement	• Connaître les règles et les règlements du RGPD spécifiques aux employés du secteur de l'approvisionnement et leur rôle général en matière de conformité	
819	« CCPA Essentials »	• Connaître les essentiels du CCPA et les étapes qui doivent être suivies par les organisations pour s'y conformer	
820	Protection des renseignements personnels	• Découvrir les principaux enjeux en matière de protection des renseignements personnels et les impacts positifs d'une sensibilisation accrue	
821	Ce qu'il faut savoir du RGPD	• Connaître les essentiels du RGPD et comment les organisations peuvent s'y conformer	
HIPAA/ HITECH	« HIPAA/HITECH »	• Connaître les essentiels de l'HIPAA/HITECH et comment assurer la conformité	
PCI	Sensibilisation à la norme PCI DSS	• Connaître la norme PCI DSS et les impacts positifs d'une sensibilisation accrue	

Serious Game

Les modules de serious game placent les utilisateurs au centre d'un scénario immersif et excitant qui permet de tester leurs connaissances en cybersécurité dans un environnement ludique. Chaque module se concentre sur un sujet spécifique tandis que les joueurs accumulent des points et font la course contre la montre pour compléter les activités d'apprentissage interactives.



CODE	SUJET	DESCRIPTION	DURÉE 5 à 10 minutes
1	Mot de passe robuste	• Dans la peau d'un agent spécial, le joueur doit livrer une course contre la montre pour protéger des informations sensibles en s'appuyant sur sa solide expertise en matière de mots de passe	
2	Sécurisation du bureau à domicile	• Dans la peau d'un agent spécial, le joueur doit livrer une course contre la montre pour sécuriser un bureau à domicile et empêcher que des données confidentielles ne tombent entre les mains de hackers	
3	Ransomware	• Incarnez un enquêteur stagiaire en cybersécurité dans une course contre la montre pour identifier la source d'une attaque par ransomware avant que le système entier d'une organisation ne soit compromis	
4	Compromission de courriers électroniques professionnels	• Jouez le rôle d'un enquêteur en cybersécurité et examinez différents e-mails afin d'identifier les paiements valides faits aux fournisseurs et d'arrêter tout paiement potentiellement frauduleux en raison d'une compromission de messagerie professionnelle	
5	Services cloud		

Cyber challenge

Les cyber challenges sont des activités d'apprentissage ludiques et attrayantes qui permettent de tester et de renforcer les connaissances fondamentales en matière de sécurité sur des sujets tels que le phishing, la sécurité des e-mails, etc.

CODE	SUJET	DESCRIPTION	DURÉE 3 minutes
1	Phishing	• Reconnaître et identifier les caractéristiques d'un message et d'un site Web de phishing	
2	Email (titre a venir)		

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, FR-FR et ES LATAM. Pour un support linguistique supplémentaire, contactez l'équipe du succès client de Terranova Security

PARTENAIRE MONDIAL DE CHOIX EN SENSIBILISATION À LA CYBERSÉCURITÉ

DEMANDER UNE SOUMISSION