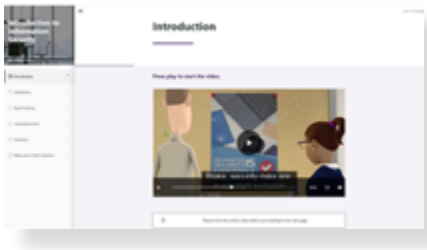
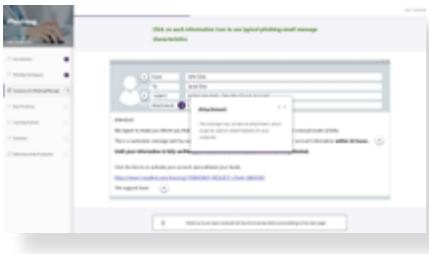
FORTRA

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.





Les cours de sensibilisation à la sécurité

Améliorez votre programme de formation par un contenu de sensibilisation à la sécurité amusant et attrayant, qui soutient les responsables de la cybersécurité et leurs initiatives de changement de comportement. Profitez d'un contenu de formation multilingue, mobile et accessible, qui rend la formation à la sensibilisation à la sécurité disponible pour tous les types d'utilisateurs tout en favorisant un climat inclusif.

Les quiz

Testez le taux d'information retenue par l'utilisateur qui suit vos cours de sensibilisation à la sécurité, à l'aide de quiz utilisant différents formats de questions. Vous pourrez choisir parmi les questions déjà prêtes proposées dans une banque, ou encore créer vos propres questions pour que votre matériel de test soit le plus pertinent possible et fournisse la rétroaction la plus fidèle possible à vos utilisateurs.

Bibliothèque sur la sensibilisation à la sécurité

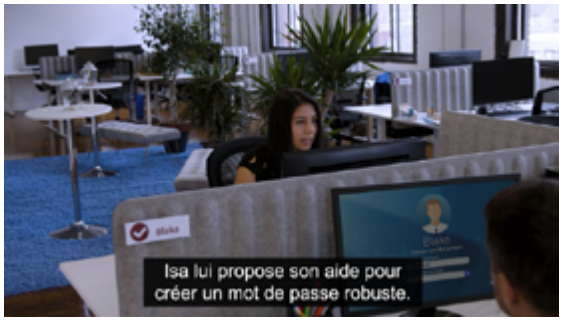
CONNAISSANCES GÉNÉRALES

Utilisateur 6 à 10 min

- Appareils mobiles
- Classification de l'information
- Compromission de courriels professionnels
- Confidentialité sur le Web
- Contrôle de l'accès
- Courriel
- Cycle de vie de l'information
- Fuite de données
- Hameçonnage
- Introduction à la sécurité de l'information
- Le bon usage d'Internet
- Logiciels malveillants
- Menace interne non intentionnelle
- Mots de passe
- Piratage psychologique
- « Prenez vos appareils personnels (PAP) »
- Principe du « bureau propre »
- Propriété intellectuelle
- Protection de votre ordinateur à la maison
- Protection des renseignements personnels
- Protéger les données des cartes de paiement
- Rançongiciel
- Réseaux sociaux
- Risques de réseaux Wi-Fi ouverts
- Sécurité physique
- Services d'infonuagique
- Signalement des incidents
- Sites Web d'hameçonnage
- Téléphones intelligents
- Travailler à distance
- Vol d'identité
- Voyager en toute sécurité

Personnages animés en 3D

Personnages en action réelle



CYBERJEU

Jeu sérieux 3 à 8 min

- Compromission de courriels professionnels
- Mot de passe robuste
- Piratage psychologique
- Rançongiciel
- Réseaux sociaux
- Sécuriser un bureau à domicile
- Services d'infonuagique
- Transfert de données
- ★ Travailler à distance
- ★ Voyager en toute sécurité

Cyberdéfi 3 min

- Appareils mobiles
- Classification de l'information
- Courriel
- Cycle de vie de l'information
- Hameçonnage
- Logiciel malveillant
- Piratage psychologique
- Protéger votre bureau à domicile
- Protection des renseignements personnels
- Rançongiciel
- Services d'infonuagique
- Identification des incidents pour le signalement
- Voyager en toute sécurité

★ **AJOUTÉ RÉCEMMENT**

BASÉ SUR LE RISQUE

Microapprentissage 3 à 4 min

- Ami ou ennemi?
- Application du principe du bureau bien rangé
- Chasse à la baleine
- Clé USB à risque
- Comprendre les demandes de consentement d'une application
- ★ Codes QR imprimés malveillants
- ★ Codes QR numériques malveillants
- ★ Compromission d'un compte d'application
- ★ Compromission d'un compte de messagerie
- ★ Compromission d'un navigateur
- ★ Compromission d'un ordinateur
- Conseils en matière de politique concernant les informations sensibles
- Contrôle d'accès
- Escroquerie par courriel d'affaires
- Hameçonnage ciblé
- Hameçonnage de marché de masse
- Hameçonnage par téléphone
- Hameçonnage par texto
- Hameçonnage via Teams
- Hameçonnage vocal
- Hameçonnage Web
- Jeu-questionnaire sur la cybersécurité
- Menaces internes involontaires
- Message d'information
- Méthode d'authentification
- Octroi de consentement à OAuth
- Partage non sécurisé d'information sensible
- Rançongiciel
- Sécuriser l'environnement de bureau à domicile
- Traiter avec des personnes non identifiées
- Usurpation d'identité d'un haut dirigeant par courriel
- Utilisation commune de l'ordinateur d'une organisation

Nanoapprentissage 2 à 3 min

- Anatomie d'une attaque de harponnage
- Détection de cyberattaque
- Être conscient de la sécurité
- Hameçonnage - Six indices qui devraient soulever des doutes
- Hammeçonnage à deux volets (Double Barrel)
- Hameçonnage par texto
- Hameçonnage vocal
- Harponnage - La fraude du PDG
- Ingénierie sociale
- Menaces internes
- Mystification
- Partage basé sur le nuage
- Piratage psychologique par courriel
- Prévention des atteintes à la sécurité
- Protection de l'information sensible - Traitement de l'information
- Qu'est-ce que l'authentification à deux facteurs?
- Rançongiciel
- Réseaux sociaux
- Risques des conférences Web
- Sécurité Wi-Fi
- Site Web d'hameçonnage
- Stegosploit
- Usurpation d'identité - Exemple d'attaque

Nanovidéos 1 à 2 min

- ★ Attaque de navigateur dans le navigateur
- Cyberfraude (fraude sur Internet)
- Exposition des données financières
- ★ IA générative : de quoi s'agit-il?
- Importance de la culture de sécurité dans l'organisation
- Logiciels malveillants
- Rançongiciel
- URL vers un site Web malveillant
- Violation des données des employés
- Vol d'identifiants
- Vol d'identité

★ **AJOUTÉ RÉCEMMENT**

BASÉ SUR LE RÔLE

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

- **Administrateurs TI**
  - Aperçu de la sécurité réseau
  - Attaques de réseau courantes
  - Sécurisation des réseaux
  - Sécurisation des référentiels de données
- **Cadres**
  - Introduction à la sécurité de l'information
  - Mots de passe
  - Hameçonnage
  - Confidentialité sur le Web
  - Appareils mobiles
  - Fuite de données
  - Compromission de courriels professionnels
- **Développeurs TI**
  - Aperçu de la sécurité applicative
  - Attaques applicatives courantes
  - Développement sécurisé
  - Aperçu de la cryptographie
  - Contrôle de l'accès
  - Cycle de vie de l'information
- **Finances**
  - Introduction à la sécurité de l'information
  - Mots de passe
  - Confidentialité sur le Web
  - Protéger les données des cartes de paiement
  - Hameçonnage
  - Fuite de données
- **Gestionnaires**
  - Les défis de la sécurité
  - Gouvernance de la sécurité
  - Montrer l'exemple
- **Ressources humaines**
  - Introduction à la sécurité de l'information
  - Mots de passe
  - Confidentialité sur le Web
  - Protection des renseignements personnels
  - Hameçonnage
  - Fuite de données
- **Service d'assistance**
  - Introduction à la sécurité de l'information
  - Mots de passe
  - Contrôle de l'accès
  - Piratage psychologique
  - Hameçonnage
  - Signalement des incidents
- **Utilisateurs privilégiés TI**
  - Introduction à la sécurité de l'information
  - Mots de passe
  - Contrôle de l'accès
  - Hameçonnage
  - Logiciels malveillants
  - Travailler à distance
  - Rançongiciel
  - Menace interne non intentionnelle
  - Signalement des incidents

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 »**
- **Intégration de la sécurité dès la conception**
- **La loi POPI**
- **La protection des renseignements personnels dans le secteur privé au Québec**
  - Les éléments clés de la réforme
  - Les obligations des entreprises
  - La protection par défaut des renseignements personnels
  - Les droits des individus et la protection de leurs renseignements personnels
- **« Personally Identifiable Information » (PII)**
- **Principes de base du respect de la confidentialité**
  - La protection des données personnelles
  - Collecte de données personnelles
  - Les principes en matière de protection de la vie privée
  - Atteintes à la vie privée
- **« Protected Health Information » (PHI)**
- ★ **La Loi sur la protection des renseignements personnels et les documents électroniques**
- **La sécurité des données de santé en Europe**
- **Sensibilisation à la norme PCI DSS**

★ **AJOUTÉ RÉCEMMENT**

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	Courriel	• Reconnaître les menaces courantes liées aux courriels et à leur utilisation abusive • Connaître les précautions à prendre avec les courriels 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	Piratage psychologique	• Comprendre le fonctionnement de l'ingénierie sociale 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 renseignements personnels	• 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	

CODE	SUJET	DESCRIPTION	DURÉE 6 à 10 minutes
210	Hameçonnage	• Connaître les tactiques d'hameçonnage 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	
211	« Prenez vos appareils personnels (PAP) »	• 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 • 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 de l'Internet. • Comprendre quels comportements peuvent être potentiellement nuisibles sur les appareils ou les comptes de l'entreprise	
306	Vol 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	Travailler à distance	• 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 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 courriels 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	

CODE	SUJET	DESCRIPTION	DURÉE 6 à 10 minutes
329	Sites Web d'hameçonnage	• Comprendre les principales tactiques utilisées par les pirates pour construire des sites Web d'hameçonnage • Apprendre comment protéger efficacement vos données des sites malveillants	
330	Risques de 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	
331	Services d'infonuagique	• Reconnaître les vulnérabilités potentielles liées au stockage, au partage et à l'accès de documents ou de systèmes basés sur l'infonuagique • Apprendre à utiliser les services infonuagiques de façon sécuritaire grâce à des techniques de collaboration axées sur la cybersécurité	
506	Téléphones intelligents	• Connaître les risques pour la sécurité de l'information liés à l'utilisation du téléphone intelligent • Apprendre les meilleures pratiques pour protéger l'information stockée sur les téléphones intelligents	

CYBERJEU

Jeu sérieux

Les modules de jeux sérieux 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 3 à 8 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 pirates informatiques	
3	Rançongiciel	• Incarnez un enquêteur stagiaire en cybersécurité dans une course contre la montre pour identifier la source d'une attaque par rançongiciel avant que le système entier d'une organisation ne soit compromis	
4	Compromission de courriels professionnels	• Jouez le rôle d'un enquêteur en cybersécurité et examinez différents courriels afin d'identifier les paiements valides faits aux fournisseurs et d'arrêter tout paiement potentiellement frauduleux en raison d'une compromission des courriels d'affaires	
5	Services d'infonuagique	• Jouez le rôle d'un analyste légendaire en cybersécurité chargé d'identifier la source des fuites de données et d'y mettre un terme, avant que d'autres dommages ne puissent être causés	
6	Transfert de données	• Incarnez une employée du département des activités commerciales et organisez soigneusement vos fichiers et courriels pour une fin de semaine sans stress, sans risquer d'être interrompue en raison d'une fuite de données majeure	
7	Piratage psychologique	• Assumez deux rôles différents en vous joignant d'abord à l'équipe Rouge pour concevoir un scénario de cyberattaque fictif et en passant ensuite à l'équipe Bleue pour choisir les défenses appropriées contre divers types de cyber menaces	
8	Réseaux sociaux	• Incarnez un nouveau gestionnaire des médias sociaux et complétez votre formation en vous tenant au fait de l'actualité dans votre domaine et en rencontrant des gestionnaires clés	
9	Voyager en toute sécurité	• Incarnez un universitaire de renommée mondiale et appliquez les meilleures pratiques en matière de sécurité de l'information en vous rendant à une conférence top-secrète sur le campus des Services Secrets	
10	Travailler à distance	• Incarnez un étudiant et assistant de recherche qui doit préserver la confidentialité de ses données tout en travaillant dans l'autobus et au café en vue de respecter un délai serré	

CYBERJEU

Cyberdéfi

Les cyber défis sont des activités d'apprentissage attrayantes et ludiques qui permettent de tester et de renforcer les connaissances fondamentales en matière de sécurité sur des sujets tels que l'hameçonnage, la sécurité des courriels, etc.

CODE	SUJET	DESCRIPTION	DURÉE 3 minutes
102	Classification de l'information	• Classer l'information en fonction de son niveau de sensibilité afin d'appliquer les mesures de sécurité appropriées	
103	Cycle de vie de l'information	• Planifier l'élimination adéquate de l'information en fonction de son format et degré de sensibilité	
201	Courriel	• Reconnaître et identifier toutes les façons dont les fraudeurs peuvent infiltrer votre réseau et protéger vos données	
205	Piratage psychologique	• Comprendre et se protéger des cyberattaques ayant pour origine des interactions sociales trompeuses	
207	Protection des renseignements personnels	• Identifier les informations personnelles gérées par votre organisation afin de les traiter en conformité avec les exigences en matière de sécurité et de confidentialité	
210	Hammeçonnage	• Reconnaître et identifier les caractéristiques d'un message et d'un site Web d'hameçonnage	
301	Logiciels malveillants	• Examiner et identifier les moyens dont les logiciels malveillants peuvent s'infiltrer dans vos appareils électroniques	
321	Appareils mobiles	• Adopter les meilleures pratiques lors de l'utilisation d'appareils mobiles afin de protéger les informations votre entreprise et vos informations personnelles	
322	Voyager en toute sécurité	• Reconnaître et évaluer les risques liés à la sécurité de l'information lors des déplacements	
323	Protéger votre bureau à domicile	• Identifiez et éliminez les failles de sécurité dans votre bureau à domicile pour travailler à distance en toute sécurité	
324	Rançongiciel	• Comprendre les risques liés aux rançongiciels, et appliquer les meilleures pratiques afin d'assurer la sécurité des données de votre organisation	
328	Identification des incidents pour le signalement	• Identifiez et signalez les incidents de sécurité sans délai afin de contribuer à la protection de votre organisation	
331	Services d'infonuagique	• Évaluer le niveau de risque associé aux divers usages de services d'infonuagique afin d'assurer la sécurité de vos informations et de celles de votre organisation	

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 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 sur le Web	
3003	Hameçonnage de marché 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 par message texte et savoir comment protéger ses informations	
3006	Chasse à la baleine	• Comprendre comment l'identité des cadres supérieures peut facilement être compromise par des attaques d'hameçonnage 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	Escroquerie par courriel d'affaires	• Apprendre comment identifier les astuces utilisées par les cybercriminels pour compromettre un compte de courriel professionnel et extorquer de l'argent	
3009	Traiter avec 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	
3011	Menaces internes involontaires	• Reconnaître 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	Application du principe du bureau bien rangé	• 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 par téléphone	
3017	Jeu-questionnaire sur la 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 de consentement d'une application	• 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'information sensible	• Découvrir les vulnérabilités inhérentes au partage de documents sensibles, et comment modifier, stocker, accéder et partager des informations confidentielles en toute sécurité	
3024	Utilisation commune de l'ordinateur d'une organisation	• 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	Sécuriser 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 en matière de politique 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	
3027	Hameçonnage via Teams	• Découvrez comment les attaques de phishing peuvent être diffusées via Microsoft Teams, ainsi que les mesures à prendre pour identifier les clavardages suspects	
3028	Octroi de consentement à OAuth	• Apprendre à se protéger ainsi que son organisation de tentatives de hameçonnages liées à l'OAuth, ou l'autorisation de tiers, en installant seulement des applications provenant de sources fiables ainsi qu'en créant un identifiant et mot de passe unique pour chaque service	
3029	Méthode d'authentification	• Connaître les risques liés à l'utilisation d'une tierce partie pour se connecter à un service en ligne, et identifier la méthode la plus sûre pour s'authentifier dans un contexte donné	
3030	Compromission d'un compte de messagerie	• Apprendre à détecter les signes de compromission d'une boîte courriel organisationelle, et tirer parti des meilleures pratiques afin de prévenir les intrusions, notamment l'activation de l'authentification à deux facteurs	
3031	Compromission d'un compte d'application	• Identifier les signes indiquant que l'un de vos comptes en ligne a été compromis, notamment recevoir des notifications de tentatives de connexion infructueuses et remarquer des modifications apportées à votre insu à vos informations personnelles	
3032	Compromission d'un navigateur	• Apprendre à détecter les signes que votre navigateur Web a été compromis et est employé à des fins malveillantes, notamment la découverte de barres d'outils ou d'extensions de navigateur que vous n'avez pas installées	

CODE	SUJET	DESCRIPTION	DURÉE 3 à 4 minutes
3033	Compromission d'un ordinateur	• Découvrir les signes courants que votre ordinateur a été infecté par un virus, par exemple l'apparition de publicités intempestives et le ralentissement de votre appareil	
3034	Codes QR numériques malveillants	• Identifier les signes indiquant qu'un code QR digital est frauduleux et appliquer les meilleures pratiques pour réduire les risques associés à la lecture d'un code QR malveillant en ligne	
3035	Codes QR imprimés malveillants	• Identifier les signes indiquant qu'un code QR imprimé est frauduleux et appliquer les meilleures pratiques pour réduire les risques associés à la lecture d'un code QR malveillant affiché dans un lieu public	

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 et quoi faire si vous croyez avoir reçu un rançongiciel	
2002	Hameçonnage vocal	• Connaître les meilleures pratiques pour détecter l'hameçonnage 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	
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	

CODE	SUJET	DESCRIPTION	DURÉE 2 à 3 minutes
2035	Hameçonnage par texto	• Savoir comment identifier l'hameçonnage par texto et s'en protéger	
2050	Anatomie d'une attaque de harponnage	• Apprendre comment protéger les informations sensibles contre les cybercriminels qui font des tentatives d'hameçonnage par téléphone	
2051	Menaces internes	• Découvrir les différents types de menaces internes et les précautions à prendre	
2052	Piratage psychologique par courriel	• Connaître les étapes et les mécanismes utilisés dans les stratagèmes d'ingénierie sociale par courriel	
2053	Mystification	• Comprendre comment les pirates informatiques peuvent usurper des sites Web populaires et les principaux signes à surveiller	
2054	Hammeçonnage à deux volets (Double Barrel)	• 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 des conférences Web	• Comprendre les risques et les principales tactiques de piratage associés aux conférences Web	
2057	Partage basé sur le nuage	• Connaître les vulnérabilités liées aux documents infonuagiques et au partage d'information	
2058	Qu'est-ce que l'authentification à deux facteurs?	• Comprendre l'utilisation, le format et le signalement et les bonnes pratiques associé au 2FA	

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, les conséquences du téléchargement d'un rançongiciel et les meilleures pratiques pour protéger les données contre ce type d'attaque	
5	URL vers un 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	Vol 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 (fraude sur Internet)	• 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 peuvent compromettre un ordinateur ou un appareil mobile, les conséquences d'une infection et comment protéger les données des maliciels	
12	Importance de la culture de sécurité dans l'organisation	• Comprendre l'importance d'avoir une forte culture de la sécurité de l'information pour une organisation et la manière dont on peut contribuer à promouvoir cette culture au sein de son organisation	
13	Attaque de navigateur dans le navigateur	• Reconnaissez les signes courants d'attaques de type navigateur dans le navigateur (ou "browser-in-the-browser") et découvrez cinq façons de vous protéger ainsi que votre organisation	
14	IA générative : de quoi s'agit-il?	• Comprendre ce qu'est l'IA générative, connaître les risques liés à son emploi, et suivre les meilleures pratiques pour assurer votre sécurité et celle de votre organisation	

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	
EXEC	Cadres	• Fournir aux dirigeants et aux cadres les informations nécessaires pour comprendre, évaluer et se défendre contre les cybermenaces les plus courantes qui les visent	
PRIT	Utilisateurs privilégiés TI	• Fournir aux utilisateurs TI privilégiés de meilleures pratiques et outils afin d'identifier, évaluer et se protéger des cybermenaces	
HD	Service d'assistance	• Fournir aux utilisateurs offrant du soutien TI dans un Centre de Service de meilleures pratiques et outils afin d'identifier, évaluer et se protéger des cybermenaces	

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	
818	Ce qu'il faut savoir du RGPD	• Connaître les essentiels du RGPD et comment les organisations peuvent s'y conformer	
819	« CCPA Essentials »	• Connaître les essentiels du CCPA et les étapes qui doivent être suivies par les organisations pour s'y conformer	
820 à 823	Principes de base du respect de la confidentialité	• Découvrir les principaux enjeux en matière de protection des renseignements personnels et les impacts positifs d'une sensibilisation accrue	
830 à 833	La protection des renseignements personnels dans le secteur privé au Québec	• Couvrir les exigences législatives en matière de traitement des données personnelles dans le secteur privé, au Québec, à la suite de l'adoption récente de la loi 25	
840	La sécurité des données de santé en Europe	• Connaître les principes essentiels de l'application du RGPD aux données de santé ainsi que les mesures à prendre par les professionnels de la santé	
846 à 848	La Loi sur la protection des renseignements personnels et les documents électroniques	• Comprendre les principes clés de la loi canadienne sur la protection des renseignements personnels et les documents électroniques, et apprendre comment contribuer à assurer la conformité de votre organisation	
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	
POPIA	La loi POPI	• Connaître la loi POPI (Protection of Personal Information Act) sur la protection des renseignements personnels pour assurer la conformité aux huit principes énoncés dans celle-ci et protéger la confidentialité de vos clients sud-africains	
SBD	Intégration de la sécurité dès la conception (SBD)	• Ce cours vise à familiariser les usagers avec les meilleures pratiques en matière de sécurité, et ce, à chacune des étapes du cycle de développement d'un projet ou d'un service informatique	

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.

Infolettres

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.

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 des 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