LUTTER CONTRE LA CYBERCRIMINALITÉ

S'approprier les bonnes pratiques de la Cybersécurité

1 JOUR, 7 HEURES

NUMÉRIQUE ET SMART CITY

CODE : GNU23

Objectifs de la formation

S'approprier les principaux concepts liés à la cyber sécurité

Identifier les cyber-menaces

Adopter les bons reflexes pour prévenir une cyberattaque

Intégrer les bonnes pratiques pour sécuriser son utilisation des outils informatiques

Parmi nos formateurs

- **PINTE Jean Paul**
  Conférencier international en cybercriminalité ,

Public concernés

- Elus ; Collaborateur en charge du numérique ; Directeur informatique ; Directeur juridique ; Directeur des Ressources Humaines

Critères d'admission

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Prérequis

- Aucun prérequis n'est nécessaire

Tarifs

- Promo d'été -10% : Communes <20.000 hab. - Sessions en virtuel : 625,50 €HT
- Promo d'été -10% : Communes >20.000 hab. - Sessions en virtuel : 805,50 €HT
- Communes < 20 000 habitants (ou élus) : Tarif Classe virtuelle : 695,00 €HT
- Communes > 20 000 habitants (ou autres établissements) : Tarif Classe virtuelle : 895,00 €HT

La cybercriminalité touche de plus en plus notre quotidien. Les modes opératoires évoluent dans le temps avec les technologies du Web et les applications mobiles. Attaques aux ransomwares, cyberattaques, « défacement de site Web », Fraudes, vols de données sont autant d'exemples auxquels les collectivités doivent se préparer aujourd'hui.

Cette formation présente des outils pour repérer les formes d'attaques pratiquées par les cyber-délinquants et propose des solutions pour faire face à ce fléau et ainsi de préserver son patrimoine

informationnel.

Présentation du cyberespace

- Le passage du Web 1.0 au Web 5.0
- Distinguer les niveaux de profondeurs d'Internet
- Du Web surfacique au Dark Web
- Focus sur l'ingénierie sociale : le mode opératoire des cybers délinquants

JEU PÉDAGOGIQUE Quiz interactif : à travers un outil interactif les stagiaires définissent la notion du cyberspace

S'approprier les enjeux de la Cybersécurité

- La Cybersécurité, c'est quoi
- Distinguer les notions de menaces et de risque
- Quelles sont les obligations des collectivités et des élus : le risque pénal
- Gérer son e-réputation : comment protéger son identité numérique

ATELIER Réflexion collective sur les enjeux de l'e-réputation des politiques et des élus, afin de faire émerger les meilleures pratiques pour préserver son e-réputation

Quels sont les typologies de cyberattaques

- Qu'est-ce qu'une attaque par déni de service
- Identifier les types de logiciels malveillants
- Que faire en cas d'hameçonnage ou Phishing
- Améliorer ses défenses en matière de téléchargement furtif
- Le cassage de mots de passe : comment bien gérer ses mots de passe
- Se prémunir contre les Faux Ordres de virements (FOVI)
- Le piratage de compte, que faire pour protéger ses comptes

Etude de cas

- Un cas réel est exposé par le formateur, les stagiaires sont amenés à analyser et identifier le type du cyber attaque appliqué par les cybers délinquants

Comment se prémunir de ces menaces

- Vérifier la mise à jour de son système
- Cerner les nouvelles recommandations sur la gestion des mots de passe
- Assurer la séparation des usages et des droits d'accès
- La surveillance des périphériques de travail
- Les recommandations sur le nomadisme numérique
- Naviguer sur internet en sécurité: distinguer les vrais et les faux sites
- Se protéger au quotidien : les bonnes pratiques à adopter
- Comment prévenir les menaces grâce à l'intelligence artificielle
- Focus sur la sensibilisation insuffisante du personnel des collectivités

Etude de cas

- En se basant sur une étude présentée par le formateur, les stagiaires sont amenés à analyser des incidents de sécurité informatique dans la collectivité et de repérer les failles

En cas de cyber attaque, comment bien agir

- Cerner le cadre juridique de la sécurité des systèmes d'informations
- Définir les acteurs et les responsabilités de la Cybersécurité
- Déclarer une cyberattaque : les délais et les contacts utiles
- L'assurance cyber sécurité, c'est quoi
- Identifier le rôle des DPO (Data Protector Officer) dans la cybersécurité
- Appréhender le dispositif de l'état : le plan de relance de l'ANSSI
- Quelles sont les aides financières à disposition des collectivités

ATELIER Les stagiaires regroupés en sous-groupes, sont amenés à établir un guide de bonnes pratiques pour une utilisation sécurisée d'internet

Débriefing en plénière / Evaluation des acquis

Dates

Classe virtuelle

29/08/2025

20/11/2025

Modalités pédagogiques, d'évaluation et techniques

- **Modalités pédagogiques:**

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

- **Modalités d'évaluation:**

Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation. Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

- **Modalités techniques FOAD:**

Les parcours sont accessibles depuis un simple lien web, envoyé par Email aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra

contacter la hotline au 01 70 72 25 81, entre 9h et 17h ou par mail au logistiqueformations@infopro-digital.com et la prise en compte de la demande se fera dans les 48h.