Sensibilisation aux Cyberattaques - prévenir, détecter, réagir

Lien :
https://innov-systems.com/formation/sensibilisation-aux-cyberattaques-prevenir-detecter-reagir

DURÉE
2 jours (14h)

RÉFÉRENCE
SEC330

CATÉGORIE
Fondamentaux
Sécurité Informatique

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les risques liés aux cyberattaques
- Identifier les différentes formes de menaces (phishing, ransomware, fraude au président…)
- Connaître les impacts potentiels sur les individus, les services et les organisations
- Prendre conscience de l'importance de la cybersécurité dans son activité quotidienne
- Adopter les bons réflexes pour se protéger
- Appliquer les bonnes pratiques en matière de gestion des mots de passe, navigation web, messagerie, et utilisation des équipements
- Réagir correctement face à une tentative d'attaque (phishing, pièce jointe suspecte, intrusion réseau…)
- Connaître les règles internes à respecter (charte informatique, signalement d'incidents…)
- Contribuer à la culture cybersécurité de l'organisation
- Intégrer la cybersécurité dans ses pratiques professionnelles quotidiennes
- Savoir relayer les bonnes pratiques auprès de ses collègues ou équipes
- Participer activement à la mise en place ou au respect de la politique de sécurité de l'information (PSI)

POUR QUI ?

- Employés de tous niveaux utilisant un ordinateur, un smartphone ou une connexion Internet dans leur travail quotidien
- Salariés d’entreprise
- Managers et responsables de service
- Responsables d’équipes devant s’assurer que les bonnes pratiques numériques sont respectées
- Chefs de projet
- Responsables RH
- Comptables
- Responsables logistiques utilisant des données sensibles
- Personnes exposées aux risques de fraude ciblée (type "fraude au président")
- Utilisateurs ayant accès à des données stratégiques : DSI, RSSI, DAF, DRH…
- Membres de la direction (CODIR)
- Personnel en télétravail ou en mobilité, plus exposé aux cyber-risques

Programme détaillé

1 / Introduction à la cybersécurité

- Enjeux et menaces actuelles
- Typologie des cyberattaques (phishing, ransomware, DDoS, etc)
- Impacts économiques, humains et réputationnels

2 / Les principales failles humaines

- L’erreur humaine : facteur n°1 d’intrusion
- Comportements à risque : clics, mots de passe faibles, négligence
- Études de cas réels et conséquences

3 / Phishing et ingénierie sociale

- Reconnaître un e-mail de phishing ou un faux SMS
- Techniques d’ingénierie sociale utilisées par les attaquants
- Exercices pratiques : démasquer les tentatives d’hameçonnage

4 / Protection des accès et des identifiants

- Bonnes pratiques de création et gestion de mots de passe
- Authentification forte (2FA, biométrie, etc)
- Gestion sécurisée des accès aux outils numériques

5 / Utilisation sécurisée des équipements et du réseau

- Sécuriser son poste de travail, son mobile et ses connexions
- Risques liés au Wi-Fi public et aux clés USB
- Importance des mises à jour et antivirus

6 / Comportements à adopter en cas de cyberattaque

- Réflexes immédiats à avoir (déconnecter, alerter, préserver les preuves)
- Procédures internes de déclaration d’incidents
- Limiter les impacts : plan de continuité et de reprise

7 / Culture cybersécurité en entreprise

- Rôle de chacun : tous acteurs de la cybersécurité
- Mettre en place une charte informatique claire
- Instaurer des rappels réguliers et formations continues

8 / ETUDE DE CAS REELS ET CAS PRATIQUES ADAPTES A VOTRE ACTIVITE (situation, causes et impacts sur les activités)

- Employés de tous niveaux utilisant un ordinateur, un smartphone ou une connexion Internet dans leur travail quotidien
- Salariés d’entreprise
- Managers et responsables de service
- Responsables d’équipes devant s’assurer que les bonnes pratiques numériques sont respectées
- Chefs de projet
- Responsables RH
- Comptables
- Responsables logistiques utilisant des données sensibles
- Personnes exposées aux risques de fraude ciblée (type "fraude au président")
- Utilisateurs ayant accès à des données stratégiques : DSI, RSSI, DAF, DRH…
- Membres de la direction (CODIR)
- Personnel en télétravail ou en mobilité, plus exposé aux cyber-risques

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

21 au 22 Juil. 2026	Présentiel -
04 au 05 Août 2026	Présentiel -
24 au 25 Sep. 2026	Présentiel -
06 au 07 Oct. 2026	Présentiel -
26 au 27 Nov. 2026	Présentiel -

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com