DMO Mickaël Ouvrard
Le RGPD simple et efficace

5 rue du Stade,
78300 Poissy
FRANCE

Tél : +336 79 71 28 28
mickaelouvrard@dmouvrard.com
https://dmouvrard.com



Formation « Les premiers gestes de cybersécurité : adopter les bons réflexes au quotidien », en 0,5 jour, par DMOuvrard

Version octobre 2026

ACTIVATEUR [N] FRANCE NUM

Mickaël OUVRARD EI – DMOuvrard
5 rue du Stade, 78300 Poissy – FRANCE
mickaelouvrard@dmouvrard.com - +336 79 71 28 28
Entrepreneur Individuel - SIRET : 918 689 720 00012
N° TVA Intracommunautaire : FR24918689720

Sommaire

Édito 2

La formation 2

Durée : 2

Lieu 2

Profil des stagiaires 2

Objectifs pédagogiques 2

Méthodes pédagogiques 3

Méthodes pédagogiques générales 3

Documents fournis 3

Programme de la formation 3

Module 1 – Comprendre les risques numériques d'aujourd'hui 3

Module 2 – Sécuriser ses accès : mots de passe et authentification 3

Module 3 – Éviter le piège du phishing et des fraudes 4

Module 4 – Protéger ses équipements et ses données 4

Module 5 – Que faire en cas d'incident ? 4

Synthèse finale 4

Édito

La majorité des cyberattaques ne reposent pas sur des techniques complexes mais sur l'exploitation d'erreurs humaines : mot de passe trop faible, clic sur un lien frauduleux, partage d'informations sensibles ou absence de mise à jour.

Quelques réflexes simples permettent pourtant d'éviter une grande partie des incidents de sécurité.

Cette formation vise à sensibiliser les participants aux principaux risques numériques et à leur transmettre les bonnes pratiques applicables immédiatement dans leur activité professionnelle quotidienne.

La formation

Durée :

0,5 jour de 3h30.

Lieu

En présentiel (dans vos locaux pour les formations Intra-entreprises) **ou en distanciel** en mode synchrone (stagiaires en visio). Le mode présentiel est privilégié pour plus d'interactivité et d'efficacité.

Pas de frais de déplacement en Eure et en Ile-de-France.

Profil des stagiaires

Tous profils. tous collaborateurs, managers de proximité, fonctions supports, membres de CSE, associations, TPE, PME et ETI.

Aucun prérequis technique.

Objectifs pédagogiques

- **Comprendre les principales menaces** numériques.
- **Adopter les bonnes pratiques** de cybersécurité au quotidien.
- **Identifier** une tentative de phishing ou une situation suspecte.
- **Sécuriser** ses accès et ses mots de passe.
- **Protéger ses équipements** professionnels et ses données.
- **Réagir de manière appropriée** en cas d'incident.

Méthodes pédagogiques

Méthodes pédagogiques générales

- **Alternance théorie/pratique** dans chaque module.
- **Parties théoriques claires et compréhensibles**.
- Exemples, analyses de situations réelles et ateliers pratiques conçus **pour une mise en œuvre simple, rapide et efficace**.
- Interactivité, échanges, micro-quiz, etc.
- **Outils applicables dès le lendemain**.

Documents fournis

- **Documents pédagogiques** : support de formation, fiche mémo « Les 10 réflexes cybersécurité », checklists d'auto-évaluation du niveau de sécurité, guide ANSSI des bonnes pratiques, grille des premiers réflexes en cas d'incident, affiche de sensibilisation à diffuser dans l'organisation.
- **Documents administratifs** : attestation de formation, questionnaire de satisfaction sur la formation.

Programme de la formation

Module 1 – Comprendre les risques numériques d'aujourd'hui

- **Objectifs :** comprendre les principales cybermenaces et prendre conscience des conséquences possibles pour l'organisation.
- **Contenu** : Pourquoi la cybersécurité concerne tout le monde ; les attaques les plus fréquentes ; les erreurs humaines à l'origine des incidents ; quelques chiffres clés ; les conséquences pour l'entreprise (arrêt d'activité, perte de données, fraude, atteinte à l'image).
- **Méthode** : exposé interactif, quiz de démarrage, échanges avec les participants.

Module 2 – Sécuriser ses accès : mots de passe et authentification

- **Objectifs :** utiliser des mots de passe robustes et comprendre l'intérêt de l'authentification multifacteur.
- **Contenu** : Créer un mot de passe robuste (longueur recommandée, phrase de passe, mots de passe uniques) ; éviter les mauvaises pratiques (réutilisation des mots de passe, conservation sur post-it, enregistrement non maîtrisé) ; utiliser un gestionnaire de mots de passe ; activer la double authentification (MFA)
- **Atelier** : analyse de mots de passe fictifs.

Module 3 – Éviter le piège du phishing et des fraudes

- **Objectifs :** identifier les signaux d'alerte et adopter une posture de vigilance numérique.
- **Contenu** : reconnaître un courriel frauduleux (adresse inhabituelle, ton urgent, pièce jointe inattendue, demande confidentielle) ; vérifier un lien avant de cliquer ; faux paiements et fausses factures ; ingénierie sociale ; règle d'or : « En cas de doute : je vérifie avant d'agir ».
- **Atelier** : analyse collective d'exemples de phishing.

Module 4 – Protéger ses équipements et ses données

- **Objectifs :** adopter une hygiène numérique simple et limiter les risques de perte ou de compromission.
- **Contenu** : les mises à jour (pourquoi elles sont indispensables, activer les mises à jour automatiques) ; les sauvegardes (principe simple ; bonnes pratiques) ; les smartphones et tablettes (verrouillage, applications officielles, mises à jour) ; le télétravail (Wifi sécurisé, écran non visible, documents sensibles) ; les déplacements (ordinateur portable, clé USB, réseaux publics).

Module 5 – Que faire en cas d'incident ?

- **Objectifs :** réagir rapidement et limiter les impacts.
- **Contenu** : les premiers réflexes (débrancher si nécessaire, prévenir rapidement, ne pas dissimuler l'incident, conserver les éléments utiles).
- **Cas pratiques** :
    - Cas n°1 : email envoyé au mauvais destinataire
    - Cas n°2 : ordinateur portable perdu
    - Cas n°3 : phishing réussi.

Synthèse finale

- **Contenu** : Les 10 réflexes à retenir.