



## Gérer la Cybersécurité au Quotidien du Bureau : Phishing, Ingénierie Sociale, Mots de Passe et Réflexes de Protection

Lien :

<https://innov-maroc.com/formation/gerer-la-cybersecurite-au-quotidien-du-bureau-phishing-ingenierie-sociale-mots-de-passe-et-reflexes-de-protection>

 DURÉE  
**4 jours (28h)**

 RÉFÉRENCE  
**AA290**

 CATÉGORIE  
**Efficacité  
Professionnelle et  
Gestion du Quotidien**

## OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les principales menaces de cybersécurité rencontrées dans l'environnement professionnel
- ✓ Identifier les techniques de phishing et les tentatives d'arnaque numérique
- ✓ Reconnaître les mécanismes d'ingénierie sociale et les tentatives de manipulation
- ✓ Adopter de bonnes pratiques pour créer et gérer des mots de passe sécurisés
- ✓ Utiliser correctement l'authentification multifacteur et les gestionnaires de mots de passe
- ✓ Protéger les postes de travail, smartphones, documents et données professionnelles
- ✓ Sécuriser les usages numériques en télétravail et lors des déplacements professionnels
- ✓ Savoir réagir rapidement et correctement en cas de suspicion ou d'incident de cybersécurité
- ✓ Réduire les risques liés aux erreurs humaines et aux comportements à risque
- ✓ Développer des réflexes de cybersécurité simples, pratiques et applicables au quotidien

## POUR QUI ?

- ✓ Assistants(es) de Direction et secrétaires
- ✓ Office Managers et responsables administratifs
- ✓ Collaborateurs des services généraux
- ✓ Responsables RH et managers
- ✓ Collaborateurs des services financiers, achats et commerciaux
- ✓ Personnel administratif et équipes support
- ✓ Télétravailleurs et collaborateurs utilisant des outils numériques professionnels
- ✓ Nouveaux collaborateurs intégrant une organisation
- ✓ Toute personne utilisant quotidiennement une messagerie, un ordinateur ou des applications professionnelles
- ✓ Managers souhaitant renforcer la culture de cybersécurité de leurs équipes



## Programme détaillé

### 1 / Comprendre les risques de cybersécurité au bureau

- Identifier les principales menaces numériques auxquelles sont exposés les collaborateurs
- Comprendre les conséquences d'une erreur humaine sur l'organisation
- Adopter une culture de vigilance et de responsabilité numérique

### 2 / Détecter et éviter le Phishing

- Identifier les e-mails, SMS et messages frauduleux
- Repérer les liens, pièces jointes et demandes inhabituelles
- Appliquer les bons réflexes avant de cliquer, répondre ou transmettre une information

### 3 / Se protéger contre l'ingénierie sociale

- Comprendre les techniques de manipulation utilisées par les cybercriminels
- Identifier les tentatives d'usurpation d'identité et de fraude au président
- Vérifier systématiquement l'identité et la légitimité d'une demande sensible

### 4 / Maîtriser les mots de passe et l'authentification

- Créer et gérer des mots de passe robustes et uniques
- Utiliser correctement un gestionnaire de mots de passe
- Comprendre l'importance de l'authentification multifacteur (MFA)

## 5 / Sécuriser les postes et les données professionnelles

- Verrouiller les sessions et protéger les équipements
- Reconnaître les risques liés aux clés USB, logiciels et fichiers inconnus
- Appliquer les bonnes pratiques de sauvegarde et de protection des données

## 6 / Sécuriser les usages du télétravail et du mobile

- Protéger les ordinateurs et smartphones professionnels
- Utiliser correctement les réseaux Wi-Fi et connexions distantes
- Éviter les fuites de données lors des déplacements et du travail hors site

## 7 / Réagir face à un incident de cybersécurité

- Identifier rapidement un comportement ou événement suspect
- Savoir quoi faire après un clic sur un lien ou une pièce jointe malveillante
- Signaler efficacement les incidents aux équipes compétentes

## 8 / Construire les réflexes de cybersécurité au quotidien

- Mettre en place une checklist des comportements sécurisés
- Éviter les erreurs humaines les plus fréquentes
- Développer une culture durable de vigilance et de protection numérique

## Approche pédagogique

- ✓ Support Ecrit et Projection
- ✓ Exposés Interactifs, Podcasts et Vidéos
- ✓ Brainstorming et Jeux de Rôle
- ✓ Mises en Situation pour faciliter l'assimilation
- ✓ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✓ Test de Validation des Acquis des Connaissances

## Prochaines dates programmées

 08 au 11 Déc. 2026

 Présentiel - Casablanca

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

## Réservation & Renseignements

 **Téléphone** : +212 522 247 210

 **Email** : [contact@innov-maroc.com](mailto:contact@innov-maroc.com)

 **Web** : <https://www.innov-maroc.com>

Document généré le 12/10/2026 — Réf : AA290  
INNOV MAROC — Tous droits réservés