

IT Security

Sensibilisation à la Sécurité Informatique

Une formation de sensibilisation qui donne à chaque collaborateur les réflexes essentiels pour protéger les informations de l'entreprise et se prémunir des cybermenaces, au bureau comme en télétravail.

DURÉE 14 heures	NIVEAU Débutant	FORMAT Présentiel & en ligne
LANGUE Français	CERTIFICAT —	FORMATEUR Nizar Haddad

Présentation

La sécurité informatique ne repose pas uniquement sur des outils techniques : le facteur humain reste le premier vecteur d'incident. Cette formation de sensibilisation s'adresse à l'ensemble des collaborateurs afin de leur faire prendre conscience des risques cyber et de leur transmettre les bonnes pratiques du quotidien.

Au fil du programme, les participants découvrent le panorama actuel des menaces (phishing, ingénierie sociale, rançongiciels, APT), le contexte législatif et leurs responsabilités, ainsi que les gestes concrets pour sécuriser leur poste de travail, leurs déplacements et leurs usages d'Internet. Une large place est accordée aux situations de nomadisme, de télétravail et de BYOD, devenues incontournables.

À l'issue de la formation, chaque participant sait reconnaître une tentative d'attaque, adopter les réflexes de protection durable et réagir efficacement en cas d'incident, contribuant ainsi à réduire les risques juridiques et opérationnels pour l'entreprise.

Objectifs pédagogiques

- ✓ Comprendre les enjeux de la sécurité informatique pour l'entreprise et le télétravailleur, ainsi que le rôle du facteur humain
- ✓ Identifier les biens à protéger et les principaux moyens de sécurisation
- ✓ Connaître le cadre législatif, les responsabilités civiles et pénales et le rôle des autorités de protection des données
- ✓ Reconnaître les principales menaces : phishing, ingénierie sociale, rançongiciels et attaques ciblées (APT)
- ✓ Sécuriser son poste de travail, ses périphériques et ses connexions en situation de nomadisme, télétravail et BYOD
- ✓ Adopter des usages sûrs d'Internet, de la messagerie et des supports amovibles
- ✓ Réagir correctement en cas d'attaque et appliquer les gestes de premiers secours numériques
- ✓ Mettre en place des réflexes de protection durable (mises à jour, antivirus, sauvegardes, plan de reprise)

Programme détaillé

La sécurité informatique pour l'entreprise et le collaborateur

- Contexte de la cybercriminalité
- Les briques de la sécurité
- Les biens à protéger et les moyens de sécurisation
- Le facteur humain, maillon clé de la sécurité

Contexte législatif et responsabilités

- Cadre législatif et réglementaire
- Responsabilités civile et pénale
- Principales lois applicables
- Rôle des autorités de protection des données (type CNIL)

Panorama des menaces

- Typologies de menaces
- Advanced Persistent Threat (APT)
- Ingénierie sociale et phishing
- Comportements à risque en et hors entreprise

Sécuriser le poste de travail et les périphériques

- Vocabulaire réseau et notions de firewall
- Risques liés aux périphériques
- Sécurisation des systèmes Windows
- Mécanismes de propagation virale

Nomadisme, télétravail et BYOD

- Risques des postes portables et des visiteurs
- Connexions sécurisées et accès VPN
- Services cloud et communications unifiées (UCaaS)
- Bonnes pratiques du BYOD

Maîtriser les risques d'Internet

- Navigation et téléchargements sûrs
- Configuration des navigateurs
- Sécurité de la messagerie électronique
- Usage maîtrisé des clés USB et supports amovibles

Réagir en cas d'attaque

- Comportements à adopter face à un incident
- Gestes de premiers secours numériques
- Évaluation des dégâts

Protection durable, synthèse et conclusion

- Réflexes quotidiens de protection
- Chantage informatique et rançongiciels
- Mises à jour, antivirus, sauvegarde et plan de reprise
- Récapitulatif, évaluation des risques et bonnes conduites

Prérequis

Aucun prérequis particulier.

Public visé

Tous les collaborateurs de l'entreprise, quel que soit leur niveau technique : utilisateurs, employés de bureau, personnel en télétravail ou en mobilité, ainsi que les managers souhaitant instaurer une culture de la cybersécurité.

Prochaines sessions

DATE	VILLE	HORAIRE	FORMATEUR
03/08/2026	En ligne	09h00 - 16h00	Nizar Haddad
07/09/2026	Tunis	09h00 - 16h00	Nizar Haddad

500 TND / personne

Acompte de 30% possible à la réservation · Financement sur demande.

Experteam — El Ghazala, Ariana (face au Technopôle La Ghazela)

+216 29 674 204 · contact@expertunisie.com · experteam.itt.tn