FORMATION INTRA-ENTREPRISE · 3H30

SENSIBILISATION CYBERSÉCURITÉ

RGPD & Souveraineté de la donnée

Une erreur humaine est à l'origine de 99 % des compromissions.

Cette formation de sensibilisation transforme vos collaborateurs en première ligne de défense face à la menace cyber — quel que soit leur niveau technique — en reliant menace, cadre juridique (RGPD), souveraineté de la donnée et usage responsable de l'intelligence artificielle.

DURÉE	FORMAT	PUBLIC	PRÉREQUIS
3h30 · 6 modules	Présentiel, intra-entreprise	Tous les collaborateurs	Aucun

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, les participants seront en mesure de :

- ✓ Comprendre et matérialiser la menace cyber pesant sur les données de l'entreprise et la vie privée des collaborateurs
- ✓ Identifier les enjeux réputationnels et juridiques d'une fuite ou d'une mauvaise gestion des données
- ✓ Connaître les acteurs malveillants (hackers étatiques, mafias cybercriminelles, IA adversariale) et leur modèle économique
- ✓ Adopter les bonnes pratiques quotidiennes : postes de travail, mobile, mots de passe, double authentification
- ✓ Utiliser l'intelligence artificielle en milieu professionnel de façon responsable et conforme
- ✓ Connaître ses droits et obligations au titre du RGPD, de la Charte SI et du droit applicable
- ✓ Prendre conscience des enjeux de la souveraineté de la donnée, aux niveaux individuel et organisationnel

PROGRAMME DE LA FORMATION

6 modules — durée totale 3h30 (pause de 10 min incluse)

M1 — **Sécurité, données & sensibilisation** — 30 min
Film ELLA ; sécurité globale vs sécurité informatique ; démonstration de l'outil ThreatManagement de Check Point ; mesure de l'exposition de l'organisation.

M2 — **Paysage des menaces cyber — catégories & modes opératoires** — 35 min
Phishing, ransomware, DDoS, ingénierie sociale, malware, supply chain, MitM, insider threat, 0-day, force brute ; films « La Hack Académie » (ANSSI) et Bank.

M3 — **Acteurs de la menace — hackers, États, IA & économie parallèle** — 30 min
APT étatiques, organisations mafieuses RaaS, hacktivistes, menace interne ; rôle de l'IA ; économie du dark web et valeur marchande des données.

M4 — **Cadre juridique — RGPD, droits & devoirs** — 25 min
Fondements (art. 8 CEDH, art. 13 Cst. féd. suisse) ; principes du RGPD (UE 2016/679) ; Data Privacy / Privacy Shield ; Cloud Act et FISA Section 702.

M5 — **Intelligence artificielle en milieu professionnel & souveraineté** — 25 min
Risques juridiques de l'IA (confidentialité, propriété intellectuelle, hallucinations) ; IA américaine, chinoise et souveraine ; bonnes pratiques d'usage.

M6 — **Charte SI & bonnes pratiques — ingénierie sociale, mots de passe** — 25 min
Portée juridique de la Charte SI ; ingénierie sociale (prétexting, baiting, vishing, shoulder surfing) ; gestion des mots de passe, MFA, sécurité du mobile.

PAUSE · 10 MIN

MÉTHODES PÉDAGOGIQUES

Apports théoriques
Présentation magistrale sur supports PowerPoint : triade CIA, principes du RGPD, cartographie des acteurs, économie du cybercrime.

Supports audiovisuels immersifs
Trois films pédagogiques — ELLA (3 min), « La Hack Académie » (ANSSI, ~12 min) et le film Bank — pour une mise en situation concrète.

Démonstrations en direct
Outil ThreatManagement de Check Point, pour contextualiser la menace de façon chiffrée et en temps réel.

Discussions interactives
Échanges structurés après chaque film : identification des vecteurs d'attaque et transposition aux habitudes professionnelles.

Tableaux comparatifs & études de cas
Valeur des données sur le dark web ; comparaison des juridictions européenne, américaine et chinoise.

MODALITÉS D'ÉVALUATION DES ACQUIS

- Fiche d'émargement individuelle attestant de la participation effective à l'ensemble de la session.
- Questionnaire d'évaluation des acquis en fin de parcours, mesurant la progression de chaque bénéficiaire au regard des objectifs pédagogiques annoncés, complété par un recueil de satisfaction à froid.
- Attestation de formation délivrée par UBCOM France SAS (objectifs, nature, durée et résultats de l'évaluation), conformément à l'article L.6353-1 du Code du travail.
- Exercice de phishing simulé recommandé dans les 90 jours suivant la formation, pour mesurer l'ancrage des apprentissages.
- Discussions post-projection après chaque film, afin de vérifier la compréhension et la capacité de transposition au contexte professionnel.

MODALITÉS & DÉLAIS D'ACCÈS

Formation dispensée en présentiel, dans les locaux du client ou dans un espace mis à disposition par UBCOM. Aucun délai particulier : la session est organisée selon les disponibilités convenues avec le client.

ACCESSIBILITÉ & HANDICAP

UBCOM prend en compte toute situation particulière signalée lors de l'inscription et adapte les modalités pédagogiques en conséquence (délais, supports, format des échanges), en s'appuyant sur un réseau de partenaires spécialisés dans l'accompagnement du handicap.

POURQUOI CHOISIR UBCOM POUR FORMER VOS ÉQUIPES ?

UBCOM porte une doctrine *by design* de la protection du secret et de la souveraineté numérique européenne. Forte d'une solide expérience en contre-espionnage économique et d'une neutralité ancrée dans la Confédération suisse, l'agence relie enjeux techniques, juridiques et humains pour faire de la vigilance une culture d'entreprise durable.

Expertise en contre-espionnage & données classifiées

Neutralité suisse, souveraineté européenne

Approche concrète : films, démonstrations, cas réels

TARIF DE LA SESSION

2 400 €

Forfait par session, hors frais de déplacement éventuels.
Format présentiel, intra-entreprise.

Contact : gv@ubcom.eu · **www.ubcom.eu**