FORMATION

Cybersécurité – Pack Niveau 1–2 (CYBER-SECU-04)

Description

Ce pack combine les niveaux 1 et 2 pour couvrir à la fois les fondamentaux et les attaques les plus courantes, puis approfondir avec des scénarios réalistes (phishing avancé, usurpation, risques OAuth, sécurité du navigateur) et des mises en situation. À l'issue de la formation, vous disposerez de réflexes concrets pour réduire significativement le risque utilisateur et améliorer la réponse aux incidents simples.

Objectifs

Identifier les menaces majeures (phishing, ransomware, vol de données) et appliquer les bons réflexes de prévention.
Sécuriser l'usage du poste (Windows 11) et de Microsoft 365 (sessions, navigation, formulaires/pièges).
Reconnaître des attaques de phishing avancé et des usurpations crédibles (scénarios réalistes).
Identifier les risques OAuth et appliquer des règles simples pour éviter les compromissions.
Sécuriser l'usage du navigateur (extensions, données, profils) et réduire la surface d'attaque utilisateur.
Appliquer une conduite à tenir en cas d'incident utilisateur (premières actions, escalade, traces utiles).

Public concerné

Collaborateurs entreprises / Tous publics.

Prérequis

Utilisation d'un ordinateur et d'une messagerie dans le cadre professionnel ou personnel.

Programme (aperçu)

Module 1 — Panorama des menaces : menaces PME, chaîne d'attaque, phishing, ransomware, cas réels.
Module 2 — Hygiène Windows 11 & sessions : verrouillage, mots de passe, postes partagés, fichiers à risque.
Module 3 — Navigateurs & M365 : profils pro/perso, rester connecté, pages factices, formulaires.
Module 4 — Évaluation & ancrage : quiz final, mini-scénarios, débriefing.
Module 5 — Phishing avancé & usurpation : sur Microsoft 365, MFA.
Module 6 — OAuth & fausses vérifications : phishing sophistiqué, compromission d'une boîte mail, faux messages Microsoft 365.
Module 7 — Navigateurs & extensions avancées : vol de données via le navigateur, extensions, bonnes pratiques.
Module 8 — Simulations & gestion d'incident : simulations de phishing, jeu de rôle "incident utilisateur", gestion d'incident basique.
Module 9 — Quiz & certification intermédiaire : quiz renforcé, cas pratiques rapides, restitution.

FORMATION

Durée & modalités

La formation a lieu sur le site de l'entreprise demandeuse ou à distance par visioconférence, elle est animée par un formateur. **Durée totale :** 8 h (2 demi-journées, consécutives ou non). **Groupe :** 5 apprenants maximum.

Tarif

Tarif : 1 440 €.
Tarifs exprimés hors taxes. TVA non applicable conformément à l'article 293 B du Code général des impôts.
Financement : Fonds propres ou via prise en charge OPCO (convention requise, voir conditions auprès de votre OPCO).

Méthodes pédagogiques

Les apprenants ont accès à un espace virtuel où ils peuvent obtenir des documents. Les formations appliquent une pédagogie interactive et ludique, avec une alternance d'apports théoriques et de mises en situation pratiques. Un support de formation sera remis aux participants, et un livret pédagogique leur permettra de réaliser différents exercices tout au long du parcours.

Évaluation

L'auto-évaluation des acquis et de l'atteinte des objectifs est réalisée à partir d'une série de quiz à la fin de chaque session. Attestation de formation délivrée par DPh Formation.

Accessibilité

Nous accordons une attention particulière à garantir que nos formations soient accessibles à tous. Pour cela, nous proposons un entretien personnalisé aux personnes en situation de handicap, afin de mieux comprendre leurs besoins spécifiques et d'identifier les aménagements ou dispositions nécessaires. Référent handicap : handicap@dphformation.fr. Registre d'accessibilité : en cours.

Délais d'accès

Délais d'accès : sous 72h.

Contact

DPh Formation
2 rue de la Mairie, 03300 Creuzier-le-Neuf
Email : contact@dphformation.fr
Téléphone : 07 87 70 22 66