

Cybersécurité – Pack Niveau 1–2–3 (CYBER-SECU-05)

Description

Ce pack complet regroupe les niveaux 1, 2 et 3 : il couvre les fondamentaux indispensables, approfondit avec des attaques avancées et des simulations, puis complète par une mise en situation « crise cyber », un plan d'action personnalisé et une certification avancée. Il vise à ancrer des réflexes durables et à structurer une réponse organisationnelle simple et efficace.

Objectifs

Appliquer les fondamentaux de protection utilisateur (poste, navigation, messagerie, Microsoft 365).

Détecter et analyser des attaques plus avancées (usurpation, OAuth, faux messages/validations).

Réussir des simulations (phishing / incident) et adopter une conduite à tenir adaptée.

Adapter les mesures de cybersécurité aux fonctions clés de l'entreprise (par métier/process).

Mettre en place des mesures organisationnelles prioritaires (ex. double validation, procédures critiques).

Contribuer à un plan d'actions cyber priorisé et réaliste (quick wins / chantiers 3–6 mois).

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.

Module 10 — Cybersécurité par fonction : adapter les réflexes à chaque type de poste.

Module 11 — Double validation financière & procédures critiques : formaliser des barrières organisationnelles simples.

Module 12 — Jeu de rôle « Crise cyber » : mise en situation de crise simulée pour tester les réflexes.

Module 13 — Plan d'action personnalisé & certification avancée : plan simple et réaliste pour l'entreprise.

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** : 12 h (3 demi-journées, consécutives ou non). **Groupe** : 5 apprenants maximum.

Tarif

Tarif : 2 160 €.

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