Fiche Technique:formation cybersécurité bonnes pratiques pour utilisateurs

Objectifs de la formation

Objectifs concrets et mesurables, orientés gestes utiles au quotidien.

- Réduire les erreurs humaines et harmoniser les pratiques entre équipes.
- Détecter phishing/arnaques, vérifier les liens et signaler rapidement un incident.
- Renforcer les accès: mots de passe robustes avec coffre-fort et MFA adapté.
- Sécuriser le poste, les navigateurs, le Wi-Fi et la mobilité.
- Protéger la donnée: classification, partage temporaire, liens publics maîtrisés, chiffrement.
- Intégrer les bonnes pratiques aux processus métiers et mesurer les progrès dans le temps.

Population cible

Ciblage large, centré sur les utilisateurs quotidiens du numérique.

- Tous collaborateurs utilisant messagerie, suites bureautiques et outils métiers.
- Prérequis: savoir utiliser un PC/smartphone, disposer d’un compte de messagerie, notions de base de la suite collaborative.
- Managers et directions métiers; fonctions support (RH, Finance, Juridique, Achat).
- Collaborateurs bureautiques, télétravailleurs et équipes commerciales exposées aux échanges externes.
- Prestataires, intérimaires, partenaires: accès temporaires, règles d’authentification et partage limité.
- Référents sécurité non techniques comme relais de proximité.

Durée de la formation

> Formats disponibles: présentiel, classe virtuelle, e-learning asynchrone et campagnes de phishing. Évaluations pré/post et quiz par module possibles (intégration LMS SCORM/xAPI).

Format	Public	Durée
Essentiel	Tout utilisateur	2 h
Atelier+	Équipes clés	1/2 journée
Parcours	Entreprise	1–2 jours
Blended	Multi-sites	4–6 semaines

Programme de la formation

Modules complémentaires mêlant concepts clés, démonstrations et exercices guidés.

Module 1 – Fondamentaux et panorama des menaces

- Typologies: phishing, smishing, vishing, malware, fraude, BEC.
- Marqueurs: expéditeur, liens, pièces jointes inhabituelles, urgence artificielle.

Module 2 – Rôle des dirigeants, exemplarité et gouvernance

- Sponsoring, exemplarité (MFA, partage limité) et suivi d'indicateurs.
- Traduire la stratégie en comportements, éviter la fatigue de sensibilisation.

Module 3 – Hygiène numérique au poste de travail

- Mises à jour, navigateurs, téléchargements, macros, signatures numériques.
- Télétravail: Wi-Fi, VPN, périphériques, machines partagées.

Module 4 – Mots de passe et authentification multifacteur

- Passphrases, non-réutilisation, coffre-fort d'équipe et partage sécurisé.
- MFA selon les rôles: application, clés FIDO2; SMS en dernier recours.

Module 5 – Phishing, arnaques et ingénierie sociale

- Lecture critique, inspection des liens, vérification hors bande.
- Signalement en un clic, panorama des arnaques fréquentes.

Module 6 – Protection des données et collaboration cloud

- Classification, niveaux de confidentialité, espaces partagés.
- Liens expirants, partage temporaire, chiffrement à bon escient.

Module 7 – Réponse aux incidents pour utilisateurs

- Gestes immédiats après clic suspect et triage de premier niveau.
- Isolement, escalade, reprise d'activité et retour d'expérience.

Module 8 – Spécificités sectorielles et contexte régional

- Adaptation aux réglementations, outils et pratiques locales.
- Scénarios contextualisés selon le secteur et la région.