PROGRAMME DE FORMATION

CYBERSÉCURITÉ POUR TOUS : LES BONS RÉFLEXES AU QUOTIDIEN - 1/2 JOURNÉE (3 H 30)

Une demi-journée pour adopter, au quotidien, les bonnes pratiques qui protègent des cybermenaces les plus courantes - reconnaître une attaque, sécuriser ses accès, réagir en cas de doute.

OBJECTIFS PEDAGOGIQUES

- **Reconnaître les cybermenaces :** Identifier les attaques qui visent un salarié ordinaire : hameçonnage, rançongiciel, fraude.
- **Déjouer l'hameçonnage :** Repérer un message, un lien ou un site frauduleux avant de cliquer.
- **Sécuriser ses accès :** Gérer ses mots de passe et activer la double authentification.
- **Protéger poste et données :** De bons réflexes au bureau comme en mobilité, dans le respect du RGPD.
- **Réagir en cas d'incident :** Savoir quoi faire, qui alerter, et signaler sans crainte.

PROGRAMME

Pourquoi suis-je une cible ?

- Ce que cherchent les attaquants : argent, données, accès, rebond vers l'entreprise
- Le maillon humain : pourquoi la technique ne suffit pas
- Panorama des menaces courantes : hameçonnage, rançongiciel, arnaque au président, fraude

L'hameçonnage : reconnaître et déjouer

- Anatomie d'un courriel piégé : expéditeur, urgence, pièce jointe, lien
- Repérer une adresse ou un site frauduleux
- Hameçonnage par SMS et par téléphone
- Exercice : trier de vrais et de faux messages

Mots de passe et authentification

- Ce qui fait un bon mot de passe - et les idées reçues
- Le gestionnaire de mots de passe : pourquoi, comment
- La double authentification, votre meilleure protection
- Ne jamais réutiliser : l'effet domino d'une fuite

Poste, données et incident

- Mises à jour, verrouillage, clés USB, Wi-Fi public, télétravail
- Pièces jointes, partages et données sensibles (notions RGPD)
- En cas de doute : ne pas cliquer, ne pas payer, ne pas effacer - qui alerter
- Synthèse : les dix réflexes à retenir + quiz

INFORMATIONS PRATIQUES

Duree	1/2 journée (3 h 30)
Public	Tous les collaborateurs
Prerequis	Aucun prérequis technique.
Modalites	Présentiel (dans vos locaux partout en France) ou classe virtuelle. Groupe conseillé : 4 à 12 personnes.
Methodes	Apports illustrés d'exemples réels, démonstrations, mises en situation et exercices interactifs. Support de synthèse remis à chaque participant.
Evaluation	Quiz de positionnement et de validation des acquis ; attestation de fin de formation.
Intervenant	Intervenant spécialisé en sûreté et cybersécurité, à l'expérience de terrain (analyse des menaces, modes opératoires de la malveillance, gestion de crise et sécurité économique).
Tarif	Nous consulter - devis sous 24 h ouvrees. DTJ Training n'etant pas certifie Qualiopi, aucun financement OPCO n'est mobilisable a ce jour.
Delai d'acces	2 semaines entre l'inscription et le démarrage. Ce délai peut être allongé si un dossier de financement doit être instruit.
Accessibilite	Formation ouverte aux personnes en situation de handicap - les aménagements sont étudiés avec notre référent handicap (contact@dtjtraining.fr), réponse sous 5 jours ouvrés.

Contact	DTJ Training - 5 rue des Indes Noires, Batiment Grand Large, Pole Jules Verne, 80440 Boves - contact@dtjtraining.fr - 09 56 52 37 64

Document commercial. Le programme detaille (competences visees, modalites d'evaluation et identite du formateur) est communique sur demande et finalise avec l'intervenant.