Module digital learning prêt à l'emploi

Cybersécurité

⏱️ Durée	👩‍💼 Cible	🔐 Prérequis	💻 Supports
40 min	Tous les collaborateurs	Aucun	Ordinateur Mobile Tablette

🎯 OBJECTIFS

Ce module s'adresse à toutes les personnes souhaitant être sensibilisées à la cybersécurité.

À l'issue de ce module les apprenants sauront :

- Définir les menaces en matière de détournement du système d'information
- Reconnaître les situations à risque
- Agir de façon appropriée pour assurer la protection des données

🎓 DÉMARCHE PÉDAGOGIQUE

- Des activités pédagogiques successives, insérées dans un scénario, portant sur des décisions à prendre ayant une incidence sur le niveau de sécurité des données
- Une jauge dont le niveau varie en fonction des choix faits : le niveau de cette jauge doit être supérieur ou égal à 80 pour valider le module
- Des règles de sécurité et bonnes pratiques sont découvertes au fil de la progression et sont toutes recensées dans un espace dédié consultable à tout moment du module

🚀 MODALITÉS DE DÉPLOIEMENT

- FULL : accès à l'intégralité du catalogue (+50 modules), dont celui-ci
- START : location du module à l'unité via notre plateforme LMS mutualisée UPility
- FLEX : achat du module, livraison du fichier SCORM, personnalisation possible

Callimedia
by Bealink

SOMMAIRE DU MODULE

Introduction – Données manipulées et objectifs

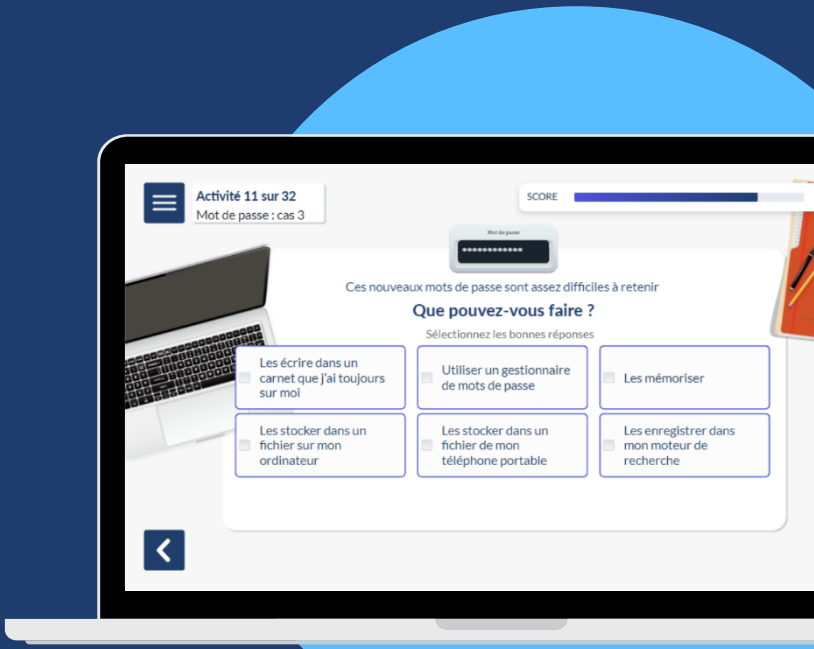
La courte introduction souligne que la protection des données manipulées concerne chacun. Elle met aussi en évidence les risques associés à ces données et, par conséquent, la nécessité de les sécuriser, notamment grâce à la cybersécurité.

Elle se conclut par l'annonce d'une série d'activités destinées à permettre aux apprenants d'évaluer leurs réflexes en cybersécurité et de découvrir les principales règles de sécurité.

Sujets des activités et des règles de sécurité

Les différentes activités de ce module abordent les thématiques suivantes :

- La définition, la gestion et la protection des mots de passe, incluant l'authentification multi-facteurs (MFA)
- L'utilisation des antivirus et l'importance des mises à jour régulières
- Les dangers du phishing, du « Social Engineering » et du « Ransomware »
- Les bonnes pratiques concernant le matériel informatique et téléphonique, au bureau et en déplacement
- La sauvegarde sécurisée des données et la protection et le partage sécurisé de documents



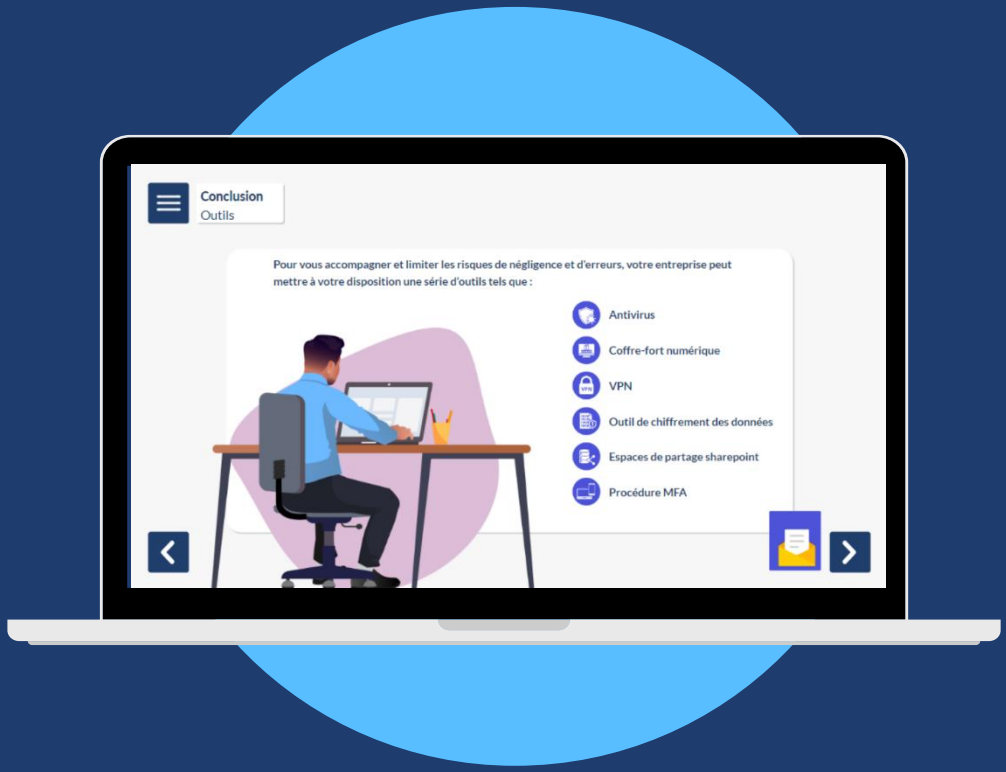
- La sélection des accès Internet, l'utilisation de VPN et le choix des site ou plateforme de téléchargement de logiciels
- La distinction claire entre les appareils personnels et professionnels
- Les réflexes à adopter en cas de cyberattaque et les réactions appropriées

Callimedia
by Bealink

Conclusion

À la fin des activités, les outils que l'entreprise peut déployer pour prévenir les risques de négligence et d'erreurs sont énoncés.

Ensuite le score obtenu par l'apprenant est repris et on lui indique s'il a validé le module : un score minimum de 80 est attendu.



ENVIE D'EN SAVOIR PLUS ?

Demander une démo gratuite du module

Voir le catalogue de formations complet

Callimedia by Bealink
contact@callimedia.fr
+33 (0)4 67 02 10 00
www.callimedia.fr