Devictio formations

MAGNIS FORMATION by Devictio

PiXio by Devictio

PROGRAMME

Formation Sensibilisation des collaborateurs aux cyberattaques

TECHNOLOGIES NUMÉRIQUES

SOFT SKILLS

MARQUE EMPLOYEUR

HANDICAP

PARCOURS CERTIFIANTS

PRÉVENTION

CENTRE DE FORMATION PROFESSIONNELLE

depuis 2007

Qualiopi processus certifié

Certification qualité délivrée au titre de la catégorie **«Actions de formation»**

PARMI NOS THÉMATIQUES

Devictio formations

Informatique & Management

- Informatique / Bureautique
- PAO - 3D - Vidéo
- Web / E-Marketing
- Management / Communication
- Juridique / Comptabilité
- Commercial / Efficacité professionnelle
- Handicap
- QVCT / RPS
- Marque employeur
- Parcours certifiants

MAGNIS FORMATION by Devictio

Sécurité & Prévention

- AIPR
- SST (Sauveteur Secouriste du Travail) / MAC SST
- Habilitations électriques
- CACES
- Manipulation d'extincteurs
- Hygiène alimentaire
- Travail en hauteur
- CSE SSCT
- Geste & posture TMS
- Sécurité Incendie

Pixio by Devictio

E-Learning & Développement personnel

- Langues étrangères
- Développement commercial DISC & WPMOT
- Développement personnel
- E-learning
- Marketing Entreprise
- Parcours en digital

DES FORMATIONS
QUALIFIANTES ET CERTIFIANTES

> *Tous nos formateurs sont des consultants et des professionnels* **experts dans leur domaine** *d'intervention [...]*

VOUS ÊTES

Une entreprise et vous souhaitez développer les compétences de vos salariés ? Renforcer votre marque employeur ? Renforcer la prévention et la sécurité dans vos locaux ?

Un particulier (salarié ou demandeur d'emploi) et vous souhaitez acquérir ou renforcer vos compétences sur les outils informatiques, en soft sills ou en développement personnel ? Obtenir une certification professionnelle ?

NOS SOLUTIONS

Formation en groupe ou sur-mesure, en centre ou sur site. Présentiel, distanciel, e-learning, apprentissage mixte (blended learning). Nos stages comprennent des mise en situation et de nombreux travaux pratiques. Nos certifications professionnelles vous permettrons de mettre en avant votre expertise.

NOS FORMATEURS

Nos formateurs sont à la fois professionnels et intervenants, ils vous font bénéficier de leur expérience professionnelle cumulée à leur compétence pédagogique. Quel que soit votre niveau, ils sauront vous écouter et vous accompagner pour vous aider à acquérir toutes les compétences nécessaires.

FAITES NOUS PART **DE VOTRE PROJET**

04 72 64 25 19
formation@devictio.fr

Formation Sensibilisation des collaborateurs aux cyberattaques

Référence : CECYB101

Nombre de stagiaires max : 5

Modalités d'inscription :
Les inscriptions sont possibles :

- **Jusqu'à 48 heures avant le début de la formation**, sous réserve des places disponibles, pour les financements en **autofinancement ou via le plan de développement des compétences de l'entreprise**.
- **Au plus tard 11 jours ouvrés avant le début de la session** pour toute inscription financée par le **Compte Personnel de Formation (CPF)**, conformément à la réglementation en vigueur.
- **Environ 4 semaines avant le début de la formation** pour les demandes de financement auprès d\'un **OPCO** ou de **France Travail**, afin de permettre l'instruction du dossier.

Accessibilité aux personnes en situation de handicap :
Devictio s'engage à favoriser l'accès à ses formations aux personnes en situation de handicap. Pour étudier les possibilités d'adaptation de la formation à vos besoins, nous vous invitons à contacter notre référent handicap :

- 04 72 64 25 19
- formation@devictio.fr

Public visé :

- Collaborateurs de tous services et de tous niveaux hiérarchiques.
- Salariés utilisant une messagerie électronique, un ordinateur, un smartphone ou des outils collaboratifs.
- Managers et responsables d’équipe.
- Personnel administratif, commercial, comptable ou technique.
- Utilisateurs travaillant en présentiel, à distance ou en situation de mobilité.
- Nouveaux collaborateurs intégrant l’entreprise.
- Toute personne souhaitant adopter des pratiques numériques plus sûres dans son activité professionnelle.

Objectifs :

- Comprendre les enjeux humains, organisationnels et économiques de la cybersécurité.
- Identifier les principales méthodes utilisées par les cybercriminels.
- Reconnaître un courriel, un message, un appel ou un site Internet frauduleux.
- Détecter les signes caractéristiques d'une tentative de phishing ou d'ingénierie sociale.
- Créer et gérer des mots de passe robustes.
- Comprendre l'intérêt de l'authentification multifacteur.
- Protéger les données professionnelles lors du travail sur site, à distance ou en déplacement.
- Adopter les bons réflexes en cas de doute, d'erreur ou d'incident de sécurité.
- Contribuer à développer une culture commune de la cybersécurité au sein de l'organisation.

Compétences visées :

- Reconnaître les principales formes de cyberattaques visant les utilisateurs.
- Analyser la fiabilité apparente d'un courriel, d'un lien, d'une pièce jointe ou d'une demande inhabituelle.
- Identifier les tentatives de manipulation fondées sur l'urgence, l'autorité, la peur ou la confiance.
- Appliquer les règles essentielles de gestion des mots de passe et des accès.
- Sécuriser l'utilisation quotidienne de la messagerie, des outils collaboratifs, des appareils mobiles et du cloud.
- Limiter les risques liés au télétravail, aux réseaux Wi-Fi et aux supports amovibles.
- Signaler rapidement une situation suspecte selon la procédure interne de l'entreprise.
- Réagir de manière appropriée après avoir cliqué sur un lien frauduleux ou transmis une information sensible.

Moyens techniques et pédagogiques :

Mises en situation par le biais d'exercices.
Répétitions des manipulations pour mémoriser l'utilisation des outils présentés.
Un ordinateur par personne.
Support de cours remis sur clé USB ou en format papier à la fin de la formation.

Modalités d'évaluation :

Évaluation pédagogique (orale et/ou écrite) effectuée à la fin de la formation afin d'attester l'acquisition de compétences. Exercice de synthèse.

Validation de la formation :

Attestation de fin de formation envoyée par mail.

Pré-requis :

- Aucun prérequis technique en informatique ou en cybersécurité n'est nécessaire.

- Utiliser couramment une messagerie électronique et les outils numériques professionnels.
- Disposer, lorsque la formation est organisée à distance, d'un ordinateur connecté à Internet, d'un navigateur récent, d'un micro et d'une webcam.

Durée : 1 jour(s) / 7 heures

Points abordés :

Module 1 – Comprendre les enjeux de la cybersécurité

- Définition de la cybersécurité et présentation des principaux enjeux pour l'entreprise.
- Pourquoi les collaborateurs constituent-ils une cible privilégiée ?
- Les conséquences possibles d'une cyberattaque :
  - vol ou destruction de données ;
  - interruption de l'activité ;
  - fraude financière ;
  - atteinte à l'image et à la réputation ;
  - perte de confiance des clients et partenaires ;
  - conséquences juridiques et contractuelles.
- Les notions essentielles : menace, vulnérabilité, risque, incident et attaque.
- Le rôle de chaque collaborateur dans la protection du système d'information.
- Étude de cas : analyse des conséquences d'une attaque au sein d'une organisation.

Module 2 – Reconnaître les principales cyberattaques

- Le phishing par courrier électronique.
- Le spear phishing ou hameçonnage ciblé.
- Le smishing par SMS et messagerie instantanée.
- Le vishing ou fraude par téléphone.
- L'usurpation d'identité et l'utilisation frauduleuse d'une adresse électronique.
- La fraude au président et les faux ordres de virement.
- Les fausses factures et les demandes de changement de coordonnées bancaires.
- Les logiciels malveillants :
  - virus ;
  - chevaux de Troie ;
  - logiciels espions ;
  - ransomwares.
- Les faux sites Internet et les pages de connexion frauduleuses.
- Les QR codes malveillants.
- Les risques liés aux pièces jointes, aux macros et aux fichiers téléchargés.
- Exercice : repérer les indices suspects dans plusieurs exemples de messages.

Module 3 – Comprendre l'ingénierie sociale

- Définition et principes de l'ingénierie sociale.
- Les leviers psychologiques utilisés par les fraudeurs :
  - urgence ;
  - autorité ;
  - peur ;
  - curiosité ;
  - récompense ;
  - confiance ;
  - pression hiérarchique.
- Les demandes inhabituelles provenant apparemment d'un dirigeant, d'un fournisseur ou d'un collègue.
- La collecte d'informations sur les réseaux sociaux.
- Les risques associés aux publications professionnelles et personnelles.
- Les deepfakes vocaux ou vidéo et les nouvelles formes d'usurpation assistées par l'intelligence artificielle.
- Les méthodes de vérification avant d'exécuter une demande sensible.
- Mise en situation : analyser une demande urgente et choisir la bonne réaction.

Module 4 – Sécuriser les mots de passe et les accès

- Les erreurs fréquentes dans la création et la réutilisation des mots de passe.
- Créer une phrase de passe longue et robuste.
- Utiliser un mot de passe différent pour chaque service sensible.
- Comprendre l'intérêt d'un gestionnaire de mots de passe.
- Activer et utiliser l'authentification multifacteur.
- Ne jamais transmettre ses codes d'accès, même à une personne se présentant comme un technicien.
- Verrouiller sa session en cas d'absence.
- Reconnaître une fausse page de connexion.
- Atelier : analyser la robustesse de différentes pratiques d'authentification.

Module 5 – Protéger les données et les équipements

- Identifier les informations sensibles de l'entreprise.
- Appliquer les règles de confidentialité et de partage des documents.
- Vérifier les destinataires avant l'envoi d'un courriel.
- Limiter les transferts de données vers des outils personnels ou non autorisés.
- Installer les mises à jour de sécurité et respecter les consignes du service informatique.
- Utiliser avec prudence les supports USB et les périphériques externes.
- Protéger les ordinateurs, tablettes et smartphones professionnels.
- Éviter les installations de logiciels non validés.
- Comprendre le rôle des sauvegardes.
- Adopter les bonnes pratiques concernant les documents papier et les écrans visibles.

Module 6 – Sécuriser le télétravail et la mobilité

- Utiliser une connexion sécurisée et les outils mis à disposition par l'entreprise.
- Comprendre les risques liés aux réseaux Wi-Fi publics.
- Éviter les connexions sensibles depuis un équipement partagé.
- Protéger son écran et ses conversations dans les espaces publics.
- Prévenir le vol ou la perte d'un équipement professionnel.
- Ne pas laisser un appareil professionnel sans surveillance.
- Respecter les procédures de stockage et de transfert des documents.
- Signaler immédiatement la perte ou le vol d'un équipement.

Module 7 – Réagir efficacement en cas d'incident

- Que faire après avoir cliqué sur un lien suspect ?
- Que faire après avoir ouvert une pièce jointe potentiellement malveillante ?
- Que faire après avoir communiqué un mot de passe ou une information sensible ?
- Pourquoi ne faut-il pas masquer une erreur ou attendre avant de la signaler ?
- Identifier les interlocuteurs et les canaux internes de signalement.
- Conserver les éléments utiles à l'analyse de l'incident.
- Ne pas supprimer seul les messages ou fichiers concernés sans consigne.
- Appliquer la procédure interne de gestion des incidents.
- Exercice final : traitement collectif d'un scénario de cyberattaque.

Les bonnes pratiques à retenir

- Prendre le temps de vérifier toute demande inhabituelle.
- Ne jamais communiquer ses identifiants ou ses codes de validation.
- Vérifier l'adresse réelle de l'expéditeur et l'adresse du site Internet.
- Ne pas ouvrir une pièce jointe inattendue sans confirmation.
- Utiliser des mots de passe robustes et l'authentification multifacteur.
- Mettre à jour ses équipements et logiciels.
- Respecter les règles internes de protection des données.
- Signaler immédiatement tout événement suspect.

Méthodes pédagogiques

- Alternance d'apports théoriques, d'exemples concrets et d'exercices pratiques.
- Analyse de courriels, de SMS, de pages Internet et de demandes frauduleuses.
- Études de cas inspirées de situations professionnelles.
- Quiz interactifs et échanges collectifs.
- Mises en situation permettant de développer les bons réflexes.
- Démonstrations réalisées par le formateur dans un environnement sécurisé.
- Adaptation des exemples au secteur d'activité et aux fonctions des participants.
- Remise d'un support pédagogique synthétisant les principales bonnes pratiques.

Moyens pédagogiques et techniques

- Salle de formation équipée d'un vidéoprojecteur ou d'un écran de diffusion.
- Ordinateur connecté à Internet pour le formateur.
- Supports de présentation et exemples de messages frauduleux.
- Études de cas, quiz et fiches réflexes.
- Accès à une plateforme de visioconférence lorsque la formation est organisée à distance.
- Possibilité d'utiliser des exemples anonymisés transmis par l'entreprise cliente.

Modalités d'évaluation

- Questionnaire de positionnement transmis avant la formation.
- Évaluation des connaissances initiales en début de session.
- Questions orales et exercices d'application tout au long de la journée.
- Analyse de situations professionnelles et de messages suspects.
- Quiz final de validation des acquis.
- Évaluation de la capacité à identifier une menace et à adopter la réaction appropriée.
- Questionnaire de satisfaction remis à l'issue de la formation.

Résultats attendus

- Reconnaître les signes caractéristiques d'une tentative de phishing ou de fraude.
- Réduire les comportements susceptibles de compromettre la sécurité du système d'information.
- Utiliser les outils numériques professionnels avec davantage de vigilance.
- Appliquer les bonnes pratiques de gestion des mots de passe et des accès.
- Protéger les données de l'entreprise en présentiel, à distance et en déplacement.
- Signaler rapidement une situation suspecte ou un incident.
- Contribuer à l'amélioration de la culture cybersécurité de l'organisation.

Modalités de suivi

- Feuille d'émargement signée par demi-journée.
- Suivi de la participation aux exercices et aux mises en situation.
- Remise d'une attestation individuelle de fin de formation.
- Remise d'un certificat de réalisation selon les modalités applicables.

Sanction de la formation

- Attestation individuelle de fin de formation.
- Évaluation des acquis réalisée en fin de session.
- Remise d'un support pédagogique ou d'une fiche mémo sur les bons réflexes de cybersécurité.

Modalités et délais d'accès

- Formation accessible en inter-entreprises, en intra-entreprise ou à distance.
- Inscription possible jusqu'à 48 heures avant le démarrage pour les financements directs ou relevant du plan de développement des compétences, sous réserve de disponibilité.
- Les délais peuvent être plus longs en cas de demande de financement par un OPCO, France Travail ou un autre organisme financeur.
- Un échange préalable peut être organisé afin d'identifier les besoins, le niveau des participants et les situations professionnelles à traiter.

Organisation de la formation

- Formation en présentiel dans le centre Devictio à Lyon.
- Formation en intra-entreprise dans les locaux du client partout en France.
- Possibilité d'organisation à distance en classe virtuelle.
- Programme personnalisable selon le secteur d'activité, les métiers et les procédures internes de l'organisation.

Accessibilité aux personnes en situation de handicap

- La formation est accessible aux personnes en situation de handicap, sous réserve de la compatibilité des besoins avec les modalités pédagogiques et techniques proposées.
- Une analyse des besoins spécifiques est réalisée avant l'entrée en formation afin de prévoir les adaptations nécessaires.
- Les supports, le rythme, les exercices et les modalités d'évaluation peuvent être adaptés lorsque cela est possible.
- Les participants sont invités à contacter Devictio en amont afin d'étudier les solutions d'accompagnement appropriées.

Formateur

- Formation animée par un professionnel expérimenté en cybersécurité, sécurité informatique, sensibilisation des utilisateurs ou gestion des risques numériques.
- Le formateur adapte ses exemples au niveau des participants et au contexte professionnel de l'entreprise.

NOS TARIFS

INTER dans nos locaux	1100 €* (1100 €* / jour)
INTRA dans toute la France	sur devis

* Nos formations ne sont pas soumises à la TVA

FINANCEMENT

COMMENT FINANCER **SA FORMATION ?**

IL EXISTE PLUSIEURS DISPOSITIFS DE FINANCEMENT

- Compte Personnel de Formation (CPF)
- AIF (Pôle Emploi)
- FNE-Formation
- Fonds d'assurances formations (FAF)
- Contrats cadres
- Opérateurs de compétences (OPCO)
- Plan de Développement des compétences

Devictio formations©

MAGNIS FORMATION by Devictio

PiXio by Devictio

CONTACTEZ NOUS !

04 72 64 25 19

magnis-formation.fr

pixio-formation.fr

devictio.fr

CENTRE DE FORMATION PROFESSIONNELLE

12 place Bir Hakeim - 69003 Lyon (siège)

57 rue d'Amsterdam - 75008 Paris

formation@devictio.fr

facebook.com/organisme.de.formation

fr.linkedin.com/compagny/devicto

instagram.com/devictioformations

Qualiopi processus certifié
Certification qualité délivrée au titre de la catégorie «Actions de formation»

TOSA Centre agréé

La Région Hauts-de-France H+ Formation

Google Partner

depuis 2007