

CYBERSECURITE - LES BASES

Objectifs pédagogiques

À l'issue de la formation, les participants seront capables de :

- Comprendre les enjeux de la cybersécurité pour eux-mêmes et leur entreprise.
- Identifier les principales menaces informatiques (phishing, ransomwares, fraude, ingénierie sociale).
- Adopter les bons réflexes au quotidien pour sécuriser leur poste de travail, leurs communications et leurs données.
- Prendre conscience de leur rôle et de leur responsabilité juridique dans la protection des informations.
- Mettre en place un plan d'action personnel en cybersécurité.

Méthodes pédagogiques

- Alternance de théorie, cas pratiques et mises en situation.
- Etudes de cas tirées de situation réelles.
- Matériel pédagogique : vidéoprojecteur, paperboard, documentation

Modalités d'évaluation

- Quiz et exercices pratiques tout au long de la formation.
- Auto-évaluation en fin de session

Inscription

Pour vous inscrire à cette formation, contactez-nous à contact@apoi.re ou au **06 93 87 33 53**. Nous vous accompagnerons dans le processus d'inscription.

Nos formateurs

Consultants spécialisés en cybersécurité et protection des données, expérimentés dans la sensibilisation des utilisateurs.

Modalités

La formation est accessible après une analyse des besoins réalisée avec l'employeur ou le référent. Le délai d'accès est d'au moins un mois après validation de la demande.

DURÉE : 7 heures = 1 jour de formation

VALIDITÉ : Pas de durée de validité, remise à jour régulière conseillée (menaces évolutives).

PUBLIC : Tout collaborateur utilisant des outils informatiques et connectés.

PRÉREQUIS : Aucun.

NOMBRE DE PARTICIPANTS : 10 stagiaires maximum

ACCESSIBILITE AUX PERSONNES HANDICAPEES : Lors de l'inscription, nous évaluons les adaptations nécessaires, avec l'appui de partenaires, et invitons les personnes en situation de handicap de contacter notre référent **M. BELGUENDOZ Benaouda** par mail à direction@apoi.re.

ATTESTATION : Une attestation de formation sera délivrée aux participants ayant validé les acquis et justifié de leur assiduité tout au long de la session.



CYBERSECURITE - LES BASES

Programme

1. Comprendre les enjeux et identifier les menaces

- Panorama de la cybersécurité : enjeux économiques, organisationnels et juridiques.
- Typologie des menaces : phishing, ransomwares, fraude au président, malwares, connexions Wi-Fi non sécurisées.
- Ingénierie sociale et manipulation : techniques de récupération d'informations (réseaux sociaux, contacts pro/perso).
- Étude de cas : analyse d'une attaque réelle.

2. Les bons réflexes et la protection au quotidien

- Sécuriser son poste de travail et ses accès (configuration, mises à jour, gestion des comptes).
- Messagerie et navigation Internet : reconnaître un mail piégé ou un site frauduleux.
- Gestion des mots de passe et authentification (bonnes pratiques, outils de gestion).
- Protection des données personnelles et professionnelles.
- Utilisation sécurisée des réseaux sociaux et outils collaboratifs.

