Cybersécurité : sensibilisation

Découvrir les enjeux de la cybersécurité en entreprise, les différents types de menaces et les moyens de s'en prémunir.

AUXERRE

>> Public(s) (H/F)

Tout public

>> Dates

Entrées/sorties à dates fixes
Du 06/01/2025 au 19/12/2025
Inscriptions fermées, contacter le centre

>> Durées

- Durée indicative : 1 Jour(s)
- Durée totale : 7 h (dont 7 h en centre)

Fractionnement possible en 3 sessions d'1 journée.

>> Effectif

De 6 à 12

>> Coût de la prestation

Coût total max. : 140.00 € TTC
Tarif individuel par candidat.
Un tarif global peut être proposé en cas de constitution d'un groupe suffisant par une ou plusieurs entreprises.

>> Lieu de la formation

GRETA 89
Antenne d'Auxerre - Site Fourier
44 boulevard Lyautey
89000 AUXERRE

>> Votre interlocuteur

Julien REGNAULT
Coordinateur pédagogique
Tél. : 03 86 72 03 22
julien.regnault@ac-dijon.fr

>> Organisme responsable

GRETA 89
Lycée Joseph Fourier, 44 Boulevard Lyautey, BP 80053
89010 AUXERRE
Tél. : 03 86 72 10 40
greta89.contact@ac-dijon.fr
Siret : 19890005200020
N° d'activité : 2689P000389
www.bourgogne-greta.fr

>> OBJECTIF(S)

- Comprendre les risques, les enjeux d'une cyberattaque.
- Identifier les menaces, les conséquences d'une cyberattaque.
- Identifier les mesures de protection, les bonnes pratiques et les bons réflexes.

>> PRÉREQUIS

- Sans niveau spécifique
- Aucun prérequis complémentaire

>> CONTENU

1 - Introduction
Pourquoi se sensibiliser à la SSI ?
Les notions clés à connaître
Cadre légal et réglementaire
les acteurs de la SSI et leur rôle

2 - Les menaces et vecteurs d'attaque
Le phishing / l'hameçonnage
L'usurpation d'identité
Les virus
Les arnaques au Président
Les clés USB
L'impact des réseaux sociaux

3 - Les risques
Le vol, la corruption, la suppression des données de l'entreprise, la collectivité.
La réputation de l'entreprise, la collectivité
La perte financière,
L'indisponibilité du Système d'information
Le lien avec l'ingénierie sociale, l'intelligence économique, l'espionnage industriel

4 - les bonnes pratiques
Les mots de passe :
? Un bon mot de passe doit?
? Les bonnes habitudes à adopter
? Les gestionnaires de mots de passe

Les e-mails :
? le principal vecteur d'attaque,
? cas pratiques : exemples hameçonnage
? comment reconnaître un faux mail L'arnaque la plus fréquente par email
? les bons réflexes

Les FOVI : Faux ordre de Virement dans le cadre des tentatives d'arnaques au Président : les bons réflexes
Le nomadisme, les déplacements (vol de matériel, ...)
Le WIFI
La navigation sur Internet
Le poste de travail, l'antivirus, les mises à jour ?
Le stockage et les sauvegardes (clés usb, locales, serveurs, ...)
La protection des données, l'archivage, la destruction ou recyclage
La politique de sécurité, la charte informatique

5. Conclusion
La résilience des entreprises, des collectivités, les responsabilités engagées,
Reprise des objectifs de la formation

>> MODALITÉ(S) DE FORMATION

- Formation en présentiel

- Intraentreprise
- Interentreprise
- En centre

- Pédagogie adaptée aux personnes en situation de handicap

Personnes en situation de handicap, prenez contact avec l'organisme en amont pour une étude préalable des possibilités d'adaptation des modalités en fonction de vos besoins spécifiques et particuliers.

>> MOYEN(S) ET MODALITÉ(S) PÉDAGOGIQUE(S)

Document pédagogique, Etude de cas, Travaux pratiques

>> MODALITÉ(S) D'ADMISSION ET DE RECRUTEMENT

Admission après entretien

>> ÉVALUATION ET RECONNAISSANCE(S) DES ACQUIS

Attestation de fin de formation

>> INTERVENANT(E)(S)

Formateur expert du domaine