Prévention des escroqueries et attaques numériques

Les entreprises sont des plus en plus exposées à des attaques complexes et sophistiquées mais pour lesquels, des leviers de prévention efficace existe, pour peu qu'ils soient connus, diffusés et appliqués.
A l'issue de cette formation, les personnels concernés seront capables d'identifier les risques et de réagir face à ceux-ci. La formation aborde notamment les faux ordres de virement ou fraude au président, les phishing ou hameçonnage, les ransoware ou rançongiciel et leurs variantes et risques associés : piratage de compte, faux conseiller bancaire ou faux support technique.

OBJECTIFS

- Comprendre les risques et les techniques utilisées par les escrocs
- Identifier les attaques sous leurs différentes formes
- Savoir les empêcher ou les stopper à temps.
- Maîtriser les réflexes urgent à mettre en œuvre en cas d'attaque subie.

2 décembre en distanciel

390€ *adhérent*
585€ *non adhérent*
(par personne)

1 jour

01 53 98 95 03 – formation@fehap.fr

Prérequis

- Aaucun pré-requis n'est nécessaire.

CONTENU

Les différents risques

- A travers un échange et un quizz, le formateur évalue le niveau de connaissance et de sensibilisation des stagiaires
- Ensemble nous définissons les types d'attaques qui existent

Les différents risques détaillés : les reconnaître

- Phishing ou hammeçonnage
- Ransoware ou rançongiciel
- Le faux ordres de virement

Exercices pratiques et quizz
En cas d'attaque identifiée ou suspectée, comment réagir ?

- Les réactions individuelles
- Les parades organisationnelles
- Rôles de chacun

En cas d'attaque réussie, comment réagir ?

- Le temps est un allier
- Identifier rôles internes et externes (banque, Police, ...)

Exercices pratiques et quizz

REMPLISSEZ UN BULLETIN D'INSCRIPTION EN LIGNE

PUBLICS

- Cette formation est destinée à tous les personnels ayant des fonctions les exposants à des contacts extérieurs et à des engagements de toutes natures susceptibles d'entrainer des conséquences pour l'entreprise (achats, RH, gestion des commandes, des stochs, sécurité informatique, sécurité des données, ...).

MÉTHODES PÉDAGOGIQUES ET MODALITÉS D'ÉVALUATION

Modalités pédagogiques

- Apports théoriques et méthodologiques
- Exercices, cas pratiques, étude de situations
- Quizz
- Échanges et mutualisation

Modalités d'évaluation

- grille d'auto-évaluation des acquis de la formation

INTERVENANTS

- Profil de(s) intervenant(s) : Septime Conseils et formations – François Thiriet
- Ancien officier de police judiciaire spécialise de la lutte contre la criminalité économique et financière, actuellement responsable d'un service de lutte contre la fraude dans un service en charge d'une mission de service publique et consultant pour des institutions telles que le Conseil de l'Europe, il est également formateur indépendant.