



# Formation : Prévention contre la cybercriminalité

## PUBLIC CIBLE

S'adresse à toute personne disposant d'une adresse de messagerie électronique, vecteur d'attaque principalement utilisé contre une entreprise, administration ou institution.

## MODÈLE DE FORMATION

Est dispensée à des groupes, en présentiel sur le lieu de travail ou dans une salle de formation ad hoc afin que les participants soient totalement dévolus à l'apprentissage et y adhèrent en ne la percevant pas comme un fardeau administratif supplémentaire.

## MÉTHODOLOGIE

Cette formation se veut cohérente avec la réalité et interactive, complétée par des exemples pratiques. Les parties théoriques seront clôturées par des travaux de groupe ou individuel, afin de maximiser leur impact.

## SUPPORT DE COURS

Un fascicule, édité spécialement et résumant les points essentiels sera remis à chaque participant. Il constituera par la suite un précieux aide-mémoire et guide pour une utilisation d'outils numériques en toute sécurité.

## Faites de votre personnel le maillon fort de votre plan de protection face à la cybermenace

L'usage de l'informatique s'est généralisé dans notre société. L'adoption de nouvelles technologies, facteur de productivité, de compétitivité et de croissance est devenue incontournable dans toutes les entreprises, administrations ou institutions.

En parallèle de cette formidable évolution, un nouveau risque a émergé : la cybercriminalité !

Les pirates informatiques n'ont jamais été autant actifs et ne cessent d'innover dans leurs modes opératoires. Les techniques d'ingénierie sociale sont de plus en plus sophistiquées afin de créer une confusion chez les utilisateurs, considérés par les hackers comme le maillon faible. Poussés à la faute mais aussi par méconnaissance, les usagers compromettent ainsi la protection de la structure mise en place par des moyens techniques.



Escroquerie financière, vol de données, ou sabotage, les conséquences pour une entreprise peuvent être désastreuses et pourraient impacter sa pérennité.

Une entreprise, administration ou institution doit prendre conscience qu'elle peut à tout moment être confrontée à la cybercriminalité. Devoir remédier à un incident dans l'urgence et en subir les conséquences par la suite peut s'avérer bien plus coûteux que de le prévenir. Par conséquent, se doter d'un plan de protection global face à la cybermenace devient une nécessité.

## Objectifs de la formation :

### • ÊTRE PROACTIF

Adopter les bonnes pratiques élémentaires dans l'ère numérique afin de limiter les cyber risques

### • ÊTRE À JOUR

Connaître les modus operandi des cybercriminels et les cyberphénomènes actuels

### • ÊTRE VIGILANT

Détecter une tentative d'attaque ou de tromperie par ingénierie sociale

### • ÊTRE RÉACTIF

Adopter les bonnes réactions en cas d'incident

## FORMATEUR

Ancien policier issu des services spécialisés, il possède de nombreuses années d'expérience dans la conduite opérationnelle d'engagements et dans la formation d'adultes.

## POINTS FORTS

- Thématiques approfondies, mais restant accessibles.
- Pragmatique, axée solutions.
- Facilité de mise en œuvre des actions concrètes.
- Recommandations et points importants documentés et synthétisés dans un fascicule.

## DURÉE

240 minutes (2 x 120 minutes).

## SOLUTIONS SUR MESURE

La formation est divisible en 2 modules différés (de 2 x 120 minutes chacun).

## CONDITIONS ET COÛTS

La formation est dispensée dès 6 participants. CHF 250.- par participant, ou CHF 300.- par participant pour 2 modules différés.

## CONTINUITÉ

- Sécurité dans l'ère numérique (240 minutes).
- Prévention contre l'espionnage industriel (240 minutes).

## À PROPOS

L'agence FOCUS est un centre de hautes compétences pluridisciplinaires basée à Fribourg, offrant des services d'investigation privée et de consulting en sécurité physique - sûreté pour les entreprises, administrations et institutions.

# Lorsque la cybersécurité d'une entité est bien conçue dans son ensemble, les ressources sont mises en combinaison, à la fois avec des outils techniques et des moyens humains

Fort de ce constat, notre formation « Prévention contre la cybercriminalité » met l'accent sur les connaissances des utilisateurs. En effet, les enjeux de la cybersécurité doivent être au cœur des préoccupations de tout le personnel d'une entreprise, administration ou institution.

Les participants seront guidés vers les bonnes pratiques à adopter dans l'ère numérique afin d'anticiper des problèmes de cybersécurité. Les modus operandi des cybercriminels et les phénomènes actuels de cyberattaques seront expliqués aux apprenants afin de les rendre capables de détecter une tentative d'attaque. Enfin, les bonnes réactions en cas d'attaque seront abordées afin d'en limiter les dégâts potentiels.

Les actions concrètes et les recommandations thématiques dans cette formation sont à la portée de toutes et tous, quel que soit le niveau de connaissance. Simples et pragmatiques, leurs mises en applications sont peu coûteuses, voire gratuites et pourront néanmoins fortement réduire les cyber risques.



## Thématiques traitées :

### Module 1 (120 minutes):

#### • GÉNÉRALITÉS

Internet et la cybercriminalité en bref

#### • BONNES PRATIQUES DANS L'ÈRE NUMÉRIQUE

Utilisation de mots de passe, méthodes de composition, consultation de sites Web sûrs et recommandations générales

#### • CYBERPHÉNOMÈNES ET MODUS OPERANDI 1/2

Ingénierie sociale

### Module 2 (120 minutes):

#### • CYBERPHÉNOMÈNES ET MODUS OPERANDI 2/2

Phishing, e-mails et méthodes d'analyse, Hacking, logiciels malveillants, pièces jointes et analyse, DDoS et cyber escroqueries

#### • BONNES RÉACTIONS EN CAS D'ATTAQUE

Reconnaître une cyberattaque et agir en conséquence

## DOMAINES DE COMPETENCES

- Enquêtes
- Renseignements
- Filatures
- Conseils
- Formations
- Audits

En savoir plus sur l'agence FOCUS :



# FOCUS

— Investigations & Consulting —

Avenue de Tivoli 3, Case postale 227

1701 Fribourg

+41 (0)26 566 71 72

info@investigations-consulting.ch

www.investigations-consulting.ch