Kit de survie de la Cybersécurité

Non-certifiante **Formation continue.**

Réf. : 2003838F — Mise à jour : 11 août 2025

Organisme responsable : **MWEB FORMATION**

Contenu

Objectifs

- Être sensibilisé aux menaces informatiques dans les activités professionnelles et privées
- Comprendre les problématiques liées à la sécurité informatique, Comprendre en quoi la prévention est nécessaire
- Adopter les bonnes attitudes et réflexes, Savoir mettre en œuvre des solutions concrètes

Programme

Définitions

- Sécurité Informatique, Sécurité des Systèmes d'Information, Cybersécurité et Cyberdéfense

Aspects juridiques

- RGPD, règlement intérieur, charte informatique, risques juridiques
- Les divers « hackers » (éthiques, black hat…)
- ANSSI, CNIL, Cybermalveillance…

Danger à tous les étages

- Les divers types de risques
- Exemples concrets de piratages (Pishing, Squishing, Smishing, Cybersquatting, Cheval de Troie…) et statistiques

Les causes

- Facteur humain (maladresse, malveillance…)
- Causes techniques (sinistre, usure, réseau, Internet)
- Malveillance : exemples de logiciels malveillants

La protection de l'information : mesures de prévention

- La gestion de la cybersécurité au sein d'une organisation
- Sécuriser le poste de travail
- Contrôles d'accès
- Notions de cryptographie (le chiffrement et ses contraintes

Cybersécurité : compréhension : prévention

Dans cette formation, nous abordons un point des plus importants : par de nombreux exemples, découverte ensemble comment des PERSONNES – même avec une bonne maîtrise du numérique – vont PERMETTRE à des PIRATES informatiques de pénétrer le réseau, un serveur ou les comptes mail de l'entreprise…

Dans 95 % des cas, malgré une sécurité informatique accrue, la faille sera rendue possible par un usager qui, par manque de temps ou dans une situation stressante et généralement « sous pression », va finir par « cliquer » sur le fameux PHISHING soigneusement préparé par un pirate, par exemple.

Nous aborderons la globalité de la Sécurité des Systèmes d'Information et pas uniquement les « bonnes pratiques » et les « recettes ».

Nous comprendrons comment nous pouvons TOUS être victime d’un piratage ou d’un accident si nous ne prenons pas le recul nécessaire avant d’agir.
Enfin, nous évoquerons la nécessité de mettre en place une politique de protection et de restauration des données avant d’être une victime.

Certifications préparées et métiers visés

Niveau d'entrée

Sans niveau spécifique

Métiers associés

M1801 — Administration de systèmes d'information

M1802 — Expertise et support en systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
2000235	À distance	—	31/08/2025	30/07/2026

Source : GREF Bretagne #2003838F