

Plus de 700 contenus cyber disponibles
Pour informer et sensibiliser les publics

- Kit de sensibilisation
- MOOC, e-sensibilisation
- Guides et méthodes
- Fiches pratiques / fiches réflexes
- Articles web
- Vidéos...



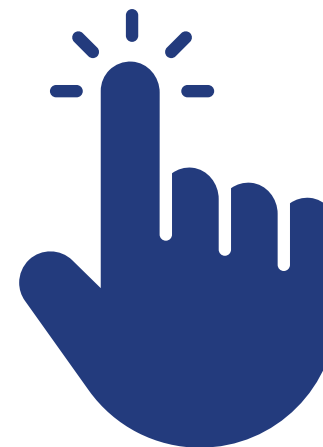
**Vous êtes victime
de cybermalveillance ?**

Ayez le bon réflexe,
rendez-vous sur

17CYBER.GOUV.FR



**LES SERVICES EN LIGNE
POUR LES
PROFESSIONNELS**



- ✓ Sensibiliser
- ✓ S'exercer
- ✓ Se sécuriser



COMPRENDRE LES MENACES ET ADOPTER LES BONNES PRATIQUES !

- **E-sensibilisation** gratuite accessible à tous : particuliers, collaborateurs des TPE/PME et agents de la fonction publique.
- Une attestation de suivi téléchargeable à l'issue des trois modules.



MODULE 1 COMPRENDRE 43 min

- Quelles menaces aujourd'hui ?
- Quels risques pour moi et mon organisation ?
- Que faire si je suis victime d'une attaque ?



MODULE 2 AGIR 33 min

- Quelles bonnes pratiques au quotidien ?
- Quels bons réflexes dans mes usages ?



MODULE 3 TRANSMETTRE 33 min

- Sensibiliser, pourquoi et comment ?
- Pour aller plus loin : acteurs nationaux et textes de référence

APPRÉHENDER LES FONDAMENTAUX DE LA GESTION DE CRISE CYBER

- **Cours en ligne** destinés aux petites et moyennes structures, publiques ou privées.
- Entièrement gratuits, ces modules didactiques sont accessibles à tous.



AVANT LA CRISE 32 min

Anticiper pour mieux se préparer

- Se connaître
- S'informer
- Se préparer



PENDANT LA CRISE 69 min

Faire preuve de résilience

- Qualifier la crise
- Gérer la crise
- Alerter
- Paroles d'experts



APRÈS LA CRISE 22 min

Capitaliser pour mieux anticiper

- Capitaliser sur la crise
- S'exercer et s'entraîner

PROTÉGER LES SYSTÈMES D'INFORMATION DE VOTRE ORGANISATION

- **Service de sécurisation** destiné au public professionnel : entreprise, association ou collectivité
- Mise en relation avec des prestataires labellisés ExpertCyber et qualifiés localisés dans votre région.

Les prestataires sont labellisés ExpertCyber à l'issue d'un audit réalisé par l'AFNOR.

Le label ExpertCyber vous garantit :

- ✓ un **niveau d'expertise** et de compétences en sécurité informatique ;
- ✓ un **conseil de qualité** pour prévenir la survenue d'actes de cybermalveillance et sécuriser leurs installations informatiques ;
- ✓ une **conformité administrative** (respect du cadre législatif et réglementaire, traitement des données personnelles conforme au RGPD...) ;
- ✓ un sens de l'**intérêt général** (veille et remontée d'incidents, conservation de la preuve numérique...).

