FFMI
FÉDÉRATION FRANÇAISE
DES MÉTIERS DE L'INCENDIE

FFMI – Cybersécurité : des dispositifs publics gratuits pour vous accompagner

Edité par « Service public – Entreprendre » le 04/11/2026 – Ministère de l'économie

Peu préparées aux cyberattaques, les TPE et PME sont particulièrement vulnérables à ces menaces en forte hausse. Vous souhaitez renforcer la cybersécurité de votre entreprise ? Vous former aux bonnes pratiques ? Vous ne savez pas vers qui vous tourner en cas d'attaque ? On vous guide en vous présentant les principaux outils et ressources existantes.

1-Vous former pour anticiper les menaces

MesServicesCyber : la plateforme publique pour vous aider à vous protéger contre les risques cyber

Lancée au printemps 2025 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), MesServicesCyber est une plateforme gratuite, 100% en ligne et accessible à tous. Cette plateforme propose un parcours de cybersécurité en ligne, pédagogique et progressif, pour aider toutes les organisations, mêmes débutantes, à agir pour leur cybersécurité. Le parcours s'articule autour de deux niveaux :

- 12 premières mesures simples et rapides à mettre en œuvre pour les organisations qui ne savent pas par où commencer, avec des explications simples et des outils pratiques pour mettre en œuvre les mesures,
- un programme cyber complet, basé sur le Référentiel Cyber France pour organisations plus matures.

Vous y retrouverez également des tests ludiques pour sensibiliser vos équipes, vos contacts cyber de proximité pour être orienté, des prestataires pour vous accompagner, les financements disponibles pour soutenir vos efforts.

Découvrir la plateforme MesServicesCyber

SensCyber, une e-sensibilisation à la cybersécurité

Cybermalveillance.gouv.fr a lancé SensCyber, une e-sensibilisation à la cybersécurité gratuite et accessible à tous.

Le programme est construit autour de trois modules, d'une durée de 25 à 45 minutes chacun :

1. comprendre les cyberattaques les plus courantes (hameçonnage, piratage de compte, rançongiciels, etc.), leur fonctionnement et les risques encourus par les individus dans la sphère privée comme professionnelle,
2. agir pour s'approprier les bonnes pratiques et les bons réflexes dans les usages du quotidien (téléphone portable, réseaux sociaux, usages pro-perso, etc.),
3. apprendre à transmettre ces connaissances et bonnes pratiques avec son entourage pour une meilleure protection collective et identifier les acteurs publics à contacter en cas d'attaques.

Démarrer l'e-sensibilisation

2-Être accompagné pour renforcer votre cybersécurité

Mon ExpertCyber : demandez une mise en relation avec des professionnels qualifiés

Mis en place par Cybermalveillance.gouv.fr, le service Mon ExpertCyber permet de mettre en relation les entreprises, et tout particulièrement les TPE-PME, avec des professionnels qualifiés pour les accompagner dans la sécurisation de leurs systèmes d'information.
Ces professionnels ont reçu le label ExpertCyber qui vous garantit un niveau de compétence et d'expertise en cybersécurité. Ils peuvent intervenir dans les domaines de l'installation, de la sécurisation, de la maintenance et de l'assistance informatique.
En fonction de la localisation et des besoins de l'entreprise, le service propose des partenaires de confiance adaptés.
Être mis en relation avec un professionnel labellisé ExpertCyber

3-Réagir en cas d'attaque

17Cyber : une assistance en ligne si vous êtes victime de malveillance informatique
Porté par la Police nationale, la Gendarmerie nationale et cybermalveillance.gouv.fr, ce service est destiné à toutes les victimes de cybermalveillance : particuliers, entreprises et collectivités.
Ce guichet unique est disponible 24h/24 et 7j/7. Il vous permet de comprendre rapidement à quel type de menace vous êtes confronté, en répondant à quelques questions en ligne, et ainsi recevoir des conseils personnalisés à votre situation.
Si besoin, vous avez également la possibilité d'être mis en contact avec un prestataire spécialisé (prestation payante) et bénéficier d'un accompagnement par tchat avec un gendarme ou un policier lorsque la menace le nécessite.
En savoir plus

Les CSIRT territoriaux, des centres de réponse aux incidents cyber au plus près des territoires
Les CSIRT territoriaux (*Computer Security Incident Response Team*) sont des centres de réponse aux incidents cyber. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité.
Au nombre de 15, ces centres portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires.
Si vous victime d'un incident de sécurité, n'hésitez pas à prendre contact avec votre CSIRT territorial.
En savoir plus