GUIDE DES BONNES PRATIQUES IT/CYBERSÉCURITÉ

SOMMAIRE

1 - SENSIBILISATION

1. **Introduction :** Pourquoi la cybersécurité concerne aussi les petites entreprises

2. **Enjeux majeurs TPE/PME** (avec témoignages)

3. **Typologie des menaces & conséquences**
   - Escroqueries courantes (phishing, faux supports, fraude au virement)
   - Malwares : virus / infostealers, rançongiciels, piratage de comptes
   - Nouveaux risques : QR codes frauduleux, espionnage mobile

4. **Décryptage des tendances :** cloud, intelligence artificielle, télétravail, évolution des métiers, rôle des prestataires IT

2 - PASSAGE À L'ACTION

1. **Bonnes pratiques de sensibilisation :** 5 conseils applicables immédiatement + 1 conseil bonus

2. **Construire la confiance :** rôle des prestataires comme partenaires stratégiques

3. **Structurer une offre adaptée :** outils pour le moyen / long terme (packs, audits, partenariats avec assureurs)

4. **Respecter la loi : le socle indispensable**
   - 8 étapes clés du RGPD
   - Réglementations sectorielles (NIS-2, DORA)
   - Argumentaire : pourquoi la conformité est incontournable

3 - FORMATION : MONTER EN COMPÉTENCES POUR RENFORCER LA SÉCURITÉ NUMÉRIQUE DE L'ENTREPRISE

1. **Les compétences clés à développer**
2. **Un financement sanctuarisé pour les TPE/PME**
3. **Les offres de formation disponibles sur la plateforme Click&Form**
4. **Pour aller plus loin : instaurer une culture "cyber" durable**

4 - OUTILS & ANNEXES

1. **Sites institutionnels de référence**
2. **Ressources de la branche et de l'Opcommerce**
3. **Autres ressources complémentaires**
4. **Contacts d'urgence et assistance**

01
SENSIBILISATION

I - INTRODUCTION : POURQUOI LA CYBERSÉCURITÉ CONCERNE AUSSI LES PETITES ENTREPRISES

En France, 99 % du tissu économique est constitué de TPE et PME (Cybersecure n°23).
Pourtant, une majorité de dirigeant·e·s continue de penser qu'elles sont "trop petites pour intéresser les hackers". Selon l'étude ImpactCyber (2024), 62 % des responsables jugent leur exposition faible.

La réalité est différente. Ces entreprises détiennent des données stratégiques (clients, factures, coordonnées bancaires), dépendent fortement de leurs outils numériques… mais disposent rarement de moyens humains ou financiers pour les protéger.

Elles deviennent donc des cibles privilégiées pour les cybercriminel.le.s.
- Une boîte mail piratée = plusieurs semaines de relations clients perdues.
- Un site bloqué = plus de commandes.
- Un rançongiciel = activité paralysée et trésorerie menacée.

Et il ne s'agit pas de science-fiction : les attaques touchent aussi bien une PME industrielle qu'une société informatique installée depuis vingt ans.

II - LES ENJEUX MAJEURS POUR LES TPE/PME

Aujourd'hui, tout passe par le numérique : messagerie, site web, ERP, logiciels de caisse, réseaux sociaux. Chaque outil est une porte d'entrée potentielle. Comme le rappelle Cybermalveillance.gouv.fr, ordinateurs, téléphones, tablettes et objets connectés "sont autant de portes d'entrée pour les cybercriminels".

Les TPE/PME sont particulièrement fragiles pour trois raisons principales :

Le facteur humain : l'hameçonnage reste la menace la plus courante en France (Rapport Cybermalveillance, 2023). Un simple clic sur un lien frauduleux ou un mot de passe trop simple peut suffire.

Des moyens limités : selon l'étude ImpactCyber (2024), 68 % des TPE/PME consacrent moins de 2 000 € par an à la cybersécurité, et 72 % n'ont aucun collaborateur dédié.

Un manque de préparation : toujours selon ImpactCyber, 70 % n'ont aucune procédure de réaction en cas d'attaque, ce qui rend la gestion de crise particulièrement difficile.

De nombreux dirigeants de TPE-PME ont témoigné de leur vulnérabilité (Étude ImpactCyber (2024)) :

"On pensait être faiblement exposés. L'attaque a révélé que nous n'avions pas les bons réflexes, ni les bonnes sauvegardes."

"La pire conséquence n'est pas technique mais client : devoir expliquer que vos données ou vos services ne sont plus disponibles."

Ces témoignages soulignent un point commun :
La plupart des dirigeant·e·s n'imaginaient pas être concerné·e·s…
Jusqu'au jour où leur entreprise a été touchée.

SELON L'ÉTUDE,

62%

DES DIRIGEANTS SOUS-ESTIMENT LEUR EXPOSITION, ALORS QU'ILS FONT PARTIE DES CIBLES PRIVILÉGIÉES DES CYBERCRIMINELS.

Ces vulnérabilités ne sont pas qu'un problème technique, elles conditionnent directement la survie de l'entreprise à d'autres niveaux :

JURIDIQUE

Une PME mal préparée peut se retrouver en infraction (RGPD, obligations contractuelles) et exposée à des sanctions.

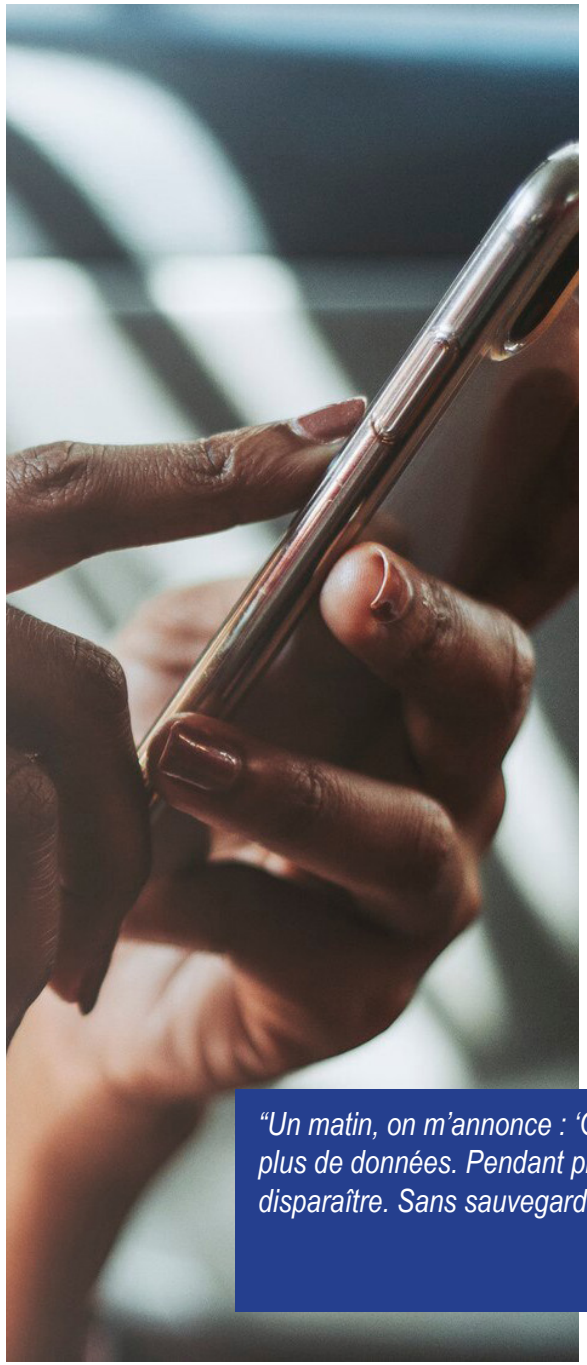
COMMERCIAL

Un incident de cybersécurité peut bloquer une commande, faire perdre un contrat ou décrédibiliser une entreprise auprès de ses partenaires.

RÉPUTATIONNEL

Une boîte mail piratée ou un site indisponible suffit à entamer la relation client. Comme le rappellent de nombreux témoignages, la perte de crédibilité est parfois plus grave que la perte financière

EN CLAIR, NÉGLIGER LA CYBERSÉCURITÉ N'EST PAS SEULEMENT UN RISQUE TECHNIQUE : C'EST UN PARI DANGEREUX POUR LA PÉRENNITÉ, LA CROISSANCE ET L'IMAGE DE L'ENTREPRISE.



III - TYPOLOGIE DES MENACES ET CONSÉQUENCES

1. Escroqueries courantes

L'hameçonnage (phishing) est la menace la plus répandue.

Un mail ou SMS imitant une banque ou un fournisseur pousse à cliquer sur un lien frauduleux.

> *"On pensait être bien protégés. Et pourtant, en octobre 2024, nous avons subi une cyberattaque. La restauration a pris quatre semaines et coûté plusieurs centaines de milliers d'euros. Psychologiquement, c'est un cataclysme."*
>
> **Patrick Désir, directeur général du Groupe Altaï (intégrateur ERP, 600 clients industriels)**

Autre technique de plus en plus fréquente : les faux supports techniques.

> *"J'ai reçu un mail de mon bailleur annonçant un changement de RIB. J'ai failli faire le virement… avant de réaliser qu'il s'agissait d'une escroquerie."*
>
> **Témoignage d'une PME locataire de ses locaux (2023)**

Un appel ou une fenêtre imite un service officiel (ex. "Microsoft") et incite à donner la main à distance. Le pirate installe alors des malwares ou extorque de l'argent.
La fraude au virement est également en plein essor. Le pirate se fait passer pour un fournisseur ou un bailleur et réclame un paiement urgent.

2. Virus, rançongiciels et piratage de comptes

Les malwares restent un classique : ils volent des identifiants, corrompent des fichiers ou ouvrent l'accès à distance.

> *"Un matin, on m'annonce : 'On ne peut plus travailler'. Plus d'accès au réseau, plus de données. Pendant plusieurs jours, j'ai cru que l'entreprise allait disparaître. Sans sauvegarde restaurée, nous aurions tout perdu."*
>
> **Nicolas Dubar, président de Saagic (fabricant de barbecues, 1 M€/an)**

Les rançongiciels (ransomwares) bloquent totalement l'activité en chiffrant les données. Les pirates réclament ensuite une rançon, sans garantie de restitution.

Enfin, le piratage de comptes (messagerie, réseaux sociaux, logiciels de gestion) permet aux attaquants d'usurper l'identité de l'entreprise et de diffuser des messages frauduleux.

3. Nouveaux risques

QR CODES FRAUDULEUX

Un QR code collé sur un menu de restaurant ou une affiche peut sembler anodin. Mais une fois scanné, il redirige vers un site piégé qui vole vos identifiants ou installe un virus sur votre téléphone.

Ce risque en hausse est signalé dans Cybersecure n° 22 (juillet–septembre 2024).

ESPIONNAGE DES APPAREILS MOBILES

Les smartphones et tablettes contiennent désormais plus d'informations sensibles qu'un ordinateur (mails, contacts, accès bancaires). Or ils sont souvent moins protégés : pas de mises à jour, applis téléchargées sans vérification, absence de chiffrement.

Le Kit de sensibilisation Cybermalveillance (2022) rappelle que les appareils mobiles sont devenus des cibles privilégiées car ils servent à la fois à un usage personnel et professionnel.

SABOTAGE ET ESPIONNAGE CIBLÉ

Certaines attaques visent non pas à voler de l'argent directement, mais à perturber un service (attaque par déni de service) ou à espionner une entreprise.

L'ANSSI indique que ces méthodes, autrefois réservées aux grands groupes, touchent désormais aussi les PME, notamment dans le cadre de sous-traitances sensibles (Panorama de la cybermenace 2024, ANSSI, cyber.gouv.fr).

LE "SHADOW IT" OU "SHADOW IA"

Cela désigne l'utilisation d'outils numériques non validés par l'entreprise (par exemple, un salarié qui utilise son compte personnel Dropbox ou ChatGPT pour traiter des données clients).

Risque : perte de contrôle sur les données, fuites accidentelles, non-conformité RGPD.

4. Décryptage des tendances

TENDANCE	OPPORTUNITÉ	RISQUE	EXEMPLE CONCRET + SOURCE
CLOUD	Flexibilité, réduction des coûts d'infrastructure, accès facilité aux outils	Dépendance aux prestataires, exposition internationale : une faille chez le fournisseur impacte directement l'entreprise.	En 2021, une panne mondiale de Microsoft Azure a bloqué des milliers d'entreprises plusieurs heures. (Étude Impact IT & cybersécurité, 2024 ; ANSSI – Panorama de la cybermenace 2024)
INTELLIGENCE ARTIFICIELLE	Détection automatisée des menaces, alertes en temps réel, protections avancées intégrées dans certains logiciels.	Utilisation par les pirates pour générer des attaques crédibles (phishing sur mesure, deepfakes, malwares adaptatifs).	Des escroqueries vocales imitant la voix de dirigeant.e.s ont déjà piégé des entreprises. (Étude Impact IT & cybersécurité, 2024 ; Cybersecure n°22, 2024)
TÉLÉTRAVAIL ET OBJETS CONNECTÉS	Organisation plus flexible, productivité accrue, automatisation des tâches via IoT.	Multiplication des points d'entrée vulnérables : Wi-Fi domestique, ordinateurs personnels, objets mal sécurisés.	Des pirates ont pris le contrôle de trottinettes électriques à distance via une faille logicielle. (Cybersecure n°23, 2024 ; Kit Cybermalveillance, 2022)

ÉVOLUTION DES MÉTIERS ET RÔLE DES PRESTATAIRES IT

Face à cette complexité croissante, les TPE/PME ne peuvent pas toujours tout gérer seules.

Les prestataires IT évoluent donc vers un rôle de partenaires stratégiques : diagnostics, formations, solutions adaptées.

De plus en plus d'entreprises comprennent qu'intégrer la cybersécurité dans leur gouvernance (désigner un référent, former leurs équipes, s'appuyer sur des prestataires de confiance) n'est plus un choix, mais une nécessité.

C'est le point de départ pour passer à l'action.

02
PASSAGE À L'ACTION

I - BONNES PRATIQUES DE SENSIBILISATION : 5 CONSEILS APPLICABLES IMMÉDIATEMENT + 1 CONSEIL BONUS

La cybersécurité repose d'abord sur des réflexes simples, faciles à appliquer.
Voici six mesures concrètes pour toute TPE/PME.

UTILISER DES MOTS DE PASSE ROBUSTES ET UNIQUES

Un mot de passe faible ou réutilisé est une invitation pour les pirates.

Outils concrets :

- ***Gestionnaires de mots de passe*** *(Keeper, KeePass, Bitwarden, Dashlane) : ils génèrent et stockent automatiquement vos identifiants. Résultat : vous n'avez plus qu'un seul mot de passe maître à retenir.*
- ***Outils de transmission sécurisée*** *comme Onetimesecret.com : pratique pour partager un mot de passe avec un collaborateur ou un prestataire. Le lien s'autodétruit après lecture, évitant qu'il circule par mail.*
- ***Outils de vérification*** *comme HaveIBeenPwned.com : en entrant une adresse e-mail, vous pouvez savoir si elle a déjà été compromise lors d'une fuite de données. Un bon réflexe pour tester la robustesse de vos pratiques.*

ACTIVER LA DOUBLE AUTHENTIFICATION (2FA)

Même le meilleur mot de passe peut être compromis. La double authentification ajoute une barrière indispensable.

Outils concrets :
Google Authenticator ou Microsoft Authenticator (applis gratuites).

SAUVEGARDER RÉGULIÈREMENT LES DONNÉES : APPLIQUEZ LA RÈGLE DU 3-2-1

Une panne, un vol ou un rançongiciel peut détruire vos fichiers. Seule une sauvegarde indépendante permet de redémarrer.

La règle du 3-2-1 :
- *Conservez **3 copies** de vos données,*
- *Sur **2 supports** différents (ex. Disque externe + cloud),*
- *Avec **1 copie** déconnectée (hors ligne ou hors site).*

Outils concrets :
- ***Disques externes chiffrés :** solution simple et peu coûteuse.*
- ***Solutions cloud sécurisées** (Nextcloud, Tresorit, pCloud Business…) : stockage en ligne avec chiffrement.*
- ***Planification :** sauvegarde automatique quotidienne + test de restauration une fois par mois pour vérifier qu'elle fonctionne vraiment.*

METTRE À JOUR SES LOGICIELS ET ÉQUIPEMENTS : NE LAISSEZ PAS DE PORTES OUVERTES

Chaque mise à jour corrige des failles de sécurité déjà connues des pirates. Reporter une mise à jour, c'est comme laisser une porte entrouverte : tôt ou tard, quelqu'un finira par entrer.

Outils concrets :
***Activer les mises à jour automatiques** sur Windows, macOS, Android et iOS.*

*Pour les PME avec plusieurs postes : **utiliser des outils d'inventaire et de gestion des correctifs** (GLPI, WSUS, Spiceworks...).*

Voir avec le service informatique.

***Ne pas oublier les objets connectés** (imprimantes, caméras, routeurs, box internet) : eux aussi contiennent des logiciels à mettre à jour régulièrement.*

SENSIBILISER LES ÉQUIPES AUX ARNAQUES : LE RÉFLEXE HUMAIN AVANT TOUT

Dans 8 cas sur 10, c'est un.e employé.e qui ouvre la porte aux pirates, sans le vouloir : un clic sur un mail piégé, un RIB validé dans l'urgence, un mot de passe communiqué à un faux support technique.

Règle simple :
"Si un message crée de l'urgence ou de la peur, méfiez-vous : c'est peut-être une arnaque."

Outils concrets :

- *MOOC ANSSI "Sensibilisation à la cybersécurité" (gratuit, en ligne) : un cours simple et accessible pour toute l'équipe : https://secnumacademie.gouv.fr/*
- *Kits Cybermalveillance.gouv.fr : affiches, vidéos, fiches réflexes pour animer des ateliers internes sans expertise technique.*
- *Exercices pratiques : simuler des attaques (ex. Envoi de faux mails de phishing) pour tester et renforcer les réflexes des collaborateurs.*

RECOMMANDATION BONUS :

ENCADRER L'USAGE DE L'INTELLIGENCE ARTIFICIELLE (ÉVITER LE "SHADOW AI")

De plus en plus de collaborateurs utilisent des outils d'IA générative (ChatGPT, Copilot, Gemini, etc.) pour gagner du temps. Mais copier-coller un devis, une base clients ou un document interne dans ces outils peut provoquer une fuite de données sensibles.

Règle simple :
"Ce que vous ne publieriez pas sur Internet, ne le mettez pas dans une IA en ligne."

Mesures concrètes :

- *Établir une charte interne définissant ce qui peut ou non être saisi dans une IA.*
- *Former les équipes aux bons réflexes, notamment sur la confidentialité des données.*
- *Privilégier des IA sécurisées, hébergées en Europe ou proposées par des prestataires respectant le RGPD*
- *Surveiller les usages avec l'appui de l'IT ou du prestataire, pour éviter le recours à des outils non validés ("Shadow IT").*

II - STRUCTURER UNE OFFRE ADAPTÉE : PENSER MOYEN ET LONG TERME

Les gestes immédiats (mots de passe, sauvegardes, mises à jour) sont essentiels, mais ils ne suffisent pas. Pour réduire durablement les risques, les TPE/PME doivent envisager des solutions structurées, qui permettent de monter progressivement en maturité sans devoir internaliser toutes les compétences.

LA BOÎTE À OUTILS CYBER

De nombreux prestataires proposent des "boîtes à outils" adaptées aux petites structures. Ces offres incluent généralement :

- Un antivirus professionnel (plus efficace que les versions gratuites grand public),
- Une sauvegarde automatique sécurisée,
- Une supervision à distance des postes et serveurs (alerte en cas de problème).

Avantage : un coût forfaitaire maîtrisé et une solution "clé en main". Pour une TPE, cela équivaut à externaliser sa sécurité de base sans avoir à gérer chaque paramètre technique.

CONSTRUIRE UNE FEUILLE DE ROUTE CYBER

Au-delà des solutions techniques, il s'agit d'intégrer la cybersécurité dans la stratégie de l'entreprise :

- Désigner un référent cyber (même si ce n'est pas son métier principal).
- Former régulièrement les équipes avec des modules courts et concrets.
- Mettre à jour un plan de réaction en cas d'incident (qui appeler, quoi faire en premier, comment informer ses clients).

Avantage : une PME qui a une vision claire et progressive sera plus résiliente face aux attaques et plus crédible auprès de ses clients et **partenaires.**

LES AUDITS DE SÉCURITÉ

Un audit de cybersécurité est une photographie du niveau de protection de l'entreprise à un instant donné. Il permet de répondre à des questions simples :

- Nos mots de passe sont-ils robustes ?
- Nos sauvegardes sont-elles fiables et testées ?
- Nos postes et logiciels sont-ils à jour ?
- Nos accès distants (télétravail, prestataires) sont-ils sécurisés ?

Avantage : l'audit débouche sur des recommandations concrètes, hiérarchisées par ordre de priorité. Une PME peut ainsi planifier ses actions sur 6, 12 ou 24 mois, en fonction de ses moyens.
Exemple d'audit pour débuter : *mon aide cyber sur https://monaide.cyber.gouv.fr/*

LES PARTENARIATS AVEC LES ASSUREURS

De plus en plus d'assureurs proposent des offres "cyber". Celles-ci exigent souvent de respecter un minimum de bonnes pratiques (sauvegardes, antivirus, mise à jour). En échange, elles couvrent certains coûts en cas d'attaque (interruption d'activité, assistance juridique, restauration des données).

Avantage : l'assurance peut être un levier de mise en conformité. Elle incite l'entreprise à adopter un socle de protection et offre un filet de sécurité financier en cas d'incident.

III - RESPECTER LA LOI : LE SOCLE INDISPENSABLE (RGPD, NIS-2, DORA)

La première étape des bonnes pratiques en IT/cybersécurité est de respecter les obligations légales. C'est le socle sur lequel tout le reste se construit : une entreprise non conforme s'expose à des amendes, mais aussi à une perte de confiance de ses clients et partenaires.

RGPD : LE SOCLE COMMUN POUR TOUTES LES ENTREPRISES

Une réglementation connue mais parfois mal comprise s'applique à toutes les entreprises : le RGPD (Règlement Général sur la Protection des Données). Toute entreprise qui manipule des données personnelles (clients, prospects, RH, etc.) doit s'y conformer.

La mise en conformité complète peut nécessiter un travail interne ou l'appui d'un spécialiste, mais ses grandes lignes tiennent en 8 points clés :

• Désigner un DPO (délégué à la protection des données) lorsque c'est requis, ou à minima un référent.
• Recenser vos fichiers et données personnelles traitées en tant que responsable de traitement : en profiter pour faire le tri, expliciter la finalité et fixer une durée de conservation.
• Identifier vos sous-traitants et, le cas échéant, les clients pour lesquels vous êtes vous-même sous-traitant.

• Tenir un registre des traitements (côté responsable de traitement).
• Publier une politique de confidentialité (site web / communication client), distincte des mentions légales et conforme à vos pratiques réelles.
• Tenir un registre spécifique lorsque vous agissez en tant que sous-traitant (registre des opérations de traitement).
• Encadrer contractuellement les rôles et obligations responsable/sous-traitant (clauses RGPD côté client et côté prestataire).
• Sécuriser les accès et les systèmes (postes, réseau, serveurs, sauvegardes) à un niveau proportionné aux risques.

LES RÉGLEMENTATIONS SECTORIELLES : NIS-2 ET DORA

NIS-2
C'est une directive européenne qui impose des règles de cybersécurité renforcées à certains secteurs jugés "critiques" (banque, énergie, santé, transports, administrations, etc.).

Concrètement : si votre entreprise IT travaille pour un client dans l'un de ces secteurs, il peut vous demander de respecter certaines obligations de sécurité dans vos contrats (sauvegardes, plans de réaction, procédures documentées).

DORA
C'est un règlement européen qui vise spécifiquement les acteurs du secteur financier (banques, assurances, gestionnaires d'actifs).

Concrètement : si vous êtes prestataire informatique de ces acteurs, vous devrez respecter leurs exigences en matière de continuité de service, de tests de sécurité ou de gestion des incidents.

POURQUOI LA CONFORMITÉ EST INCONTOURNABLE

En résumé : si vos clients appartiennent à des secteurs critiques ou financiers, vos contrats et vos pratiques devront être alignés avec leurs obligations.

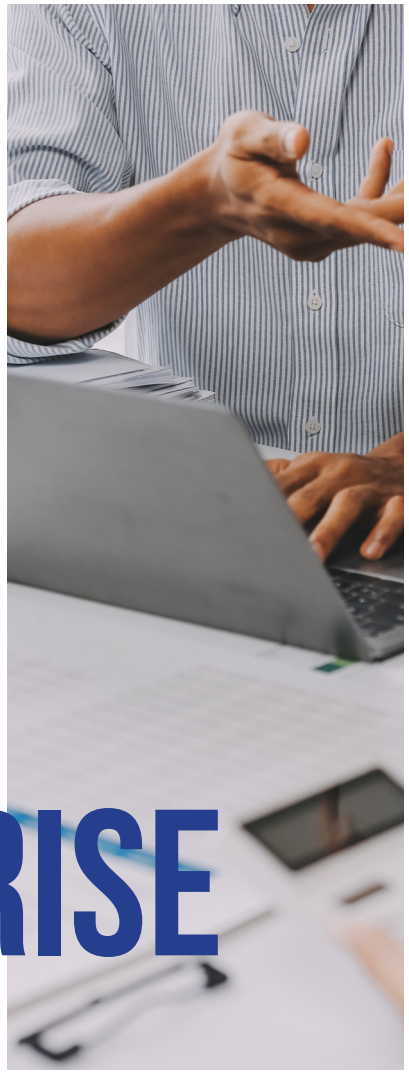
Dans le cas contraire, vous risquez non seulement de perdre le marché, mais aussi de fragiliser votre image.

La conformité ne se résume pas à "éviter une sanction":

- **C'est une exigence juridique:** le RGPD prévoit des amendes pouvant atteindre plusieurs millions d'euros.
- **C'est un atout commercial:** de plus en plus d'appels d'offres, même de PME ou de collectivités locales, exigent désormais des garanties de conformité.
- **C'est une question de confiance :** une entreprise qui démontre qu'elle protège correctement les données inspire davantage de crédibilité à ses clients, partenaires et investisseurs.

AUTREMENT DIT : LA CONFORMITÉ RÉGLEMENTAIRE N'EST PAS SEULEMENT UNE CONTRAINTE, C'EST AUSSI UN LEVIER DE COMPÉTITIVITÉ ET UN GAGE DE PROFESSIONNALISME.

03
FORMATION : MONTER EN COMPÉTENCES POUR RENFORCER LA SÉCURITÉ NUMÉRIQUE DE L'ENTREPRISE



Passer à l'action, c'est aussi faire évoluer les compétences.
La cybersécurité ne dépend pas uniquement des outils : elle repose avant tout sur la connaissance et les réflexes de celles et ceux qui les utilisent au quotidien.
La branche des entreprises du bureau et du numérique, avec l'appui de l'Opcommerce, a fait de la formation un levier prioritaire pour accompagner les TPE et PME dans cette montée en maturité.

I - LES COMPÉTENCES CLÉS À DÉVELOPPER

La cybersécurité doit s'ancrer à tous les niveaux de l'entreprise.
Chaque rôle, dirigeant·e, référent·e ou collaborateur·rice a un rôle spécifique à jouer.

PUBLICS CONCERNÉS	OBJECTIFS	EXEMPLES DE COMPÉTENCES À DÉVELOPPER
DIRIGEANT·E / RESPONSABLE	Piloter la stratégie de sécurité numérique de l'entreprise	Comprendre les risques majeurs, évaluer le niveau de protection, définir un plan d'action dans la durée et choisir les bons prestataires.
RÉFÉRENT·E / ENCADRANT·E	Mettre en œuvre et suivre les mesures de sécurité	Identifier les vulnérabilités, gérer les accès, organiser les sauvegardes et la sensibilisation de l'équipe. Anticiper la gestion de crise et de la continuité de l'activité
COLLABORATEUR·RICE	Adopter les bons réflexes au quotidien	Reconnaître les tentatives de phishing, sécuriser ses mots de passe, appliquer les mises à jour, protéger ses données et ses appareils.

Ces compétences s'articulent sur trois niveaux de progression :

NIVEAU 1

Sensibilisation : comprendre les menaces et les risques et adopter les bonnes pratiques.

NIVEAU 2

Opérationnel : savoir détecter, prévenir et réagir face à un incident.

NIVEAU 3

Avancé : maîtriser les infrastructures et piloter la sécurité dans la durée.

OBJECTIF : QUE CHAQUE ENTREPRISE, QUELLE QUE SOIT SA TAILLE, DISPOSE D'AU MOINS UNE PERSONNE "RÉFÉRENT.E CYBER" FORMÉE ET CAPABLE D'AGIR EN CAS D'INCIDENT.

II - UN FINANCEMENT SANCTUARISÉ POUR LES TPE/PME (IMPORTANT)

Consciente que la cybersécurité représente un investissement, la branche a choisi de sanctuariser un budget dédié à la formation.

Le catalogue Click&Form (la sélection de votre Branche), dans la limite d'un nombre d'inscriptions par an et par entreprise pour les formations métiers sélectionnées et prises en charge directement sur ce budget dédié.
Ce dispositif permet aux petites structures d'accéder à des formations concrètes et immédiatement applicables, sans contrainte administrative lourde.

Les entreprises de moins de 50 salarié·e·s bénéficient d'une prise en charge spécifique dans le cadre du **Plan de développement des compétences** pour une/des formation(s) de leurs choix. Il s'agit d'un plafond annuel qui couvre tout ou partie du coût de la formation.
Les critères de prise en charge sont sur votre espace adhérent.

III - LES OFFRES DE FORMATION DISPONIBLES SUR LA PLATEFORME CLICK&FORM (DISPONIBLE SUR VOTRE ESPACE ADHÉRENT)

Cette plateforme en ligne, développée par l'Opcommerce, propose des modules courts et interactifs adaptés aux besoins des TPE et PME.
Les formations peuvent être suivies en distanciel, mixte ou en présentiel, selon les thématiques.

Exemples de parcours proposés par la branche :

- Cybersécurité : niveau débutant : comprendre les risques numériques et adopter les bons réflexes.
- Cybersécurité : niveau avancé : approfondir la gestion des risques et piloter la sécurité de l'entreprise.
- Sensibilisation à la RGPD : comprendre comment se mettre en conformité

Ces modules peuvent être complétés par d'autres formations thématiques (protection des données, gestion de crise, objets connectés, etc.), en fonction des besoins identifiés avec le conseiller formation de l'Opcommerce.

IV - POUR ALLER PLUS LOIN : INSTAURER UNE CULTURE “CYBER” DURABLE

Former ne doit pas être un événement ponctuel, mais un processus continu.

Quelques bonnes pratiques pour ancrer durablement la cybersécurité dans la culture de l’entreprise :

- **Former régulièrement les équipes :** un rappel annuel ou semestriel suffit souvent à maintenir la vigilance.
- **Capitaliser sur les outils gratuits :** le kit de sensibilisation de Cybermalveillance.gouv.fr (affiches, quiz, vidéos) ou le MOOC de l’ANSSI peuvent compléter les parcours internes.
- **Valoriser le rôle du référent cyber :** le/la référent·e devient le point de contact pour centraliser les alertes et diffuser les bonnes pratiques.
- **Faire de la cybersécurité un réflexe de management :** intégrer la sécurité dans les réunions d’équipe, les achats informatiques, les projets clients.

EN SOMME, FORMER, C’EST PRÉVENIR. UNE ENTREPRISE OÙ CHACUN.E COMPREND LES RISQUES ET SAIT COMMENT RÉAGIR EST UNE ENTREPRISE PLUS RÉSILIENTE, PLUS CRÉDIBLE ET PLUS COMPÉTITIVE.
GRÂCE À L’APPUI DE L’OPCOMMERCE, LES TPE/PME DISPOSENT DÉSORMAIS DE TOUS LES LEVIERS NÉCESSAIRES POUR DÉVELOPPER CES COMPÉTENCES, À LEUR RYTHME ET SELON LEURS MOYENS.

04
OUTILS & ANNEXES

Retrouvez ici les ressources, contacts et outils officiels pour approfondir votre démarche de cybersécurité.

SITES INSTITUTIONNELS DE RÉFÉRENCE

ANSSI (Agence nationale de la sécurité des systèmes d'information)
Le site de référence de l'État pour la cybersécurité : guides, alertes, outils d'évaluation et MOOC SecNumAcadémie.
https://cyber.gouv.fr

Cybermalveillance.gouv.fr
Dispositif national d'assistance aux victimes d'actes de cybermalveillance : fiches pratiques, kits de sensibilisation, vidéos, quiz.
https://www.cybermalveillance.gouv.fr

MonAideCyber.gouv.fr
Plateforme gratuite d'auto-diagnostic et de mise en relation avec des prestataires de confiance agréés par l'État.
https://monaide.cyber.gouv.fr

CNIL (Commission nationale de l'informatique et des libertés)
Conseils pratiques pour protéger les données personnelles et respecter le RGPD.
https://www.cnil.fr

RESSOURCES DE LA BRANCHE ET DE L'OPCOMMERCE

Étude "Impact de l'IT et de la cybersécurité" (2024)
Réalisée par l'Opcommerce et la branche, cette étude met en lumière les enjeux et besoins en formation des TPE/PME du secteur.
(Lien à fournir)

Plateforme Click&Form – L'Opcommerce
Formations en ligne sur la cybersécurité, la protection des données et les usages numériques.
https://www.lopcommerce.com

Fédération EBEN
Accompagnement des entreprises du bureau et du numérique : actualités, dossiers juridiques, initiatives autour de la cybersécurité et de la conformité.
https://www.federation-eben.com

Motion Design cybersécurité
Outil de sensibilisation visuel à la cybersécurité, destiné à favoriser la prise de conscience et les bonnes pratiques au sein des entreprises.

AUTRES RESSOURCES COMPLÉMENTAIRES

CyberÉdu
Programme de sensibilisation destiné aux enseignants et formateurs à la cybersécurité.

France Num
Portail gouvernemental d'accompagnement à la transformation numérique des TPE/PME.
https://www.francenum.gouv.fr

MOOC SecNumAcadémie (ANSSI)
Formation gratuite et certifiante à la sécurité numérique.
https://secnumacademie.gouv.fr

Le glossaire cyber de l'ANSSI
Dictionnaire en ligne des termes et concepts de la cybersécurité.
https://cyber.gouv.fr/le-cyberdico

Le mémento cybersécurité de la CPME
Guide pratique pour les dirigeant.e.s de TPE/PME.
https://www.cpme.fr/publications/guides/memento-cybersecurite

CONTACTS D'URGENCE ET ASSISTANCE

CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI)
Point de contact national 24h/24 pour incidents cyber.
Email : cert-fr@ssi.gouv.fr
Téléphone (France) : 3218 ou 09 70 83 32 18
Depuis l'étranger : +33 9 70 83 32 18
https://www.cert.ssi.gouv.fr

17 Cyber
Numéro national d'urgence pour incidents et menaces cyber (accessible 24h/24).
Idéal en cas d'urgence.

Signal Spam
Plateforme de signalement des spams et tentatives d'hameçonnage.
https://www.signal-spam.fr

l'opcommerce
Opérateur de compétences

Document conçu en partenariat avec

LA BRANCHE DES ENTREPRISES DU BUREAU ET DU NUMÉRIQUE