



**PRÉFET  
DE LA RÉGION  
PAYS DE LA LOIRE**

*Liberté  
Égalité  
Fraternité*



**MINISTÈRE  
DE L'ÉCONOMIE,  
DES FINANCES  
ET DE L'INDUSTRIE**

*Liberté  
Égalité  
Fraternité*

# Sécurité numérique et sécurité économique

**Ninog KERVELLA** – Déléguée à l'information stratégique et à la sécurité économique (DREETS PdL)

**Daphné PRIOUZEAU** – Chargée de mission cybersécurité et IA (DREETS PdL)

ninog.kervella@dreets.gouv.fr – daphne.priouzeau@dreets.gouv.fr



**PRÉFET  
DE LA RÉGION  
PAYS DE LA LOIRE**

*Liberté  
Égalité  
Fraternité*



**MINISTÈRE  
DE L'ÉCONOMIE,  
DES FINANCES  
ET DE L'INDUSTRIE**

*Liberté  
Égalité  
Fraternité*

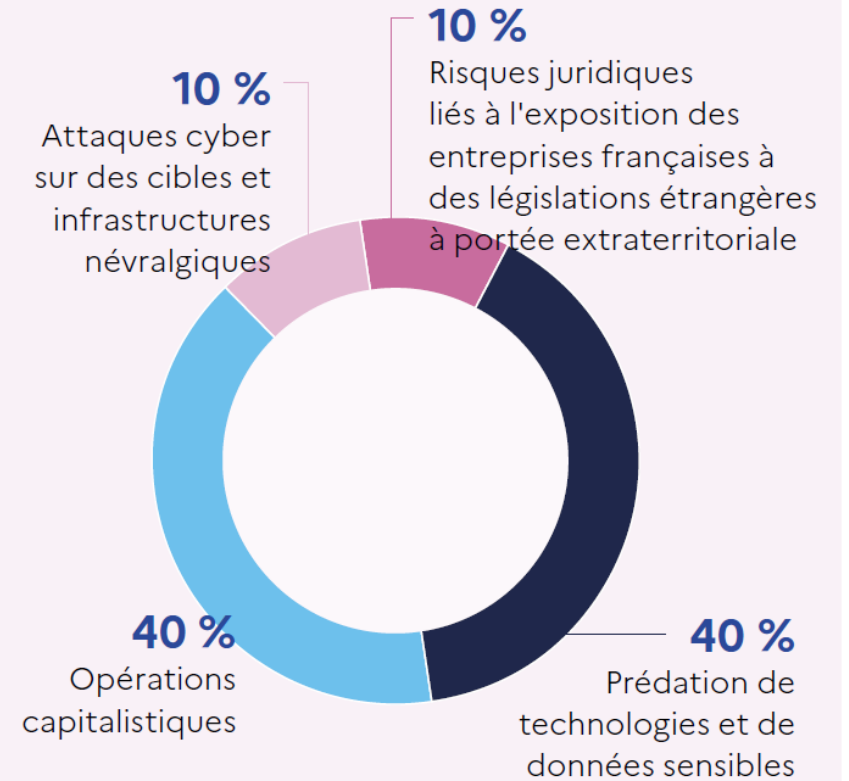
# Pourquoi se protéger ?

# Etat de la menace

## Au niveau national :

- ✓ Tendances générales de course à l'armement économique et de hausse conséquente du risque cyber ;
- ✓ Cybercriminalité (ransomware, phishing, fraudes par ingénierie sociale...);
- ✓ Risque d'espionnage industriel et de fuites de données;
- ✓ Impact financier, activité et réputation de l'entreprise.

## Menaces détectées par la plateforme interministérielle de sécurité économique





**PRÉFET  
DE LA RÉGION  
PAYS DE LA LOIRE**

*Liberté  
Égalité  
Fraternité*



**MINISTÈRE  
DE L'ÉCONOMIE,  
DES FINANCES  
ET DE L'INDUSTRIE**

*Liberté  
Égalité  
Fraternité*

# Comment se protéger ?

# 10 mesures essentielles Cybermalveillance.gouv.fr



## LES 10 MESURES ESSENTIELLES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE



Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? Voici 10 bonnes pratiques essentielles à adopter pour assurer votre sécurité numérique.

ADOPTER LES BONNES PRATIQUES

### 1 PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité.

### 3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS (PC, TABLETTES, TÉLÉPHONES...), DÈS QU'ELLES VOUS SONT PROPOSÉES

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner (mises à jour).

### 4 UTILISEZ UN ANTIVIRUS

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

### 5 TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple: Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streamings illégaux) qui pourraient également installer un virus sur vos matériels.

### 2 SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages...). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.



EN PARTENARIAT AVEC:  
MINISTÈRE DE L'INTÉRIEUR  
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

### 6 MÉFIEZ-VOUS DES MESSAGES INATTENDUS

En cas de réception d'un message inattendu ou alarmiste par messagerie (e-mail), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (phishing) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

### 7 VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

### 8 MAÎTRISEZ VOS RÉSEAUX SOCIAUX

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez

l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (fake news).

### 9 SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « clouds »... Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles (usages personnels et professionnels).

### 10 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WIFI publics. Ces réseaux WIFI sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire...). Si vous n'avez d'autre choix que d'utiliser un WIFI public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)



Licence Ouverte v2.0 (ATALAR)

# Bonnes pratiques

- La maturité cyber est une brique essentielle d'une stratégie de sécurité économique :
  - Prévention du risque de fraude et de fuite de données stratégiques;
  - Mise en place de **bonnes pratiques** partagées au sein de l'entreprise (verrouillage écran, pas de partage des droits administrateurs, sauvegardes et mises à jour régulières, organisation du télétravail...);
  - Sensibiliser et former ses collaborateurs;
  - Assurance cyber, plan de reprise d'activité;
  - Ressources de base : Documentation de l'ANSSI, [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr).



# Dispositifs d'accompagnement

- **Aides financières**
  - Pays de la Loire Conseil - Région
  - Pays de la Loire Investissement Numérique - Région
  - PASS PI - INPI
  - Cyber PME – BPI France
  
- **Dispositifs de diagnostic et d'audit subventionnés**
  - Mon Aide Cyber – ANSSI
  - Di@gonal – Gendarmerie
  - Pays de la Loire Cyber Diagnostic – Région
  - Digipilote - CCI
  - Cyber PME – BPI France
  
- **Dispositif d'assistance en cas d'attaque**
  - Pays de la Loire Cyber Assistance





**PRÉFET  
DE LA RÉGION  
PAYS DE LA LOIRE**

*Liberté  
Égalité  
Fraternité*



**MINISTÈRE  
DE L'ÉCONOMIE,  
DES FINANCES  
ET DE L'INDUSTRIE**

*Liberté  
Égalité  
Fraternité*

# Elargir la réflexion



# Déploiement d'une stratégie globale d'intelligence économique

- Sécurisation des installations physiques et numériques ;
- Identification des données sensibles et protocole de sécurisation ;
- **Maîtrise des risques** propres à son modèle économique mais également **anticipation des opportunités** (ruptures techno, mutations de l'environnement concurrentiel ou normatif...) notamment par une veille stratégique ;
- Structuration de la gouvernance et mise en place de procédures internes ;
- Sensibilisation des personnels aux exigences de discrétion, dans le cadre professionnel (salons...) comme personnel (loisirs, transport, réseaux sociaux...) ;
- Encourager les rappports d'étonnement et le signalement de tout fait inhabituel, avec des interlocuteurs internes dédiés ;

# DIAGSECO - Auto-diagnostic de sécurité économique

Diagseco est un outil d'autodiagnostic de sécurité économique mis à disposition des entreprises par la Direction générale des Entreprises (DGE). Il permet d'évaluer vos forces et faiblesses en matière de sécurité économique, et vous offre des recommandations adaptées en quelques minutes.



## Résumé des rubriques du questionnaire

1 - Capitaux et financement de l'entreprise

2 - Perte, vol ou captation d'informations stratégiques

3 - Propriété intellectuelle et compétences des salariés

4 - Système d'information et protection contre les cyberattaques

5 - Procédure de conformité

6 - Veille économique

7 - Rupture d'approvisionnement

8 - Réputation et image de l'entreprise

9 - Protection des locaux et des biens



## Résultats synthétiques

[→ Voir les résultats avancés](#)

Résultat global



Capitaux et financement de l'entreprise



Procédure de conformité



Système d'information et protection contre les cyberattaques



Propriété intellectuelle et compétences des salariés



Perte, vol ou captation d'informations stratégiques



Protection des locaux et des biens



Veille économique



Rupture d'approvisionnement



Réputation et image de l'entreprise



Très vulnérable

Vulnérable

Peu vulnérable

### 1 - Capitaux et financement de l'entreprise

### 2 - Procédure de conformité

### 3 - Système d'information et protection contre les cyberattaques

### 4 - Propriété intellectuelle et compétences des salariés

### 5 - Perte, vol ou captation d'informations stratégiques

### 6 - Protection des locaux et des biens

### 7 - Veille économique

### 8 - Rupture d'approvisionnement

### 9 - Réputation et image de l'entreprise

## 1 - Capitaux et financement de l'entreprise

**▲ Le score obtenu est de 2,5 sur 10**

→ Bilan des questions qui montrent une faiblesse d'organisation

Question	Votre réponse
Quelle est la structure de votre capital ?	Très dispersée
Des investisseurs étrangers sont-ils présents au capital de votre entreprise ?	Oui
Souhaitez-vous réaliser une levée de fonds pour vous développer ?	Oui
Connaissez-vous la réglementation des investissements étrangers en France ?	Non
Avez-vous un client représentant plus de 25 % de votre chiffre d'affaires ?	Oui
Disposez-vous des capacités d'investiguer sur votre éventuel futur partenaire ?	Non

→ **Conseils pour améliorer sa protection**

[Sécuriser son recours aux modes de financements extérieurs](#)

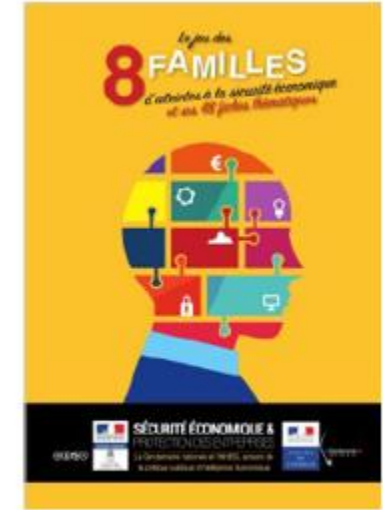
[Utiliser la procédure de contrôle des investissements étrangers en France](#)

[Mener une politique de sécurité économique au sein de l'entreprise](#)

[Solutions de financements de la BPI France](#)

# Ressources documentaires

- **Guides de bonnes pratiques**
  - La sécurité économique au quotidien en 28 fiches (site du SISSE)
  - Le jeu des 8 familles d'atteintes à la sécurité économique (Gendarmerie, IHEMI)
- **Flashs mensuels ingérence DGSI**
- **Guide d'identification des données sensibles (AFEP – MEDEF)**
- **Guides de l'AFA – politiques de conformité**
- **Guides de l'ANSSI**



Contre-espionnage  
**Conseils aux entreprises : Flash  
ingérence**



# Dispositifs d'accompagnement

## ➤ Cyber PME

- Faire monter en compétences les PME et ETI en matière de cybersécurité au travers d'une approche de bout en bout qui va du diagnostic à l'implémentation d'un plan d'action, y compris l'achat de solutions
- Un dispositif en 2 phases :
- Phase A – Un diagnostic de l'entreprise permettant d'évaluer son niveau de maturité en matière de cybersécurité. Ce diagnostic inclue la définition d'une stratégie cyber et d'un plan d'action, dit de sécurisation. Il est réalisé par un prestataire mandaté par BPI
- Phase B – Un accompagnement de l'entreprise dans la mise en œuvre du plan de sécurisation incluant le financement partiel de solutions type produits et services cybersécurité en réponse aux recommandations prioritaires qui auront été identifiées dans le plan de sécurisation élaboré.

# Dispositifs d'accompagnement

## ➤ Mon Aide Cyber

- MonAideCyber s'adresse aux entités publiques et privées, quel que soit leur taille, déjà sensibilisées au risque et souhaitant s'engager dans une première démarche proportionnée et concrète de renforcement de leur cybersécurité.
- MonAideCyber met en relation les entités de faible maturité cyber avec des « Aidants » qui réalisent des diagnostics cyber de premier niveau et qui les aiguillent vers les dispositifs complémentaires existants.
- Le diagnostic est gratuit et oriente sur 6 mesures de sécurité prioritaires à mener sur les 6 prochains mois.
- Pour en savoir plus : <https://www.monaidecyber.ssi.gouv.fr/>

# PAYS DE LA LOIRE CONSEIL

## VOLET NUMÉRISATION : CONSEIL/ACCOMPAGNEMENT

### Le dispositif en bref...



Faciliter le recours par les **Petites et Moyennes Entreprises** (- de 250 salariés et - de 50M€ de CA) aux **services de conseils extérieurs**.

9 volets thématiques dont :

- ✓ Transition numérique :
  - Audit et définition d'un cahier des charges en vue d'acquérir une solution numérique
  - Etude pour faire évoluer le système d'information
  - Etude pour valider la faisabilité technique et la pertinence économique d'un projet de réalité virtuelle
  - Etude dans une démarche relative au "numérique responsable".
- ✓ Cybersécurité :
  - Analyse des risques,
  - Audit de la maturité en matière de sécurité informatique et définition d'un plan d'actions.



Soutien régional sous forme de **subvention** à hauteur de **30% du montant HT** des coûts éligibles.

*Minimum 5 000 € HT et aide plafonnée à 15 000 €.*



[numerique@paysdelaloire.fr](mailto:numerique@paysdelaloire.fr)

En savoir + :


<https://www.paysdelaloire.fr/conseil>



# PAYS DE LA LOIRE INVESTISSEMENT NUMÉRIQUE

## VOLET INVESTISSEMENT

### Le dispositif en bref...

 Soutenir les **Petites Entreprises** (- de 50 salariés et - de 10M€ de CA) dans l'acquisition de **solutions numériques immatérielles** à forte valeur ajoutée :

- ✓ Progiciels (*ex : ERP, CRM, EBP, CAO, ...*).
- ✓ Logiciels/applications métier sur-mesure (*répondant à un besoin spécifique non couvert par les progiciels génériques*).
- ✓ Logiciels de sécurité informatique s'inscrivant dans une démarche de cybersécurité (*ex : logiciels VPN, EDR, anti-phishing, de protection de messagerie, de gestion de mots de passe, ... hors antivirus « classiques », pare-feu*)



Soutien régional sous forme de **subvention** à hauteur de **30% du montant HT** des coûts éligibles.  
*Minimum 5 000 € HT et aide plafonnée à 15 000 €.*



**Bonification** du soutien régional à hauteur de **40%** pour l'acquisition de **solutions numériques immatérielles** développées dans une démarche d'éco-conception.



[numerique@paysdelaloire.fr](mailto:numerique@paysdelaloire.fr)

En savoir + :

<https://www.paysdelaloire.fr/les-aides/pays-de-la-loire-investissement-numerique>

# PAYS DE LA LOIRE CYBER DIAGNOSTIC NOUVEAU DISPOSITIF SORTI EN MARS 2024



## Le dispositif en bref...



Soutenir les **Petites et Moyennes Entreprises** (- de 250 salariés et - de 50M€ de CA) face aux risques cyber en les accompagnant dans la **réalisation d'un diagnostic pour évaluer leur niveau de maturité en cybersécurité** et **définir un plan d'actions de sécurisation de leur SI** (Système d'Information).



Prise en charge à hauteur de **30 % du coût de la prestation** (financement : 21% FEDER  et 9% Région  ).

## Une solution innovante « clé en main » :

- **Attribution par la Région du prestataire en charge du diagnostic** (sélectionné en amont via un accord-cadre), en fonction de la zone géographique de l'entreprise.
- Durée moyenne du diagnostic : **1,5 jour** (dont 1 journée sur site).
- Livrables :
  - **Compte-rendu du diagnostic** : état des lieux et failles de sécurité identifiées.
  - **Rapport de préconisations de solutions techniques et d'outils organisationnels à mettre en place en priorité**, dans le cadre d'un plan d'actions efficaces pour protéger l'entreprise des menaces externes et internes.



[numerique@paysdelaloire.fr](mailto:numerique@paysdelaloire.fr)

En savoir + : [Pays de la Loire Cyber Diagnostic](#)

# MODALITÉS DU SOUTIEN RÉGIONAL ET EUROPÉEN

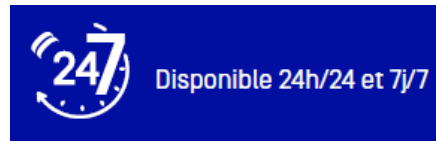
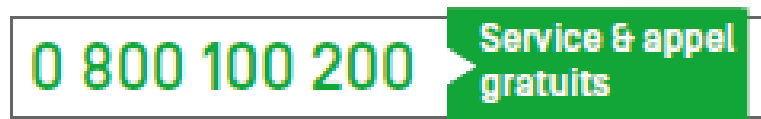



Prestation	Coût (HT)	Prise en charge Région (HT)	Prise en charge FEDER (HT)	Reste à charge	Taux de subvention
Diagnostic réalisé dans les départements de la Mayenne et du Maine et Loire par NIJI	1 000 €	90 €	210 €	<b>700 €</b>	30 %
Diagnostic réalisé dans les départements de la Sarthe et de la Loire Atlantique par KOESIO OUEST	1 320 €	118,80 €	277,20 €	<b>924 €</b>	30 %
Diagnostic réalisé dans le département de la Vendée par ORNISEC	1 125 €	101,25 €	236,25 €	<b>787,50 €</b>	30 %

# PAYS DE LA LOIRE CYBER ASSISTANCE

Dispositif gratuit de réponse à incident de sécurité (réactif) et de mise en relation.

- Plateforme téléphonique d'appel de signalement d'incidents informatiques :



- Qualification et triage des incidents.
- Suivi des incidents.
- Mise en relation avec des prestataires labellisés «  »
- Pour la communauté cyber, « PDL Cyber Assistance » constitue le Centre de Réponse à Incidents de Sécurité de la région (CSIRT régional).



En savoir + :

<https://www.paysdelaloire.fr/economie-et-innovation/entreprise/mon-organisation-subit-une-cyberattaque>

0 800 100 200

PAYS DE LA LOIRE  
**CYBER ASSISTANCE**

cyberassistance@paysdelaloire.fr

**Votre allié**  
en cas de  
cyberattaque



Soutenu  
par





# Contacts utiles

**Ninog KERVELLA** – Déléguée à l'information stratégique et à la sécurité économique (DREETS PdL) [ninog.kervella@dreets.gouv.fr](mailto:ninog.kervella@dreets.gouv.fr)

**Daphné PRIOUZEAU** – Chargée de mission cybersécurité et IA (DREETS PdL)

– [daphne.priouzeau@dreets.gouv.fr](mailto:daphne.priouzeau@dreets.gouv.fr)

**Elise LENORMAND-JEANNIN** - Chargée de programme transition numérique des entreprises (Région) [elise.lenormand@paysdelaloire.fr](mailto:elise.lenormand@paysdelaloire.fr)



PRÉFET  
DE LA RÉGION  
PAYS DE LA LOIRE

Liberté  
Égalité  
Fraternité

Direction régionale  
de l'économie, de l'emploi,  
du travail et des solidarités

