ENTREPRENDRE DANS L'OUEST
2 & 3 NOVEMBRE RENNES | PARC EXPO

RENNES - PARC EXPO
www.entreprendre-ouest.fr
#EDO

Cybersécurité
Protégez votre entreprise des menaces numériques





Animé par :
Gwenc'hlan LE BRECH et Emmanuel LE MOUELLIC, Brocéliande Digital

Vos intervenants

BROCÉLIANDE Digital

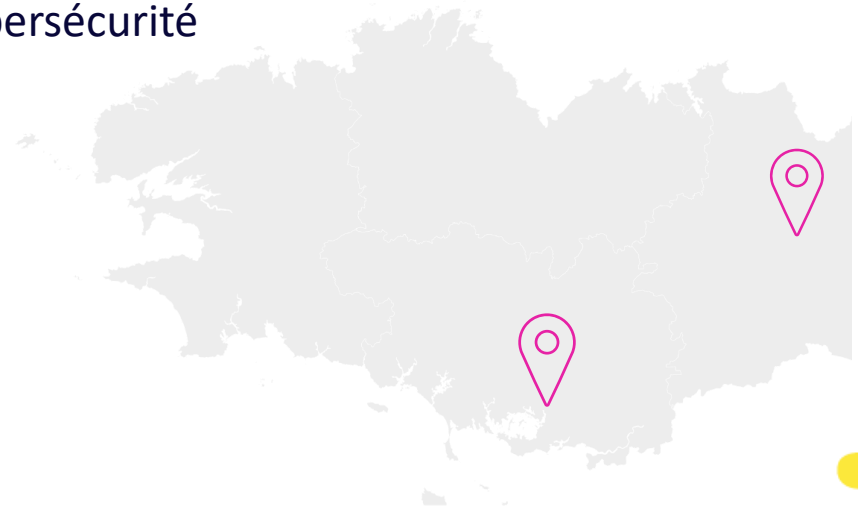


EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Nous sommes labellisés Expert Cyber,
une reconnaissance attestant de notre expertise en cybersécurité.

Emmanuel LE MOUËLLIC
Technico-Commercial

Gwenc'hlan LE BRECH
Conseiller en cybersécurité



Pourquoi parler de cybersécurité ?

Les TPE et PME sont des cibles privilégiées

Moins protégées

Les petites entreprises ont souvent moins de protections que les grandes. Les pirates le savent.

Des attaques en masse

Personne ne vous vise « vous » : des robots envoient des milliers de pièges chaque jour, automatiquement.

Un vrai coût

Activité à l'arrêt, données perdues, virement détourné : une seule attaque peut coûter des milliers d'euros.

Bonne nouvelle : quelques réflexes simples suffisent à éviter la grande majorité des attaques.

5 réflexes à adopter

Réflexe 1

L'antivirus

Le gardien de vos ordinateurs

Réflexe 2

Les mots de passe

La clé de votre maison numérique

Réflexe 3

Les mises à jour

Refermer les fenêtres

Réflexe 4

La sauvegarde

Votre parachute

Réflexe 5

La boîte mail

Repérer les arnaques

Et pour finir : comment aller plus loin.

1. L'antivirus

Le gardien de vos ordinateurs

L'image à retenir

C'est l'alarme de la maison : elle repère l'intrus et prévient tout de suite quelqu'un capable d'intervenir.

Un antivirus professionnel sur chaque poste

Ordinateurs fixes et portables, sans exception.

Infogéré : l'alerte arrive chez votre prestataire

Vous n'êtes pas seul à surveiller : un expert est prévenu et agit.

Ne jamais le désactiver

Il bloque un logiciel ou semble « ralentir » ? On appelle plutôt que de le couper.

Vécu chez nos clients

Un virus caché dans le navigateur, sans antivirus : 2 h d'intervention, environ 200 € HT, et des jours de lenteurs.

Cas concret : le virus caché dans le navigateur

Vécu chez nos clients · Réflexe 1, l'antivirus

Ce qui s'est passé

Chrome ouvre des pages non demandées et une extension inconnue revient après chaque suppression. L'origine : un logiciel gratuit installé avec un autre téléchargement.

Ce que nous avons fait

Nettoyage en profondeur du poste : réglages cachés, extension forcée, logiciel responsable. Sans réinstallation ni perte de données.

Ce qui aurait tout changé

Un antivirus pro infogéré : le logiciel douteux est bloqué dès l'installation et l'alerte arrive chez le prestataire.

Le bilan

≈ 200 € HT

d'intervention, soit 2 h de technicien

Des jours

de lenteurs et de redirections

À retenir : un clic malheureux, ça arrive à tout le monde. L'antivirus professionnel est le garde-fou qui l'arrête avant les dégâts.

2. Le mot de passe

La clé de votre maison numérique

À éviter

NomEntreprise56

Nom de l'entreprise + département : c'est la première chose que les robots essaient.

La phrase de passe

hélicoptère-rigolo-famille-transport25

Longue, facile à retenir, très difficile à deviner. La longueur compte autant que la complexité.

Un mot de passe différent
pour chaque compte

Un gestionnaire
pour tous les retenir à votre place

La double authentification
un code en plus sur le téléphone

Vécu chez nos clients

Mot de passe « nom de l'entreprise + 56 » : boîte mail piratée depuis l'étranger, tentative de virement de 1 500 € bloquée à temps.

Cas concret : la boîte mail piratée depuis l'étranger

Vécu chez nos clients · Réflexe 2, les mots de passe

Ce qui s'est passé

Mot de passe de la messagerie : nom de l'entreprise + 56. Un pirate s'y connecte depuis l'étranger et lit les e-mails, sans que rien ne se voie.

Ce que le pirate a tenté

Depuis la vraie adresse du client, une demande de virement de 1 500 € vers un faux RIB. La demande inhabituelle éveille les soupçons : alerte avant paiement.

Ce que nous avons fait

Nouveau mot de passe long et unique, double authentification activée, vérification des règles de transfert cachées.

Le bilan

≈ 1 800 €

de préjudice évité (virement et intervention)

5 min

pour activer la double authentification

À retenir : jamais le nom de l'entreprise dans un mot de passe. Et la double authentification sur toute messagerie professionnelle.

3. Les mises à jour

Refermer les fenêtres avant les cambrioleurs

Une faille est découverte
dans Windows, un logiciel ou le navigateur

L'éditeur publie le correctif
c'est la mise à jour

Les robots cherchent les retardataires
les PC pas à jour sont attaqués en priorité

Mettre à jour dans la journée	Windows, logiciels, navigateur, téléphone : dès que c'est proposé.
Redémarrer quand c'est demandé	Beaucoup de mises à jour ne s'appliquent qu'au redémarrage.
Remplacer le matériel trop ancien	**Windows** 10 ne reçoit plus de correctifs de sécurité depuis octobre 2025.

Cas concret : WannaCry, la faille qui avait déjà son correctif

Dans l'actu · Réflexe 3, les mises à jour

Mars 2017 : le correctif est publié

Microsoft corrige une faille grave de Windows. Il suffit d'installer la mise à jour pour être protégé.

Mai 2017 : le robot attaque

Un rançongiciel (un virus qui bloque les fichiers et réclame une rançon) se propage tout seul d'ordinateur en ordinateur, via cette faille.

Seuls les retardataires tombent

Hôpitaux britanniques, usines Renault à l'arrêt en France… Les ordinateurs à jour, eux, n'ont rien eu.

Le bilan

2 mois

entre le correctif et l'attaque

200 000+

ordinateurs touchés dans 150 pays

À retenir : la mise à jour était disponible depuis deux mois. Installée dans la journée, elle refermait la fenêtre.

4. La sauvegarde

Votre parachute en cas de pépin

3

copies de vos données

l'original + 2 sauvegardes

2

supports différents

par exemple un disque et le cloud

1

copie hors de l'entreprise

à l'abri d'un vol, d'un incendie ou d'un virus

La question à se poser

« Si je perds tout ce soir, qu'est-ce que je récupère demain matin ? »

Et surtout : tester la restauration. Une sauvegarde qu'on n'a jamais essayé de récupérer ne rassure personne.

Vécu chez nos clients

PC d'un paysagiste hors service : grâce à la sauvegarde de son logiciel de facturation, reprise en 48 h, aucune facture perdue.

Cas concret : le PC du paysagiste ne redémarre plus

Vécu chez nos clients · Réflexe 4, la sauvegarde

Ce qui s'est passé

Un matin, écran noir définitif. Dans l'ordinateur : devis, factures et fichier clients, tout le logiciel de facturation.

Ce qui a tout changé

Une sauvegarde du logiciel de facturation, conservée en dehors de l'ordinateur en panne.

Ce que nous avons fait

Nouveau PC, réinstallation du logiciel, restauration de la sauvegarde : clients, devis et factures, tout est revenu.

Le bilan

48 h

pour refacturer normalement

0

facture ou fiche client perdue

À retenir : la machine se remplace, les données non. Une panne, ce n'est pas une question de « si », mais de « quand ».

5. La boîte mail

La porte d'entrée n°1 des arnaques

L'adresse réelle de l'expéditeur
un « fournisseur » qui écrit depuis une adresse Gmail

Les fautes et tournures bizarres
un ton inhabituel, un logo approximatif

L'urgence
« à régler avant ce soir », « dernier rappel »

La demande inhabituelle
nouveau RIB, carte cadeau, identifiants

Le bon réflexe

Au moindre doute, on ne clique pas : on vérifie par un autre canal, en appelant au numéro habituel.

Vécu chez nos clients

Facture de 7 000 € d'un « fournisseur », envoyée depuis une adresse Gmail avec un nouveau RIB : un simple appel a évité la perte.

Cas concret : la facture à 7 000 € au faux RIB

Vécu chez nos clients · Réflexe 5, la boîte mail

Ce qui s'est passé

Une facture de 7 000 € de son fournisseur habituel : bon nom affiché, présentation soignée, et un RIB pour le règlement.

Le détail qui cloche

La vraie adresse d'expédition : une adresse Gmail anonyme. Nom usurpé, facture modifiée, RIB falsifié.

Le bon réflexe

Elle ne paie pas et nous alerte. Notre analyse : messagerie non piratée, fraude détectée avant tout paiement.

Le bilan

7 000 €

de virement frauduleux évité

2 min

de vérification ont suffi

À retenir : un nouveau RIB reçu par e-mail = un appel au numéro habituel, jamais à celui indiqué dans le mail.

Faux RIB : qui paie mal paie deux fois

Cour de cassation, 17 juin 2026

Payer la bonne facture sur le compte d'un escroc, ce n'est pas payer.

Même de bonne foi, l'entreprise piégée doit régler une seconde fois son vrai fournisseur.

- Un changement de RIB ne se traite jamais par e-mail seul
- On appelle le fournisseur au numéro déjà connu, pas celui du mail
- On forme la personne qui fait les virements

À retenir : un e-mail avec un nouveau RIB = un appel de vérification. Deux minutes au téléphone contre une facture payée deux fois.

Les 5 réflexes à retenir

À afficher près de votre bureau

1. Un antivirus professionnel, surveillé par un expert
2. Une phrase de passe différente par compte, et la double authentification
3. Les mises à jour, dans la journée
4. Une sauvegarde 3-2-1, et une restauration testée
5. Un doute sur un mail ? On vérifie par un autre canal

A vous de jouer !

Quiz · Question 1/5

Le fichier clients de votre entreprise a fuité. Combien de temps avez-vous pour prévenir la CNIL ?

A 24 heures

B Aucune obligation pour une TPE

C 72 heures après en avoir pris connaissance

D 15 jours

Réponse

La bonne réponse : C

A 24 heures

B Aucune obligation pour une TPE

✓ 72 heures après en avoir pris connaissance

D 15 jours

Pourquoi ? Le RGPD impose de notifier la CNIL dans les 72 h après avoir pris connaissance d'une violation de données personnelles, sauf si elle ne présente pas de risque pour les personnes. La taille de l'entreprise ne change rien. Si le risque est élevé, il faut aussi prévenir les personnes concernées.

A vous de jouer !

Quiz · Question 2/5

Parmi ces méthodes de double authentification, laquelle est la plus facile à contourner pour un pirate ?

A Elles se valent toutes

B Une application d'authentification sur le téléphone

C Une clé de sécurité physique (USB)

D Le code reçu par SMS

Réponse

La bonne réponse : D

A Elles se valent toutes

B Une application d'authentification sur le téléphone

C Une clé de sécurité physique (USB)

✓ Le code reçu par SMS

Pourquoi ? Le SMS peut être intercepté, notamment par un « SIM swapping » : le pirate fait transférer votre numéro sur sa carte SIM. Il peut aussi être obtenu via une fausse page de connexion. Le SMS reste bien mieux que rien, mais une application ou une clé physique est plus robuste.

A vous de jouer !

Quiz · Question 3/5

En cas de violation grave du RGPD, quelle amende maximale une entreprise risque-t-elle ?

A 50 000 €

B 1 500 €

C 1 % du chiffre d'affaires

D 20 M€ ou 4 % du CA mondial, le montant le plus élevé étant retenu

Réponse

La bonne réponse : D

A 50 000 €

B 1 500 €

C 1 % du chiffre d'affaires

✓ 20 M€ ou 4 % du CA mondial, le montant le plus élevé étant retenu

Pourquoi ? C'est le plafond prévu par le RGPD. Pour une TPE, l'amende est proportionnée, mais la CNIL sanctionne aussi les petites structures, surtout pour un défaut de sécurité des données ou une fuite non déclarée.

A vous de jouer !

Quiz · Question 4/5

Vous travaillez depuis le wifi gratuit d'un café ou d'une gare. Comment protéger vos connexions professionnelles ?

A. Aucun risque si le wifi demande un mot de passe

B. Passer par un VPN, ou par le partage de connexion de votre téléphone

C. Utiliser la navigation privée

D. Choisir le réseau qui a le meilleur signal

Réponse

La bonne réponse : B

A Aucun risque si le wifi demande un mot de passe

✓ Passer par un VPN, ou par le partage de connexion de votre téléphone

C Utiliser la navigation privée

D Choisir le réseau qui a le meilleur signal

Pourquoi ? Sur un wifi public, n'importe qui peut créer un faux point d'accès au nom du café et observer ou détourner votre trafic. Un VPN chiffre tout ce qui sort de votre poste ; le partage de connexion 4G/5G évite le réseau public. La navigation privée efface seulement l'historique de votre ordinateur : elle ne protège rien sur le réseau.

A vous de jouer !

Quiz · Question 5/5

Un salarié trouve sur le parking de l'entreprise une clé USB marquée « RH – Salaires 2026 ». Que doit-il faire ?

A. La brancher pour retrouver à qui elle appartient

B. La brancher sur un vieux PC non connecté au réseau, par prudence

C. Ne pas la brancher et la remettre au responsable informatique

D. La brancher : l'antivirus la bloquera si elle est piégée

Réponse

La bonne réponse : C

A La brancher pour retrouver à qui elle appartient

B La brancher sur un vieux PC non connecté au réseau, par prudence

✓ Ne pas la brancher et la remettre au responsable informatique

D La brancher : l'antivirus la bloquera si elle est piégée

Pourquoi ? C'est un appât classique : l'étiquette est là pour attiser la curiosité. Une clé piégée peut se faire passer pour un clavier et taper des commandes en quelques secondes, sans que l'antivirus ne réagisse. On ne la branche nulle part, même sur un vieux PC : on la remet au responsable informatique ou au prestataire.

La plus grande faiblesse d'une entreprise, c'est le facteur humain : la curiosité, l'urgence, la confiance.

Et pour aller plus loin ?

Faites le point avec nos experts cyber

Un point sur votre situation
postes, sauvegardes, messagerie, mots de passe

Compléter votre protection
antivirus professionnel, sauvegarde, accès sécurisés

Testez-vous

audit.install-cyber.fr

ENTREPRENDRE DANS L'OUEST

2 & 3 NOVEMBRE RENNES | PARC EXPO





MERCI DE VOTRE ATTENTION

Retrouvez cette présentation

sur notre site internet

www.entreprendre-ouest.fr

> Réagissez sur nos réseaux sociaux #EDO2026