🧰 Boîte à outils Cybersécurité

Les gestes qui sauvent pour les pros du Tourisme du Cantal

PME · TPE · HÉBERGEURS · COMMERCES

CCI CANTAL
1er ACCÉLÉRATEUR DES ENTREPRISES

Pourquoi vous êtes concernés

Les TPE/PME du tourisme : des cibles privilégiées

Les cybercriminels ciblent de plus en plus les petites et moyennes structures, souvent considérées comme **moins bien préparées** que les grandes entreprises. Pourtant, vos établissements traitent quotidiennement des données hautement sensibles :

- Pièces d'identité et passeports de vos clients
- Adresses postales et coordonnées personnelles
- Numéros de carte bancaire et modes de paiement
- Systèmes de réservation et fichiers clients

La cybersécurité n'est plus une option réservée aux grandes entreprises — c'est un **enjeu stratégique pour la pérennité de votre activité**.

Le saviez-vous ?

40 % des victimes de rançongiciels en France sont des PME et ETI.

80 % des intrusions informatiques commencent par un simple e-mail.

Une cyberattaque coûte en moyenne **plusieurs dizaines de milliers d'euros** à une petite structure — sans compter la perte de confiance des clients.

🧠 Quiz : Évaluez votre maturité cybersécurité

Sous-titre : 5 questions pour faire le point sur vos pratiques numériques

Quel mot de passe utilisez-vous pour votre plateforme de réservation (Airbnb, Booking...) ?

- a) Le même que pour mes e-mails personnels
- b) Un mot de passe simple facile à retenir
- c) Un mot de passe unique de 12 caractères minimum

Votre logement dispose d'un Wi-Fi pour les voyageurs. Comment est-il configuré ?

- a) C'est le même réseau que celui que j'utilise pour gérer mes réservations
- b) J'ai créé un réseau "invité" séparé pour les voyageurs
- c) Je n'ai pas de Wi-Fi dans mon logement

Vous recevez un e-mail de Booking.com vous demandant de "vérifier votre compte" en urgence. Que faites-vous ?

- a) Je clique sur le lien et je saisis mes identifiants
- b) Je vérifie l'adresse e-mail de l'expéditeur et je me connecte directement sur le site officiel
- c) Je transfère l'e-mail à un ami pour qu'il vérifie

Où conservez-vous les documents de vos voyageurs (copies de pièces d'identité, contrats...) ?

- a) Sur mon ordinateur personnel, sans sauvegarde
- b) Sur une clé USB que je prête parfois
- c) Sur un disque externe dédié, sauvegardé régulièrement et débranché après usage

Quand avez-vous mis à jour votre ordinateur ou smartphone pour la dernière fois ?

- a) Je ne sais pas, je repousse toujours les mises à jour
- b) Il y a plusieurs mois
- c) Récemment — j'active les mises à jour automatiques

✅ Corrigé du quiz

5 questions pour faire le point sur vos pratiques numériques

Mots de passe plateformes de réservation

c) Un mot de passe unique de 12 caractères minimum

Chaque plateforme (Airbnb, Booking…) doit avoir un mot de passe unique et robuste. Un gestionnaire gratuit comme KeePass vous évite de tout mémoriser.

Wi-Fi pour les voyageurs

b) J'ai créé un réseau "invité" séparé pour les voyageurs

Un réseau invité isolé empêche vos voyageurs d'accéder à vos données professionnelles et personnelles. À configurer dans les paramètres de votre box internet.

E-mail suspect de Booking.com

b) Je vérifie l'adresse e-mail de l'expéditeur et je me connecte directement sur le site officiel

Les plateformes ne demandent jamais vos identifiants par e-mail. Connectez-vous toujours directement via votre navigateur, jamais via un lien reçu par e-mail.

Conservation des documents voyageurs

c) Sur un disque externe dédié, sauvegardé régulièrement et débranché après usage

Les données de vos voyageurs sont sensibles (RGPD). Une sauvegarde déconnectée vous protège en cas de panne ou d'attaque par rançongiciel.

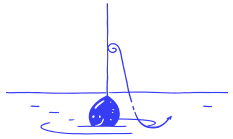
Mises à jour

c) Récemment — j'active les mises à jour automatiques

Les mises à jour corrigent des failles de sécurité critiques. Les activer automatiquement est le geste le plus simple et le plus efficace pour se protéger.

ⓘ 📊 Résultats : 4-5 bonnes réponses → Vous êtes bien protégé, continuez ! | 2-3 bonnes réponses → Quelques ajustements simples s'imposent. | 0-1 bonne réponse → Pas de panique ! Ce webinaire est fait pour vous. Consultez cybermalveillance.gouv.fr

Les 4 principales menaces qui vous ciblent



🎣 Hameçonnage (Phishing)

Un faux e-mail se faisant passer pour votre banque, un fournisseur ou une plateforme de réservation. Son objectif : voler vos mots de passe ou données bancaires. **Plus de 80 % des intrusions commencent par un e-mail.**

🔒 Rançongiciel (Ransomware)

Un virus bloque et chiffre tous vos fichiers clients et votre système de réservation. Une rançon est exigée pour les récupérer — sans aucune garantie. **40 % des victimes en France sont des PME.**

🎧 Faux Conseiller Bancaire

Un escroc se présente comme votre conseiller bancaire et crée un sentiment d'urgence pour vous faire valider des virements ou opérations frauduleuses par téléphone.

💻 Faux Support Technique

Votre écran est bloqué avec un numéro d'urgence à appeler. L'escroc prétend réparer votre ordinateur à distance pour vous extorquer de l'argent ou accéder à vos données.

Les 5 gestes qui sauvent au quotidien

Sécuriser votre établissement ne demande pas d'être un expert en informatique. Il s'agit simplement d'adopter **5 réflexes fondamentaux**, accessibles à tous, qui réduisent drastiquement votre exposition aux risques.

Ces cinq piliers forment le socle de votre protection numérique. Chacun est simple à mettre en place et peut faire la différence en cas d'attaque.

Les 5 gestes en détail

🔑 1. Mots de passe en béton

Minimum **12 caractères**, uniques pour chaque service. Utilisez un gestionnaire gratuit et certifié comme **KeePass** pour ne retenir qu'un seul mot de passe maître.

🔄 2. Mises à jour immédiates

Chaque mise à jour corrige des failles de sécurité connues. Activez les **mises à jour automatiques** sur tous vos appareils : ordinateurs, smartphones, logiciels de réservation.

💾 3. Sauvegardes déconnectées

Copiez régulièrement vos données sur un disque externe, puis **débranchez-le**. C'est votre seule véritable bouée de sauvetage en cas de rançongiciel.

🔒 4. Sécurisation du Wi-Fi de l'établissement

Changez le mot de passe par défaut du routeur, créez un **réseau Wi-Fi invité séparé** pour les clients, distinct du réseau professionnel, et **ne partagez jamais le mot de passe du réseau pro**.

🚫 5. Séparation Pro / Perso

Ne mélangez jamais vos usages professionnels et personnels. Un virus attrapé via une messagerie personnelle peut infecter tout le réseau de votre établissement. **Pas de clés USB personnelles non plus.**

Ressources gratuites

🎁 Votre kit de sensibilisation offert par l'État

Cybermalveillance.gouv.fr est la plateforme gouvernementale officielle d'assistance et de prévention. Elle met à disposition un kit de sensibilisation **entièrement gratuit et libre de droits**, conçu pour les professionnels comme pour leurs équipes.

Ce kit contient :

- Des mémos pratiques à afficher en salle de pause
- 8 vidéos explicatives claires et accessibles
- Des bandes dessinées pédagogiques
- Des quiz de sensibilisation pour vos collaborateurs
- Des fiches pratiques thématiques téléchargeables

Trouver un expert de confiance

Le service **MonExpertCyber** vous met en relation avec des prestataires informatiques **audités et labellisés par l'État** pour leurs compétences en cybersécurité.

Fini les doutes sur la fiabilité de votre prestataire : chaque professionnel référencé a été évalué sur des critères stricts de compétence et d'éthique.

👉 **monexpertcyber.fr**

🚨 Fiche Réflexe : Que faire si on a cliqué ?

Malgré toutes les précautions, l'erreur est humaine. En cas d'incident, **les premières minutes sont décisives**. Suivez ces 4 étapes dans l'ordre, sans panique.

🔌 1. Déconnecter

Coupez immédiatement le Wi-Fi et débranchez le câble réseau. Isolez la machine pour **stopper la propagation**. Ne l'éteignez surtout pas — cela détruirait des preuves numériques précieuses.

🛑 2. Ne jamais payer

Payer la rançon **ne garantit pas** la récupération de vos fichiers. Vous financeriez le crime organisé et deviendriez une cible récurrente pour de futures attaques.

📸 3. Conserver les preuves

Photographiez l'écran, conservez tous les messages suspects, historiques de navigation et journaux d'activité. Ces éléments seront **indispensables pour l'enquête**.

👮 4. Alerter et Porter plainte

Contactez les forces de l'ordre et déposez plainte. Si des données clients ont été compromises, vous avez **72 heures pour notifier la CNIL** — c'est une obligation légale.

⚠ ⚠️ Rappel critique : Ne jamais éteindre l'ordinateur infecté avant l'intervention des experts. Cela pourrait détruire des éléments de preuve essentiels à l'enquête judiciaire.

Vos alliés sur le terrain

🤝 La Gendarmerie Nationale à vos côtés

Ces services sont **gratuits, confidentiels et accessibles à toutes les entreprises** du Cantal. N'attendez pas d'être victime pour les contacter.

CCI CANTAL
1er ACCÉLÉRATEUR DES ENTREPRISES