LA CYBERSÉCURITÉ VERSION TOURISME

LES BASES POUR BIEN SE PROTÉGER

LIVRET THÉMATIQUE DE L'OFFICE

VALLÉE DU TARN
& MONTS DE L'ALBIGEOIS
TOURISME | OCCITANIE

SOMMAIRE

Ce livret, édité par l'Office de Tourisme de la Vallée du Tarn & Monts de l'Albigeois en 2024, vous propose une initiation, en 20 pages, à la cybersécurité. Vous trouverez tous les fondamentaux pour lutter contre les attaques en ligne.

L'évolution des transports de l'information s'est accélérée dans les années 2000. Elle aboutit aujourd'hui à une information transmise en temps réel.

La cybercriminalité est sans doute un fléau du 21ème siècle pour les entreprises et particuliers.

Le confinement a eu un effet accélérateur, les attaques se font de plus en plus fréquentes et touchent toutes les entreprises, de la plus petite à la plus grande.
Ce guide présente la mise en place de premières règles de prévention.

La cybersécurité c'est quoi ?

La mise en place de mesures de sécurité permettant de réduire les risques de cyberattaques et d'en limiter les conséquences en cas d'attaques malveillantes.

QUELQUES NOTIONS

Les cyberattaques

Les **cyberattaques** sont des tentatives d'abuser des données, en les volant, en les détruisant ou en les exposant. Elles visent à perturber ou à détruire les systèmes et réseaux informatiques.

La cyberdéfense

La **cyberdéfense,** incluse dans la cybersécurité, est l'analyse des menaces et les stratégies visant à se protéger contre les potentielles attaques dirigées contre les citoyens, les institutions et les gouvernements.

« Les cyberattaques sont la forme de criminalité à la croissance la plus rapide au monde. Le coût annuel de la cybercriminalité pour l'économie mondiale en 2020 est estimé à 5 500 milliards d'euros, soit le double de celui de 2015. »

LE RGPD, C'EST QUOI ?

Le **Règlement Général de la Protection des Données** est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne.

<u>3 objectifs :</u>

- Renforcer le droit des personnes
- Responsabiliser les acteurs traitant des données
- Crédibiliser la régulation (grâce à une coopération renforcée entre les autorités de protection des données)

<u>À qui s'adresse-t-il ?</u> Le RGPD s'adresse à toutes les structures privées ou publiques qui effectuent de la collecte et/ou du traitement de données personnelles, peu importe leur secteur d'activité et leur taille.

⚠️ Attention aux arnaques au RGPD

La **CNIL** et la **DGCCRF** mettent en garde les professionnels souhaitant faire appel à une société pour se mettre en conformité avec le RGPD car de multiples arnaques ont été constatées.

Certaines entreprises qui démarchent les professionnels, parfois de manière agressive, pour leur proposer leurs services, se prétendent mandatées par les pouvoirs publics et proposent des prestations onéreuses ou de faux services.
Elles peuvent proposer des prestations incomplètes, comme un simple échange ou l'envoi d'une documentation.

Sachez que se mettre en conformité avec le RGPD nécessite un véritable accompagnement par un professionnel qui analyse vos besoins, propose une solution adaptée et assure un suivi.

Quelques informations à vérifier avant de vous lancer avec une entreprise :

- L'identité de l'entreprise qui vous a démarché
- La nature des services proposés
- Les dispositions contractuelles ou pré contractuelles
- Méfiez-vous des entreprises utilisant des communications prenant les formes d'une communication officielle émanant d'un service public.
- Ne payez aucune somme d'argent supposée stopper une action contentieuse.

En cas de doute sur le message ou l'appel reçu (identité de l'interlocuteur, numéro de téléphone affiché, etc.), vous pouvez **contacter la CNIL**. Si vous êtes victime d'une arnaque, vous pouvez également **contacter la DGCCRF.**

LES DONNÉES PERSONNELLES, C'EST QUOI ?

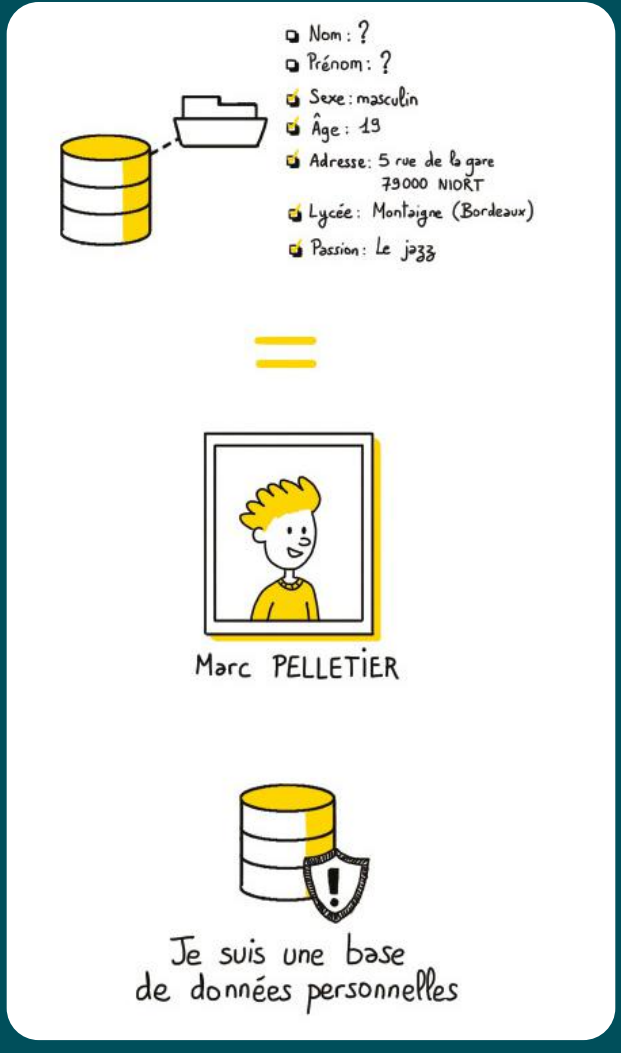
Une **donnée personnelle** est toute information se rapportant à une personne physique identifiée ou identifiable. Une personne peut être identifiée directement (ex : nom, prénom) ou indirectement (ex : un identifiant, une donnée biométrique, un numéro, etc.).

Un **traitement de données personnelles** (collecte, enregistrement, conservation, etc.) doit obligatoirement avoir un objectif. Il n'est pas possible de collecter des données au cas où cela serait utile un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

⚠ **Attention ! Les coordonnées d'une entreprise ne sont, généralement, pas des données personnelles.**

7 catégories de données personnelles :

- Relatives à l'identité (nom, prénom, adresse, photo, lieu de naissance, date de naissance, etc.)
- Relatives à la vie personnelle (habitudes de vie, de consommation, situation familiale, les loisirs, etc.)
- Relatives à la vie professionnelle (CV, diplôme, formation, fonction, lieu de travail, etc.)
- Informations économiques (revenus, impôts, données bancaires, etc.)
- Localisation (données GPS, géolocalisation, télépéages, etc.)
- Judiciaire
- Sensible (une « information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle)



LES CYBERMENACES LES PLUS FRÉQUENTES

Le phishing

Le **phishing**, appelé aussi **hameçonnage**, consiste à envoyer un e-mail frauduleux qui semble provenir d'une source fiable.

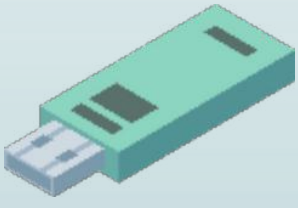
Son objectif est de voler des données sensibles comme les informations de carte de crédit et les identifiants de connexion ou d'installer des logiciels malveillants sur l'appareil de la victime.

L'hameçonnage est une cybermenace de plus en plus courante,. Selon le CESIN, pour 80% des entreprises ayant subi un acte de cyber malveillance, le principal vecteur d'attaque était le phishing.

Le malware

Le **malware** regroupe divers programmes malveillants (logiciels espions, rançongiciels, virus, vers). Un logiciel malveillant va être injecté dans le système informatique pour obtenir un accès non autorisé, perturber son fonctionnement et obtenir des informations.

Les cybercriminels profitent de la négligence et de la vulnérabilité des utilisateurs pour parvenir à faire installer les logiciels malveillants : clic sur un lien dangereux ou une pièce jointe infectée.



Les ransomwares

Les **ransomwares**, ou **rançongiciels** , sont un type de logiciel malveillant qui vise à bloquer l'appareil de l'utilisateur et/ou crypter ses données dans le but d'obtenir de l'argent. Le paiement de la rançon ne garantit pas que les fichiers seront récupérés ou le système restauré.

Ces attaques ont connu la plus importante augmentation ces dernières années ; le gouvernement a analysé + 95% d'attaques ransomwares en 2021.

Le déni de service

L'**attaque en déni de service**, ou en **déni de service distribué**, consiste à inonder les systèmes, serveurs ou réseaux de trafic pour provoquer une panne ou une suspension de service au sein du système informatique. Le système dysfonctionne et n'est plus accessible pour répondre aux demandes.

L'intercepteur

L'attaque de l'homme par le milieu, aussi appelé **attaque de l'intercepteur**, est un pirate qui s'insère entre deux transactions ou dans un échange entre deux interlocuteurs. L'agresseur va s'introduire dans l'échange, il va alors interrompre le trafic et voler les données. Le point d'entrée principale de ce type d'attaque est une connexion Wi-Fi publique non sécurisée.

L’injection SQL

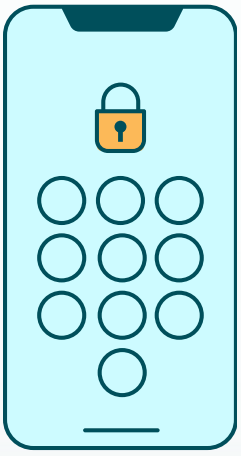
L’**attaque par injection SQL** (Strutured Query Language) se produit lorsque l’agresseur insère un code malveillant dans le serveur en utilisant un langage SQL (langage informatique). Il force le serveur à révéler des informations confidentielles. Les agresseurs utilisant cette technique s’attaquent souvent aux sites internet adossés à une base de données.

L’attaque au président

L’**attaque au président** consiste à se faire passer pour un dirigeant d’entreprise afin d’inciter un employé à divulguer des informations ou à réaliser des actions.

Drive by download

L’**attaque par téléchargement furtif**, ou **« Drive by download »**, consiste à diffuser un logiciel malveillant en s’insérant dans les failles de sécurité des plateformes (sites mal sécurisés, systèmes d’exploitation mal protégés, navigateur web pas mis à jour, etc.). Cette infection ne nécessite aucune action de l’utilisateur, c’est la plateforme consultée ou l’outil employé qui en est la cause.



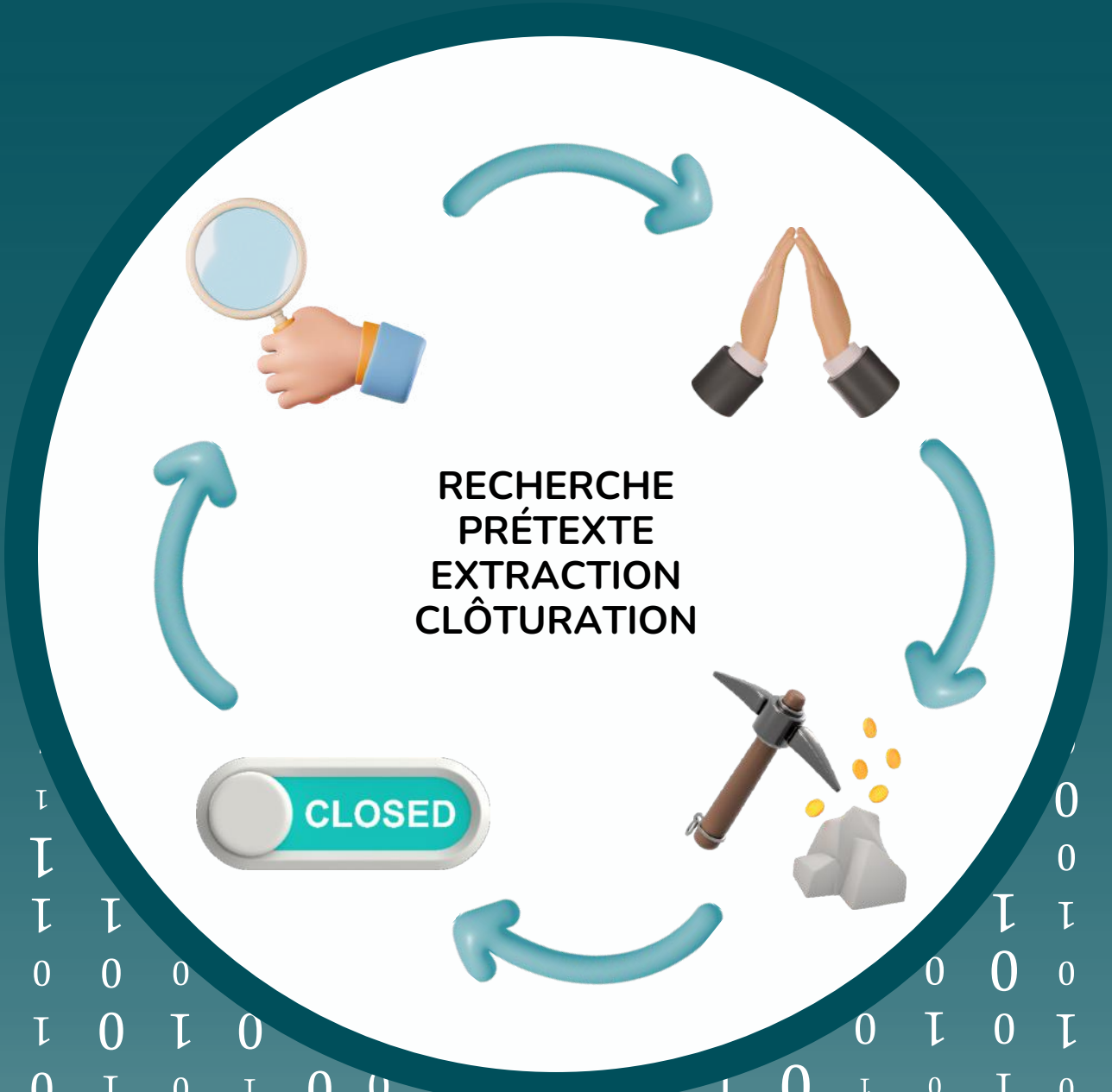
Le mot de passe

Le **mot de passe** est une ressource précieuse pour les cybers hackers. Ils mettent en place différentes techniques pour obtenir les mots de passe des collaborateurs d'une entreprise, ce qui leur permet d'accéder au système d'informations et ensuite de voler les données ou induire un dysfonctionnement.

L'écoute illicite

L'**attaque par écoute illicite**, ou **clandestines,** consiste à intercepter le trafic réseau pour obtenir des informations confidentielles. Les utilisateurs ne se doutent pas qu'ils sont sur écoute et livrent sans crainte des informations confidentielles. Les agresseurs utilisant cette technique s'attaquent souvent aux sites internet adossés à une base de données.

COMMENT FONCTIONNENT LES HACKERS ?

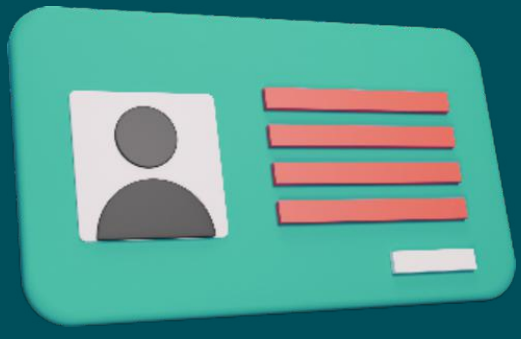


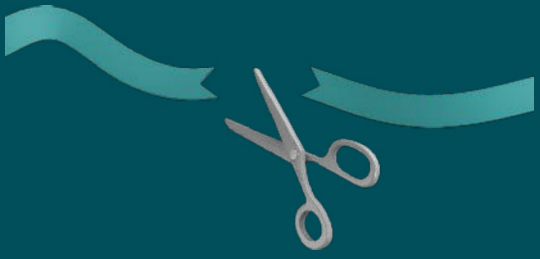
Un cyberhacker agit en 4 étapes :

L’hacker va choisir un évènement d’actualité ou d’intérêt collectif pour sélectionner et cerner ses cibles et les moyens de les atteindre, il va ensuite recueillir des renseignements sur ces dernières.

Il va aborder les cibles avec une histoire fausse mais vraisemblable, bâtir une relation ou établir le contrôle pour pousser, sous l’effet de la peur, et motiver les cibles à agir et à donner des renseignements.

Une fois la confiance gagnée, il va obtenir des informations personnelles ou financières de façon frauduleuse, et/ou convaincre les cibles à envoyer de l'argent.





Le pirate va alors mettre fin à la relation, décourager les cibles à répondre et brouiller les pistes.

COMMENT BIEN SE PROTÉGER ?

Utilisez des mots de passe robustes : il faut que vos mots de passe soient longs, complexes et composés de différents caractères (lettres majuscules et minuscules, des chiffres et des caractères spéciaux). Il faut qu'ils soient à la fois difficiles à trouver par un système automatisé mais également par une personne tierce. Variez vos mots de passe, évitez de mettre le même partout.

Préservez votre identité numérique : soyez vigilant en ligne et sur les réseaux sociaux, ne donnez pas vos données sensibles n'importe comment.

Sauvegardez régulièrement les données : il faut penser à sauvegarder vos fichiers régulièrement sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée, équipé d'un antivirus efficace ainsi qu'un système d'exploitation et de logiciels à jour.

Mettez à jour vos équipements : vos équipements informatiques doivent être équipés d'un antivirus efficace ainsi qu'un système d'exploitation et de logiciels à jour. Les hackers ciblent les ordinateurs utilisant des logiciels qui ne sont pas à jour pour exploiter les vulnérabilités non corrigées.

Évitez de se connecter aux réseaux non sécurisés. Évitez aussi les réseaux publics ou inconnus. Privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) lorsque vous êtes en déplacement.

Ne répondez pas aux demandes suspectes d'expéditeurs inconnus. Assurez-vous également qu'en passant la souris au-dessus du lien proposé, l'adresse du site soit conforme à l'expéditeur annoncé. Souvent, le contenu des sites frauduleux comporte des fautes de français, mais de plus en plus, les tentatives d'hameçonnage emploient un français correct. Enfin, soyez vigilant avant d'ouvrir les pièces jointes. Elles constituent le principal vecteur d'attaque et peuvent véhiculer des programmes malveillants.

VICTIME DE CYBERATTAQUE, QUE FAIRE ?

- **Déconnectez** immédiatement les équipements suspects du réseau en retirant le câble réseau ou en se déconnectant de la Wi-Fi.
- **Isolez** les éléments et les postes touchés en quarantaine sans éteindre le système.
- **Laissez les équipements suspects allumés** et ne les touchez plus afin de préserver les éléments techniques.
- **Ne connectez aucun appareil** au réseau.
- **S'il y a une demande de rançon, ne la payez pas !**

MISES À JOUR ET SAUVEGARDES

Les bons gestes !

Les mises à jour contribuent à lutter contre les cyberattaques, il ne faut donc pas les repousser !
Pensez à activer les mises à jour automatiques et utilisez uniquement les sites officiels des éditeurs !
Rendez-vous sur CERT.SSI.GOUV.FR pour connaître toutes les attaques en cours !

Pensez à sauvegarder vos documents régulièrement et sur plusieurs supports !

- **sauvegarde complète** : copie totale des données dans un nouvel espace de stockage
- **sauvegarde incrémentielle** : enregistre les données créées ou modifiées depuis la dernière incrémentielle. C'est plus long et complexe.
- **sauvegarde différentielle** : enregistre les données créées et modifiées depuis la dernière sauvegarde complète et les cumule. Plus simple et rapide à restaurer mais plus gourmande en espace.

  - sauvegarde sur bande
  - disque dur mécanique
  - disque flash
  - sauvegarde dans un cloud

SE FORMER ET S'INFORMER!

Gendarmerie nationale

6 Avenue de Millau
81250 ALBAN

Tel : 05 63 79 21 15

---

1 Chemin d'Albertis
81340 VALENCE-D'ALBIGEOIS

Tel : 05 63 56 48 10

---

26 Avenue de Millau
81430 VILLEFRANCHE-D'ALBIGEOIS

Tel : 05 63 56 48 10

CCI TARN

1 Avenue Général Hoche
81000 ALBI

Tel : 05 67 46 60 00

Mail : contact@tarn.cci.fr

France Services
Proche de vous au quotidien

1 rue du Sénateur Boularan
81250 ALBAN

Tel : 05 63 79 26 70

Mail : accueil@ccmav.fr

---

45 Avenue Pierre Souyris
81340 VALENCE-D'ALBIGEOIS

Tel : 05 63 53 72 15

Mail : val-81@france-services.gouv.fr

Quelles sources ont été utilisées ?

Quelques notions

https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd#

http://bit.ly/europal_europa_eu-pourquoi-la-cybersecurite-est-elle-important

Le RGPD, c'est quoi ?

https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd#

Les données personnelles, c'est quoi ?

https://bit.ly/koesio-10-questions-autour-du-RGPD

Les cybermenaces les plus fréquentes

https://www.cisco.com/c/fr_ca/products/security/common-cyberattacks.html

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-les-cybermalveillances-les-plus-frequentes

https://www.oodrive.com/fr/blog/securite/cybersecurite-top-10-des-cyberattaques-frequentes-en-2023/

https://www.cisco.com/c/fr_fr/products/security/what-is-cybersecurity.html#~types-de-menaces

Comment bien se protéger ?

https://www.gouvernement.fr/actualite/attention-aux-arnaques-en-ligne

Victime de cyberattaques, que faire ?

https://www.ssi.gouv.fr/uploads/2022/02/20220311_cyberattaque-comment-reagir.pdf

Plusieurs informations proviennent de formations faites par des professionnels.

LIVRET THÉMATIQUE DE L'OFFICE

www.valleedutarn-tourisme.com
accueil.tourisme@valleedutarn.fr
+33 (0)5 63 55 39 14

PLUS DE CONSEILS SUR NOTRE SITE