Ils font la cyber

Entretiens avec :
le Pôle d'excellence cyber
l'ANSSI
ITrust…
P. 2-4

le journal de la CYBER

Parlez-vous cyber ?
Quelques définitions **au fil des pages**

+ Mots de passe, phishing…
Les conseils de notre expert Ajyle
pour se protéger efficacement

#31* - Octobre 2024

Cybermenaces : Toulouse passe à l'action !

© Adonis Créative

ÉDITO

Toulouse, au cœur de l'innovation numérique et de la cybersécurité

© Toulouse Métropole

La démocratisation d'Internet et de l'Internet des Objets (IoT) a permis un extraordinaire foisonnement, mêlant curiosité et innovation. Néanmoins, ces évolutions technologiques comportent des risques, comme le développement de la cybercriminalité et des cyberattaques contre des institutions publiques et privées.
Face à cela, une véritable filière de la cybersécurité s'est organisée et nous pouvons nous enorgueillir, à Toulouse et dans notre Métropole, d'accueillir **un écosystème en plein essor, créateur d'emplois**.
Pour faciliter l'implantation de ces acteurs et créer un environnement propice à l'innovation et adapté à leurs besoins, nous offrons l'opportunité aux entreprises et aux écoles spécialisées dans la cybersécurité et l'intelligence artificielle de rejoindre un nouveau campus d'innovation dédié au numérique, Grand Matabiau quais d'Oc, au cœur d'un nouvel écoquartier.
Ainsi, nous anticipons et préparons l'avenir en nous appuyant sur les forces économiques déjà présentes sur notre territoire afin de permettre aux filières en développement de disposer d'un véritable lieu d'excellence au sein de ce campus.
Pour sensibiliser encore davantage à la cybersécurité, nous sommes ravis d'accueillir le CyberTour à Toulouse, le 22 octobre.
Puis nous accueillerons, le 28 novembre, le salon professionnel de la sécurité numérique des entreprises et des collectivités, au MEETT, notre parc des expositions et centre de conventions et congrès.

Jean-Luc Moudenc
Maire de Toulouse
Président de Toulouse Métropole

Vous avez dit CyberTour ?

Organisé par Projet X, ce **programme de conférences locales interactives au format TED** permet aux pros, experts et novices de partager leurs expériences autour de la cybersécurité. **Keynotes**, **tables rondes** et **ateliers** rassemblent des intervenants de premier plan pour offrir aux participants une compréhension approfondie des défis de demain. Après avoir fait étape dans le Gers, à Rodez et dans les Hautes-Pyrénées, le CyberTour s'arrête en octobre à Toulouse avec un programme exceptionnel ! Il reviendra dans la Ville rose en juin 2025. Restez informés : consultez le site https://www.cyber-tour.fr.

REGARDS CROISÉS

Rencontre avec **Bertrand Serp**, vice-président de Toulouse Métropole, et **Jean-Christophe Cau**, directeur général d'IKI, qui a conçu une solution de thérapie connectée. Cette dernière permet le suivi précis, régulier et personnalisé de l'état nutritionnel de l'utilisateur *via* l'analyse urinaire, avec pour objectif d'améliorer durablement ses habitudes alimentaires.

Comment Toulouse Métropole et ses entreprises abordent-elles la question de la cybersécurité ?

© Toulouse Métropole

Bertrand Serp : Nous devons créer un environnement favorable pour accompagner entreprises et citoyens face aux défis contemporains de l'intelligence artificielle et de la cybersécurité. Aujourd'hui, chacun peut être confronté aux dangers du hacking ou du cyberharcèlement. Toulouse Métropole aspire à devenir une métropole innovante et protectrice, pour ses citoyens comme pour ses entrepreneurs. L'IA et la cybersécurité sont au cœur de notre stratégie de transformation numérique.

© IKI

Jean-Christophe Cau : La cybersécurité est cruciale pour IKI, car nous travaillons dans le domaine de la santé. La sécurité des données y est primordiale, particulièrement après les récentes cyberattaques contre les centres hospitaliers.

Quels sont les besoins des entreprises en matière de cybersécurité ?

J-C.C. : Chez IKI, nous aimerions tout d'abord acculturer nos collaborateurs à la cybersécurité, les failles provenant majoritairement de facteurs humains. Ensuite, nous aimerions voir se développer un écosystème autour de la cybersécurité et de l'IA pour aller rechercher des synergies avec d'autres entreprises spécialisées.

Comment Toulouse Métropole peut-elle répondre aux besoins de son territoire ?

B.S. : Cette ambition de transformation digitale se matérialisera notamment par le futur campus numérique du Grand Matabiau, qui, à terme, sera doté de 50 000 m² dédiés à l'IA et à la cybersécurité. Ainsi, les start-up, PME, ETI, écoles et universités pourront travailler ensemble pour créer la ville numérique responsable et inclusive des Toulousains.

Comment Toulouse Métropole compte-t-elle associer à cette ambition l'ensemble de ses concitoyens ?

B.S. : L'IA et la cybersécurité ont un impact direct sur la vie quotidienne des citoyens et des entreprises. Il est essentiel de prendre conscience de ces défis et de structurer leur gestion au sein de nos territoires. Nous avons ainsi le projet de créer une « maison de l'IA » sur le site du Grand Matabiau, pour acculturer les Toulousains à ces sujets.

Quel rôle les entreprises joueront-elles dans cette dynamique ?

J-C.C. : IKI s'y retrouve tout à fait, avec la maison de l'IA et le futur campus numérique du Grand Matabiau. Les entreprises doivent à la fois jouer un rôle dans l'acculturation des citoyens, mais également proposer des solutions technologiques pour répondre aux défis du numérique. Elles doivent faire preuve d'ouverture vers la société et les autres entreprises, car ce sont des sujets qui deviennent cruciaux dans tous les domaines d'activité.

COMCYBER-MI, FORMER ET PROTÉGER À TOUS NIVEAUX

Au sein du Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI), le lieutenant-colonel Sophie Lambert est adjointe à la division de la connaissance, de l'anticipation et de la gestion de crise. Elle revient sur les missions de son équipe, qui a notamment contribué à la sécurisation des Jeux olympiques.

© BRC Frédéric ARRIGHI

Les Jeux olympiques sont terminés. Quel est votre sentiment ?

Fierté et soulagement ! Le 9 septembre a marqué pour nous la fin d'une période hors-normes. Même si nous avions fait un énorme travail de préparation et d'anticipation, nous redoutions forcément d'être passés à côté de quelque chose.

Le niveau de menace annoncé était effectivement sans précédent. Comment s'est passé l'été ?

Avant et pendant les Jeux, nous avons connu une vague d'attaques aux formes variées. Les fraudes à la billetterie en particulier ont été nombreuses (396 sites web frauduleux découverts). Plus globalement, nous avons observé 3 pics d'attaques pendant l'été : pendant les législatives, après la « Cène » de la cérémonie d'ouverture, et le troisième à la suite de l'arrestation de Pavel Durov, patron de Telegram.

Comment est organisé le Commandement du ministère de l'Intérieur dans le cyberespace?

Le COMCYBER-MI coordonne les 3 services chargés de la lutte contre les cybermenaces, ce qui représente environ 200 personnes. La première division élabore la stratégie de lutte contre la cybercriminalité, travaille à la coopération internationale et à la veille juridique. La deuxième, à laquelle j'appartiens, a pour but d'anticiper les menaces et la gestion de crise. La troisième division rassemble et met à disposition des compétences rares, telles que [celles d']enquêteurs hautement spécialisés en cryptomonnaies. Enfin, le COMCYBER-MI pilote aussi le Centre national de formation cyber pour les forces de sécurité intérieure.

Parlez-nous de votre division.

Nous effectuons la surveillance, la détection et l'analyse des cybermenaces.
En revanche, nous ne faisons pas de réponse à incidents. Nos analystes pistent les cybercriminels dans le but de fournir un maximum d'éléments les concernant aux autorités compétentes : le PNACO, l'OFAC, l'UNC… Nous tâchons aussi de sensibiliser les entreprises et les aider à anticiper l'imprévu pour éviter la sidération le jour de la cyberattaque. Cybermalveillance *(voir p. 4)* est notre partenaire incontournable.

> **Nous tâchons aussi d'aider les entreprises à anticiper l'imprévu pour éviter la sidération le jour de la cyberattaque.**

Vous avez été élue Femme cyber de l'année 2023 (catégorie défense et sécurité) par le Cercle des femmes de la cybersécurité (CEFCYS), et l'association Women4Cyber vous compte comme l'une de ses ambassadrices. Pourtant, rien ne vous prédestinait à évoluer sur ce cyberterrain…

Je viens effectivement d'une autre sphère, celle du judiciaire, des homicides. Soit dit en passant, la cyber infuse partout : il n'existe pas aujourd'hui une seule scène de crime sans un objet connecté. En 2022, j'ai passé un MBA en cyber avant de prendre mon poste actuel. La gendarmerie n'opte que rarement pour des hyper-spécialistes, dans le but d'éviter l'« effet tunnel » : elle m'a positionnée sur cette matière pour avoir un regard neuf. Mon expérience du terrain me permet d'apporter des réponses au citoyen. C'est lui que l'on sert, toujours. Enfin, au travers de Women4Cyber, je souhaite promouvoir les femmes dans la cyber, et vice-versa : il y existe des métiers pour toutes et tous, pas que pour les fondus d'informatique. Et le sujet prend tellement d'ampleur qu'aujourd'hui, on a besoin de tout le monde !

LEXIQUE

PNACO : Parquet national anticriminalité organisée

OFAC : Office anti-cybercriminalité

UNC : Unité nationale cyber

BL2C : Brigade de lutte contre la cybercriminalité

DGSI : Direction générale de la sécurité intérieure

CHIFFRES-CLÉS (en 2023)

Environ 850 000
signalements ou plaintes (+ 8 % par an)

dont :

278 770
plaintes déposées au commissariat ou à la gendarmerie

104 439
déclarations ou dépôts de plaintes sur la plateforme THESEE

259 094
signalements sur la plateforme Perceval (arnaques à la carte bancaire)

211 543
contenus illicites signalés sur Pharos

NB : Ces chiffres sont en dessous de la réalité du nombre d'attaques.

PÔLE D'EXCELLENCE CYBER, FAIRE ÉMERGER UNE CYBERDÉFENSE FRANÇAISE AUTONOME

Père fondateur de la cyberdéfense française, Arnaud Coustillière est devenu en 2011 le premier commandant cyber des armées, poste qu'il a occupé jusqu'en 2017. Président du Pôle d'excellence cyber depuis 2021, il nous en explique les missions.

© David Marnier

En matière de cyberdéfense, où la France se place-t-elle sur l'échiquier international ? Et quelles sont nos forces ?

La France a atteint un niveau de maturité satisfaisant – en témoigne le récent succès olympique –, mais cela ne s'est pas fait en un jour. En 2009-2010, nous étions un minuscule acteur à la traîne derrière toutes les nations anglo-saxonnes. L'État a fait un gros effort de moyens et a mis en place le cadre juridique : en 10 ans, la France a rattrapé son retard.
Sur le volet civil, elle se place au même niveau que l'Allemagne, derrière les Britanniques. La France est très bien organisée et dispose d'un corpus réglementaire très complet, bâti de façon continue depuis 2013 avec la loi de programmation militaire, renforcée en 2017, et plus récemment avec la loi SREN. Dans les évolutions de la cyber en France, nos parlementaires ont toujours été à la manœuvre.
Enfin, côté militaire, et si on laisse de côté les États-Unis, la technique française est, selon moi, la plus avancée parce que la mieux intégrée à tous les processus opérationnels. Le cybercommandement de l'armée rassemble désormais plus de 4 500 personnes, contre une centaine en 2010.

> **La cyberdéfense française a rattrapé son retard.**

Quels sont les défis de la filière, notamment en termes de formation ?

Pour être souverain, il faut des compétences. La désaffection pour les matières scientifiques pose un gros problème dans tous les métiers du numérique, et en particulier dans cette filière très pointue et stratégique de la cyber, tout comme la faible féminisation (entre 11 et 15 %) : non seulement on se prive de la moitié des talents, mais on manque aussi de variété dans les schémas de pensée. Que ce soit pour entraîner correctement les IA ou pour traquer les attaquants, il faut penser autrement, car le bon hacker, lui, réfléchit *outside the box*. L'offre de formation, enfin, est insuffisante par rapport au nombre de postes ouverts, car les écoles sont bridées par le manque de formateurs. En revanche, la cyber commence doucement à infuser dans tous les enseignements. Point positif : cela montre que l'enjeu, très transverse, de sécurité et de confiance dans l'espace numérique a été compris.

Le Pôle d'excellence cyber (PEC) est une association fondée en 2014 par le ministère des Armées et la Région Bretagne. Quel est son rôle ?

Le PEC est né d'une volonté de centraliser les efforts en recherche, formation et *business development* pour faire émerger une cyberdéfense française autonome, moins dépendante des grands acteurs internationaux. Le PEC anime la filière et favorise les échanges : aujourd'hui, ses 130 entreprises membres dans toute la France interagissent notamment *via* une trentaine de groupes de travail où elles croisent leurs regards sur des sujets variés, par exemple le *zero trust*. Les livrables produits sont mis à disposition de la communauté : il y a eu un « Guide pratique pour la sécurisation des collectivités territoriales et des PME », plusieurs analyses en matière de formation, etc. Cette partie est la plus visible du grand public. Mais le Pôle permet aussi la création de consortiums, qui ont remporté plusieurs appels à projets, comme CyberSkills4All récompensé par France 2030. Enfin, le PEC organise aussi l'European Cyber Week, cette année du 18 au 21 novembre, un rendez-vous français annuel et incontournable de la communauté cyber régalienne.

Quels sont les nouveaux métiers de la cyber ?

Data analysts et scientists spécialisés en cyber, experts en intelligence artificielle… De manière générale, tous les métiers en lien avec le traitement de la donnée et la gestion de crise ont vocation à émerger. Le *social engineering* a toujours le vent en poupe. Les métiers de l'OSINT sont amenés à se multiplier, des profils généralistes pour le web classique et des spécialistes, qui tentent d'aller retrouver les données volées sur le dark web. Enfin, on voit apparaître des profils très pointus, comme des experts en rétro-ingénierie appliquée à la cyber.

Zero trust security (sécurité à confiance zéro) : Modèle de sécurité qui n'accorde une confiance automatique à aucun utilisateur ou appareil, à l'intérieur ou à l'extérieur du réseau de l'organisation. Il nécessite une vérification continue de tous les utilisateurs et dispositifs tentant d'accéder aux ressources du système.

Plus d'infos : https://cyber.gouv.fr/publications/le-modele-zero-trust

LE PHISHING

Dans le vaste univers de la cybersécurité, naviguer à travers les menaces peut s'avérer un défi. Quelques conseils pratiques de notre **expert Ajyle.**

QU'EST-CE QUE C'EST ET COMMENT L'ÉVITER ?

Le phishing ? Une technique utilisée par les cybercriminels pour vous tromper et vous amener à divulguer des informations personnelles, comme vos mots de passe ou détails bancaires. Ils envoient souvent des e-mails ou des messages qui semblent provenir de sources légitimes.

3 RÈGLES POUR SE PROTÉGER EFFICACEMENT :

1. VÉRIFIEZ TOUJOURS L'ADRESSE E-MAIL DE L'EXPÉDITEUR

POURQUOI C'EST IMPORTANT
Les cybercriminels sont habiles pour masquer leur identité derrière des adresses e-mail qui semblent légitimes à première vue. Ils peuvent utiliser des techniques de spoofing pour faire apparaître leur e-mail comme venant d'une entreprise ou d'une personne de confiance. En inspectant attentivement l'adresse de l'expéditeur, vous pouvez déceler des indices révélateurs, comme des fautes d'orthographe subtiles ou des domaines étrangement formulés, qui indiquent une tentative de phishing.

COMMENT PROCÉDER
- Survolez (sans cliquer) le nom de l'expéditeur pour afficher l'adresse e-mail complète.
- Comparez l'adresse avec celle que vous savez être authentique.
- Soyez particulièrement vigilant avec les e-mails qui demandent des actions urgentes ou des informations personnelles.

2. MÉFIEZ-VOUS DES LIENS ET DES PIÈCES JOINTES DANS LES E-MAILS NON SOLLICITÉS

POURQUOI C'EST IMPORTANT
Les liens et pièces jointes dans les e-mails non sollicités sont des vecteurs courants pour les logiciels malveillants. Cliquer sur un lien ou ouvrir une pièce jointe malveillante peut entraîner l'installation de malwares sur votre appareil, compromettant ainsi votre sécurité et celle de vos données. Ne pensez pas qu'une pièce jointe est forcément un document inerte !

COMMENT PROCÉDER
- Avant de cliquer, survolez le lien pour prévisualiser l'URL et vérifier si elle mène à un site web légitime.
- Évitez d'ouvrir des pièces jointes d'expéditeurs inconnus ou non attendus.
- Si un e-mail semble provenir d'une source fiable mais que vous n'attendiez pas de pièce jointe, contactez l'expéditeur par un autre moyen pour confirmer son authenticité.
- Utilisez des logiciels de sécurité qui incluent une protection contre les liens et pièces jointes malveillants.

3. UTILISEZ LA VÉRIFICATION EN 2 ÉTAPES POUR VOS COMPTES EN LIGNE

POURQUOI C'EST IMPORTANT
La vérification en 2 étapes (également appelée authentification à 2 facteurs ou 2FA) ajoute une couche de sécurité supplémentaire à vos comptes en ligne. Même si un cybercriminel parvient à obtenir votre mot de passe, il lui sera beaucoup plus difficile d'accéder à votre compte sans également avoir accès à votre second facteur d'authentification, qui peut être un code envoyé à votre téléphone, une application d'authentification ou un dispositif matériel.

COMMENT PROCÉDER
- Activez la 2FA sur tous les comptes qui proposent cette option, en particulier sur les comptes critiques tels que les e-mails, les réseaux sociaux et les services bancaires en ligne.
- Préférez les applications d'authentification ou les clés de sécurité matérielles aux SMS ou e-mails, car ces derniers peuvent être interceptés ou détournés.
- Gardez un dispositif de secours configuré pour la 2FA au cas où vous perdriez l'accès à votre principal moyen d'authentification.

UN PEU D'HISTOIRE…

Au milieu des années 1990, on se connectait à Internet *via* un modem. Les pirates, cherchant à obtenir un accès gratuit au web, créaient des programmes qui se faisaient passer pour des logiciels d'authentification légitimes.

DÉFINITIONS

- **Spoofing**
Pratique malveillante visant à se faire passer pour une autre entité ou personne dans le but de gagner la confiance d'une victime, d'obtenir des informations sensibles, de voler des données ou de diffuser des malwares. Cette technique peut être utilisée dans divers contextes, notamment : spoofing d'adresse e-mail, d'adresse IP, d'identifiant d'appelant (*caller ID spoofing*), de site web…

- **Malware**
Logiciel malveillant, conçu pour endommager ou infiltrer un système informatique. Il peut se présenter sous forme de virus, de « ransomware » (qui prend en otage les données et menace de les diffuser si une rançon n'est pas payée) ou de « spyware » (qui espionne l'activité et vole les données).

- ***Social engineering*** (ingénierie sociale)
Manipulation psychologique des personnes dans le but d'obtenir des informations confidentielles ou d'accéder à des systèmes sécurisés. Les attaquants exploitent souvent la confiance, la curiosité ou la peur des victimes.

Suite : voir p. 6.

L'ANSSI EN RÉGION OCCITANIE, PRÉVENIR ET ACCOMPAGNER

Chef de file national de la cybersécurité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) coordonne les acteurs français, pilote la coopération internationale et conseille le gouvernement. Rémy Daudigny, délégué à la sécurité numérique pour l'Occitanie, fait le point sur les enjeux régionaux.

© Hélène Ressayres/ToulÉco

En tant que délégué régional de l'ANSSI, quelle est votre mission ?

En Occitanie, nous sommes 2 délégués, mais il y aurait du boulot pour 10 ! Notre rôle est justement de trouver des relais et d'accompagner environ une centaine de collectivités sur le plan réglementaire de la cyber. Nous contribuons aussi au dispositif de sécurité économique piloté par la préfecture, en apportant notre expertise technique aux structures sensibles. Enfin, nous aidons les universités et écoles à développer des formations en cyber, notamment du côté de Castres.

Quelles sont les cybermenaces en Occitanie ?

Elles peuvent venir des États – souvent de l'espionnage, concernant principalement l'aéronautique – comme de cybercriminels indépendants, qui s'attaquent aux adresses IP pour les récupérer et les exploiter, sans se soucier de leur propriétaire.

> **Tout le monde – absolument tout le monde – est concerné. Peu importe que vous vous estimiez être ou non « intéressant » pour un cyberattaquant.**

Quelles organisations réclament une vigilance accrue ?

Pour la sécurité des activités d'importance vitale (SAIV) – transports, santé, distribution de l'eau… – l'ANSSI dispose d'une « coordination sectorielle » nationale. Localement, nous veillons à la cybersécurité des acteurs hors SAIV, comme ceux de l'écosystème aéronautique, certains des domaines médical, énergétique, agricole, ou encore des nombreux pôles de compétitivité.

Intervenez-vous directement lors d'une cyberattaque ?

Nous intervenons en renfort pour des cas très graves, comme des attaques contre des structures hospitalières. L'ANSSI ne conduit pas d'opérations judiciaires mais vient en soutien de l'enquête.

La directive NIS 2 est entrée en application le 17 octobre. Qu'implique-t-elle pour les PME, et comment l'ANSSI va-t-elle les accompagner ?

NIS 2, c'est la « RGPD de la cybersécurité ». Dans 18 secteurs d'activité très larges, toute entreprise de plus de 50 personnes et réalisant au moins 10 millions d'euros de chiffre d'affaires devra par exemple se déclarer sur le site dédié, dédier une personne à la cybersécurité et adopter les bonnes pratiques : systèmes d'information à jour, mots de passe robustes, sauvegardes régulières… Une vingtaine d'objectifs de sécurité simples ont été définis. Nous avons développé MonAideCyber pour acculturer les PME et les accompagner durant 2 à 3 ans. Au-delà de ce délai de mise en œuvre, celles qui n'auront fait aucun effort pourront être sanctionnées par une amende.

La multiplication des actions de sensibilisation a-t-elle permis une prise de conscience générale ?

Très clairement, non ! Même si nous sommes sur la bonne voie, les chefs d'entreprise ont toujours du mal à réaliser qu'ils sont en guerre économique et que les outils numériques dont ils sont dépendants sont des armes. C'est la même chose pour les maires, parfois inconscients des risques encourus pour leurs administrés. Beaucoup d'attaques visent à déstabiliser notre démocratie. Même une petite mairie peut être une cible, et beaucoup sont déjà attaquées.

LIENS UTILES

La directive NIS 2
https://cyber.gouv.fr/la-directive-nis-2

Mon espace NIS 2
https://monespacenis2.cyber.gouv.fr/

MonAideCyber
www.monaidecyber.ssi.gouv.fr/

CYBERMALVEILLANCE, LANCEMENT D'IMPACTCYBER

Plus connu sous le nom de son portail cybermalveillance.gouv.fr, le GIP ACYMA* mène des actions d'assistance et aussi de prévention, comme le Cybermoi/s. Laurent Verdier, directeur du pôle sensibilisation, présente notamment l'opération ImpactCyber.

© DR

Comment sera déployée ImpactCyber?

Cette opération comprend 3 volets : une enquête nationale auprès d'entreprises de toutes tailles et tous secteurs, une campagne originale de sensibilisation avec 3 clips vidéo, et la publication d'un mémento de cas réels d'attaques. L'objectif est d'inciter les entreprises à mieux appréhender les enjeux cachés derrière les cyberattaques et à s'approprier une véritable démarche de sécurisation technique, organisationnelle et humaine.

Comment améliorer la sensibilisation des PME et TPE ?

Il est essentiel de comprendre les problématiques d'un chef d'entreprise, constamment sollicité. Il faut être audible à des moments où il est réceptif, avec des mots simples et des propositions de ressources faciles à mettre en place. Lui expliquer concrètement les enjeux de la manière la plus pédagogique possible, par exemple *via* des témoignages de pairs.

> **« 4 entreprises sur 5 ne sont pas préparées à une cyberattaque. »**

Comment les missions de Cybermalveillance s'articulent-elles avec celles des centres régionaux, comme Cyber'Occ ?

Nous sommes complémentaires : Cybermalveillance s'adresse à tous, particuliers et professionnels, avec une assistance en ligne. En cas de besoin spécifique, l'entreprise sera orientée vers un partenaire. Cyber'Occ *(voir p. 5)* propose un service beaucoup plus personnalisé, avec une assistance téléphonique et un suivi sur mesure.

CHIFFRE-CLÉ

280 000
recherches d'assistance enregistrées sur le portail en 2023.

ITRUST, PURE PLAYER EN CYBERSÉCURITÉ

Société toulousaine créée en 2007 et filiale du Groupe iliad, ITrust est profondément ancrée dans l'écosystème cyber régional : création d'emplois, accès à la formation, représentation de la Région à l'étranger, participation à la sécurisation de grandes entreprises locales, innovations technologiques… Rencontre avec Jean-Nicolas Piotrowski, son fondateur et président.

© Xavier Popy

Quelles sont les principales difficultés rencontrées par les entreprises françaises en matière de cybersécurité aujourd'hui ?

Le manque de ressources dédiées, ainsi qu'une sensibilisation et une formation insuffisantes. En outre, les PME n'ont souvent pas les moyens d'accéder à des solutions complètes et robustes.

Quels conseils leur donneriez-vous ?

Nous recommandons aux entreprises de commencer par une évaluation complète de leurs risques cyber (audits, pentests). Une fois ces risques identifiés, il est important d'adopter une approche proactive et efficace, incluant non seulement la mise en place d'outils avancés, mais aussi la sensibilisation des collaborateurs.

Quelle est votre philosophie ?

Notre ambition est de démocratiser la cybersécurité pour toutes les entreprises, organisations et collectivités locales, quels que soient leur taille ou leur secteur d'activité, avec des logiciels et services 100 % souverains, faciles d'accès et ultra-performants.

> **« Avec l'adoption croissante du cloud et l'Internet des objets (IoT), les menaces vont devenir plus complexes. »**

Quelle est l'actualité d'ITrust ?

Nous continuons d'innover avec des solutions basées sur l'IA, comme Reveelium, qui permettent une détection avancée des anomalies et une réponse rapide aux menaces, réduisant ainsi le risque d'attaques abouties. Nous créons aussi de nouvelles offres visant à rendre la cybersécurité accessible à tous.

Quelles sont vos forces ?

Nos solutions se distinguent par leur intégration de nouvelles technologies, dont l'IA. Nous offrons une gamme complète allant de la protection préventive à la détection d'intrusions et à la réponse aux incidents. En outre, nous proposons un accompagnement personnalisé, ce qui permet à nos clients d'adapter nos solutions à leurs besoins spécifiques.

*Groupement d'intérêt public Action contre la cybermalveillance.

TRUCS & ASTUCES

Quelques conseils pratiques de notre **expert Ajyle.**

#FAQ : MALWARES

COMMENT IDENTIFIER ET SE PROTÉGER CONTRE LES MALWARES ?

Les malwares, ou logiciels malveillants, sont conçus pour endommager ou infiltrer un système informatique. Ils peuvent se présenter sous forme de virus, de ransomwares ou encore de spywares.

LES BONNES PRATIQUES

1. INSTALLEZ UN ANTIVIRUS FIABLE ET METTEZ-LE À JOUR RÉGULIÈREMENT

POURQUOI C'EST IMPORTANT

Un logiciel antivirus joue un rôle crucial dans la détection et la neutralisation de logiciels malveillants qui pourraient infecter votre appareil. Un bon antivirus peut vous protéger contre une vaste gamme de menaces, y compris les virus, les logiciels espions, les ransomwares et d'autres formes de malwares.

COMMENT PROCÉDER

- Choisissez un logiciel antivirus réputé en vous basant sur des évaluations indépendantes et des critiques fiables. Prenez en compte les fonctionnalités offertes, la facilité d'utilisation et l'impact sur les performances de votre système.
- Activez les mises à jour automatiques pour votre antivirus afin de vous assurer qu'il est toujours actualisé avec les dernières définitions de virus et améliorations de fonctionnalités. Les menaces évoluant constamment, ce point est essentiel pour une protection efficace.
- Effectuez des analyses régulières pour détecter et supprimer les éventuels malwares présents sur votre appareil. Bien que la protection en temps réel soit essentielle, des analyses complètes périodiques peuvent révéler des menaces qui ont pu passer inaperçues.

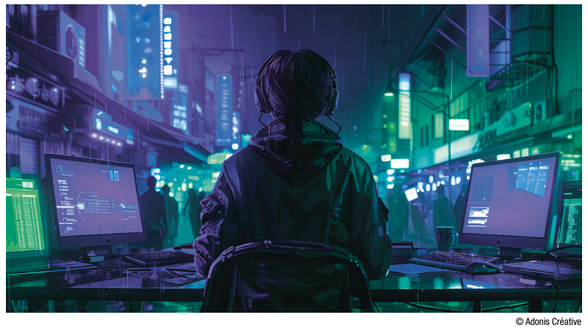
2. ÉVITEZ DE TÉLÉCHARGER DES FICHIERS OU DES LOGICIELS DEPUIS DES SITES WEB NON SÉCURISÉS

POURQUOI C'EST IMPORTANT

Les sites web non sécurisés peuvent héberger des logiciels malveillants déguisés en téléchargements légitimes. Télécharger et installer ces fichiers peut compromettre la sécurité de votre appareil.

COMMENT PROCÉDER

- Vérifiez la fiabilité des sources avant tout téléchargement. Privilégiez les sites officiels ou les plateformes de distribution reconnues.
- Recherchez des signes de sécurité, tels qu'une connexion HTTPS sécurisée (indiquée par un cadenas dans la barre d'adresse de votre navigateur), et lisez les avis d'autres utilisateurs si disponibles.
- Utilisez un logiciel antivirus avec protection web, qui peut vous avertir et vous protéger contre les téléchargements dangereux et les sites web malveillants.



© Adonis Créative

3. GARDEZ VOTRE SYSTÈME D'EXPLOITATION ET VOS APPLICATIONS À JOUR

POURQUOI C'EST IMPORTANT

Les mises à jour de logiciels incluent souvent des correctifs pour les vulnérabilités de sécurité qui, si elles sont exploitées, peuvent permettre aux attaquants d'infiltrer ou de compromettre votre appareil. En maintenant votre système et vos applications à jour, vous minimisez le risque d'attaques.

COMMENT PROCÉDER

- Activez les mises à jour automatiques pour votre système d'exploitation et vos applications. Cela garantit que vous recevez et appliquez les correctifs de sécurité dès qu'ils sont disponibles.
- Vérifiez manuellement les mises à jour périodiquement, surtout pour les logiciels critiques ou ceux qui ne se mettent pas à jour automatiquement.
- Soyez attentif aux notifications de mise à jour de votre système ou de vos applications et n'ignorez pas les recommandations d'installation de mises à jour de sécurité.

Pour en savoir plus : voir p. 8.

CYBERINSÉCURITÉ : MENACE OU OPPORTUNITÉ ?

Par Marc Sztulman,
conseiller régional délégué au numérique et président de Cyber'Occ.

© Région Occitanie - DR

Un spectre hante le monde, celui de la cyberinsécurité.
Notre économie ne connaîtra plus jamais les eaux calmes de la cybersécurité. L'omniprésence des attaques modifie notre définition même du numérique, que l'on peut désormais appréhender comme l'ensemble des activités humaines soumises à des risques cyber.

Notre monde est dorénavant celui de la cyberinsécurité, et ce changement constitue une évolution structurante et sans concurrence pour nos économies. Là où tout un chacun s'émerveille des prouesses de l'IA, nous pouvons y discerner les mouvements de fond derrière l'écume. Gageons que l'élément central de l'édifice sera le développement de la cyberinsécurité. Qu'on y songe, la seule possibilité d'utiliser en confiance un LLM est *in fine* une question de cyberinsécurité. L'âge d'or de la sécurité est derrière nous, nos mots de passe, guère plus sécurisés qu'un schibboleth, nos protocoles aussi sûrs que le télégraphe qui causa la ruine de Danglars.
Qui ne voit derrière le paravent des discours techniques et sécuritaires une concentration criminelle et étatique jamais rencontrée dans l'histoire ? Le retour sur investissement des cyberattaques est massif, et cette activité criminelle est d'autant plus attractive que le risque pénal est faible. Rendons-nous à l'évidence, Robert Solow avait tort ; la vraie productivité engendrée par la généralisation de l'informatique est la productivité criminelle.

> **« Ce bouleversement n'est ni un jeu de mots, ni un concept marketing ; il constitue un changement de paradigme dans le monde de l'informatique. »**

Quelle est notre réponse collective face à ce risque existentiel ? Une augmentation marginale des budgets des services informatiques ? Une approche par le biais de la réglementation qui génère des documents que personne ne lit, et que désormais, grâce aux LLM, plus personne n'écrit ? Des discours très généraux sur la souveraineté, tenus par des libéraux, sans accepter qu'elle ait pour conséquence une limitation des usages des technologies étrangères, aussi intéressantes soient-elles ?

Une autre voie est possible.
Il nous faut en effet nous emparer de la cyberinsécurité comme d'un levier de transformation et d'évolution de nos entreprises. Confrontés aux facilités hypnotiques de la technologie, nous devons nous interroger sur nos usages : est-il vraiment nécessaire d'avoir accès à l'ensemble des comptes bancaires de l'entreprise en distanciel ? Nos entreprises étaient-elles réellement moins productives quand un virement ne pouvait pas s'effectuer de manière instantanée ? Compte tenu des périls majeurs qui nous guettent, nous devons nous saisir collectivement du problème de la cyberinsécurité. On ne peut lutter contre un fléau de cette ampleur avec des pratiques et des réponses individuelles. C'est de manière collective, dans le temps long, qu'il importe d'agir. Pour ce faire, nous devons retrouver le bon sens ordinaire, cette chose du monde la mieux partagée, et cesser de considérer que les solutions les plus modernes sont nécessairement les meilleures…

Le monde de la sécurité est derrière nous, et il nous appartient de transformer le désastre annoncé en opportunité.

DÉFINITION

LLM (*large language model*)
Modèle d'intelligence artificielle entraîné sur d'énormes volumes de données textuelles. Il comprend et génère du langage naturel, permettant des interactions complexes avec les usagers humains.

CYBERSÉCURITÉ EN OCCITANIE : CHIFFRES-CLÉS

De 3 000 à 6 000
personnes mobilisées par la cybersécurité, un nombre qui devrait doubler dans les 2 ans.

150 millions d'euros
dédiés entre 2023 et 2027 au contrat de filière numérique, qui comprend de nombreuses actions destinées à la cybersécurité.

Près de 200 entreprises
régionales spécialisées en cybersécurité.

Une quarantaine d'universités, écoles et laboratoires
impliqués dans la région.

Source : laregion.fr

GROUPAMA D'OC, ASSURER CONTRE LE RISQUE CYBER

Tony Texeira, responsable partenariats et innovation chez Groupama d'Oc, détaille les actions mises en place pour protéger les assurés de la compagnie.

© Groupama d'Oc

La cybersécurité est devenue un facteur-clé pour les assurances. Comment Groupama d'Oc accompagne-t-elle ses clients face aux cyberattaques ?

Groupama d'Oc a lancé en 2018 une assurance cyber pour couvrir ce risque croissant, avec + 30 % de cyberattaques en 2023, dont 69 % visant les entreprises. Notre offre couvre la prise en charge de l'attaque, la remédiation du système d'information, la perte d'exploitation et l'e-réputation.

Comment sensibilisez-vous vos assurés, notamment les PME et TPE, aux risques cyber ?

Seules 4 à 5 % des entreprises possèdent une assurance cyber, un chiffre faible face à ce risque majeur qui peut affaiblir ou anéantir une entreprise non préparée. Il faut comprendre que nous venons sécuriser la trésorerie d'une entreprise et sécuriser la responsabilité du dirigeant, qui est forcément engagée.
Pour cela, Groupama d'Oc a mis en place un plan de sensibilisation en offrant un « CyberScan », c'est-à-dire un premier niveau d'audit des vulnérabilités liées aux informations publiques, comme sur le site web, et l'exposition sur le dark web. Nous organisons également des webinaires, [proposons] des tutos, et sommes partenaires du CyberTour, pour continuer de sensibiliser sur ce fléau dans les territoires.

> **« Seulement 5 % des entreprises souscrivent une assurance pour le risque cyber ! »**

Quel rôle joue l'innovation dans la protection des données de Groupama d'Oc et de ses assurés ?

L'innovation, notamment l'IA, est au cœur de notre stratégie. La cyber est un sujet très complexe qui nécessite beaucoup d'expertises diverses et des collaborations avec nos partenaires technologiques pour contrer des organisations malveillantes, très bien outillées. Nous regardons de près certaines ESN qui sont en capacité de faire du prédictif sur la cyber. Aujourd'hui, l'idée n'est plus de savoir si on va être attaqué ou pas, mais plutôt de se dire : « Comment mon entreprise est en capacité de repartir en condition opérationnelle le plus rapidement possible pour subir le moins d'impact possible ? »

BOUGE TOULOUSE, VIVRE-ENSEMBLE, PROGRÈS ET CYBERSÉCURITÉ

Le vivre-ensemble est au cœur de l'action de Bouge Toulouse, un think tank qui propose, recense et accompagne les idées pour faire avancer la métropole. Quel rapport avec le CyberTour ? Les réponses de Philippe Joachim, son fondateur et président.

© Hugo Breams

Pourquoi un think tank comme Bouge Toulouse s'intéresse-t-il au CyberTour ?

L'objectif du think tank Bouge Toulouse est d'être force de proposition pour notre ville, dans tous les domaines, toujours au profit de l'intérêt général. Nous avons aussi le souhait d'accompagner les initiatives qui nous font avancer collectivement. De ce point de vue, il est évident que le CyberTour fait œuvre utile. Nous sommes ravis de nous associer à ce très bel événement. De plus, la question des sécurités, dont la cybersécurité, est devenue un sujet majeur pour le « vivre-ensemble ».

Quels sont les apports mutuels entre Bouge Toulouse et le CyberTour ?

Nous souhaitons en premier lieu sensibiliser notre réseau sur les thématiques évoquées lors de cette journée et inciter les personnes qui nous suivent à participer à l'événement. Nous interviendrons aussi dans les débats. Enfin, nous lancerons une enquête sur la question de la cybersécurité, dont les résultats seront présentés à cette occasion.

> **« La cybercriminalité est devenue l'une des insécurités les plus répandues dans nos sociétés, avec un taux de progression record. »**

Au delà de l'événement du jour, quelles actions en matière de cybersécurité le CyberTour inspire-t-il ?

La cybersécurité a pris une importance majeure en moins de 10 ans, tant pour les entreprises, les institutions que pour chacun d'entre nous, à titre individuel. La cybercriminalité est devenue l'une des insécurités les plus répandues dans nos sociétés, avec un taux de progression record. D'où l'importance d'échanger les expériences, de se former sur le sujet, comme nous le faisons avec le CyberTour. Mais au-delà de l'événement, notre think tank accompagnera des initiatives locales de proximité pour diffuser les bons réflexes, en particulier auprès des publics les moins formés face à ce fléau.

AJYLE, CATALYSEUR DE TRANSFORMATION NUMÉRIQUE ET SOCIÉTALE

La société Ajyle accompagne les organisations publiques et privées dans leur parcours de transition numérique. Samuel Cette, l'un de ses cofondateurs, nous dévoile son offre.

© Rémy Gabalda - ToulÉco

Quelles sont les spécificités d'Ajyle ?

Nous offrons des formations spécialisées, des conseils stratégiques et un accès à des compétences expertes *via* le modèle des salariés à temps partagé. En mettant l'accent sur l'IA, la cybersécurité et les technologies émergentes, nous dotons nos clients des outils et connaissances nécessaires pour naviguer dans un paysage numérique en constante évolution, donc instable.

Comment Ajyle intègre-t-elle les aspects de cybersécurité et de sécurité économique dans ses services de conseil et de formation ?

À travers des formations dédiées, des audits de sécurité et des conseils stratégiques pour renforcer la résilience des organisations face aux menaces numériques, à l'augmentation des attaques ciblées, à l'émergence de nouvelles formes de malwares.

Quelles motivations vous poussent à participer au CyberTour ?

En participant au CyberTour, Ajyle cherche à sensibiliser davantage les organisations aux enjeux de la cybersécurité, partager son expertise, raison pour laquelle nous axons nos interventions sur la transmission d'un message clair et la présentation de solutions concrètes pour y faire face.

> **La mesure de l'efficacité s'envisage, […] cela est unique, sur le suivi longitudinal des incidents de sécurité.**

Quelle approche adoptez-vous pour former et sensibiliser les organisations et leurs collaborateurs à la cybersécurité et à la sécurité économique ?

Notre approche repose sur des programmes obligatoirement sur mesure, des ateliers pratiques et des séminaires interactifs, conçus pour engager et acculturer les participants. La mesure de l'efficacité s'envisage, certes, à travers des évaluations avant et après formation, des retours d'expérience, mais surtout, et cela est unique, sur le suivi longitudinal des incidents de sécurité.

Cyber'Occ

Hacker éthique :
Professionnel de la cybersécurité qui utilise ses compétences pour détecter et corriger les vulnérabilités des systèmes informatiques de manière légale. Son objectif ? Améliorer la sécurité en identifiant les failles avant les cyberattaques. Il agit avec l'autorisation des propriétaires des systèmes.

POINT DE VUE « LE MONDE CHANGE ET SE REFERME »

Par Baptiste Robert,
PDG de Predicta Lab, start-up toulousaine spécialisée dans l'OSINT, « hacker éthique » et chercheur en cybersécurité.

© PredictaLab

L'utopie initiale

Dès ses premières heures, Internet s'est érigé autour de principes fondamentaux comme le partage de ressources, la culture de l'échange et la liberté d'expression. Cet idéal libertaire portait en lui les espoirs d'une société mondiale connectée, ouverte et libre.

La situation actuelle

55 ans plus tard, le paysage a changé. L'utopie libertaire des débuts s'est muée en une toile tentaculaire aux multiples facettes. Loin de l'esprit originel, certains États, tels que la Chine, ont cloisonné leur Internet. En verrouillant l'infrastructure et en façonnant un écosystème numérique autonome, elle a créé ses propres géants du web, indépendants de l'Internet mondial. Sur fond de tensions internationales, notamment avec le conflit en Ukraine, la Russie s'apprête à suivre cette voie en créant son propre réseau, le Runet, marquant ainsi sa « sécession » numérique. Le cyberespace est désormais devenu un champ de bataille stratégique, une composante essentielle de la guerre dite « hybride ».

> **Assurer la protection de nos organismes publics et de nos entreprises privées ne sera plus une option, mais une nécessité impérieuse.**

Des nations comme la Corée du Nord exploitent les attaques cybernétiques pour cibler les plateformes de cryptomonnaies et contourner ainsi les sanctions internationales qui leur sont imposées. La Russie utilise les capacités cyber pour mener des opérations de guerre informationnelle, pour manipuler l'opinion publique et déstabiliser ses adversaires.

Quel avenir pour Internet ?

À l'ère de la numérisation généralisée, la cybersécurité représente un enjeu économique majeur. Assurer la protection de nos organismes publics et de nos entreprises privées ne sera plus une option, mais une nécessité impérieuse. Les attaques incessantes qui visent nos entreprises, qu'elles soient motivées par des intérêts financiers ou par des objectifs de renseignement économique, constituent et continueront de constituer une menace sérieuse pour la souveraineté de notre pays. Sur le plan sociétal, la lutte contre la désinformation doit devenir une priorité absolue, car elle érode les fondements mêmes de nos démocraties. Pour garantir une sécurité à tous les niveaux, la réponse devra être collective et globale. Quelle que soit la profession, la vigilance cyber doit s'imposer comme un réflexe quotidien. Il est impératif de renforcer la sensibilisation dès le plus jeune âge, dans les écoles, et de poursuivre cet effort au sein des entreprises. L'État doit non seulement jouer un rôle de régulateur, mais aussi d'accompagnateur, en fournissant aux sociétés les moyens nécessaires pour renforcer leur sécurité numérique.

CPME 31, « REPRENDRE LE CONTRÔLE »

France Charruyer a fondé au sein de la CPME 31* la Commission sécurité économique. Entretien.

© DR

Pourquoi la CPME 31 s'est-elle saisie des questions de cybersécurité ?

Le braquage mondial des données avec l'IA générative (ChatGPT-3 et son million d'utilisations par jour), sans aucun garde-fou en termes de cybersécurité, de propriété intellectuelle, de désinformation, etc., met à rude épreuve les entreprises. Notre but est de les sensibiliser sur les cyber-risques et de les accompagner dans la sécurisation et la valorisation de leurs actifs immatériels.

Comment accompagnez-vous les PME ?

Nous avons rejoint le groupe de travail ImpactCyber *(voir p. 4)* pour remplir 3 missions : mener une enquête sur le rapport des TPE/PME à la cybersécurité, conduire une campagne de sensibilisation et rédiger un mémento à destination des TPE/PME. Nous avons aussi signé un partenariat avec Cyber'Occ pour irriguer les bonnes pratiques et démystifier la cybersécurité. La CPME s'est également engagée au sein de cybermalveillance.gouv.fr pour représenter les utilisateurs chefs d'entreprise et les faire bénéficier d'informations claires *via* une plateforme dédiée, mais aussi pour qu'ils puissent obtenir de l'aide en cas de suspicion d'attaque. Enfin, nous travaillons avec des acteurs du monde de l'entreprise et membres actifs de la CPME, des prestataires techniques locaux dans l'OSINT ou la protection et valorisation des données, des avocats, des délégués à la protection des données, des sociétés en ingénierie informatique…

> **[…] la protection des données : il s'agit d'un capital à protéger et sur lequel les organisations doivent investir.**

Quels enjeux pour les PME en 2025 ?

Celui de vigilance et de modestie face à des systèmes complexes, *a fortiori* lorsqu'ils sont dopés à l'IA. Elles devront veiller à la légalité de leurs cas d'usage et à une utilisation responsable et durable. L'hyperconnexion des organisations, notamment avec l'extension de l'iot ou du cloud, croisée avec l'évolution des technologies comme l'IA, ouvrira sans aucun doute le champ des cyberattaques, mais aussi le champ des possibles. Face à ces défis, la CPME souhaite contribuer à faire de nos entrepreneurs des entrepreneurs de la donnée et à privilégier des solutions souveraines et soutenables dans le respect du droit des personnes.

*Confédération des petites et moyennes entreprises de Haute-Garonne

L'INFO EN +

Les autres formes de phishing

- **Le phishing à ciblage étroit (*spear phishing*)** vise des individus ou des organisations spécifiques avec des messages particulièrement personnalisés pour augmenter les chances de succès. Exemples : attaques de médias comme celle contre TV5 Monde en 2015, le piratage de la campagne présidentielle française de 2017 ou encore les atteintes à la sécurité des données des hôpitaux.
- **L'hameçonnage vocal (*vishing*)** est pratiqué par téléphone. Les attaquants utilisent des techniques d'ingénierie sociale pour extorquer des informations personnelles, financières ou de sécurité à leurs victimes, souvent en se faisant passer pour des institutions de confiance. Exemples : l'arnaque au support technique, les fausses alertes de fraude bancaire, les offres d'investissement frauduleuses…
- **Le smishing (*SMS phishing*)** utilise les messages texte comme vecteurs d'attaque pour tromper les destinataires en leur faisant divulguer des informations sensibles ou en les poussant à cliquer sur des liens malveillants *via* leur téléphone mobile.

Quelques conseils pratiques de notre **expert Ajyle.**

CRÉER UN MOT DE PASSE SÉCURISÉ

C'EST VOTRE PREMIÈRE LIGNE DE DÉFENSE !

Les mots de passe faibles et répétitifs sont l'une des principales failles exploitées par les cybercriminels pour accéder à vos données en ligne. Quelques conseils à suivre !

COMBIEN DE TEMPS POUR CRAQUER VOTRE MOT DE PASSE ? (En 2023)

NOMBRE DE CARACTÈRES	Uniquement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Lettres minuscules et majuscules + chiffres	Lettres minuscules et majuscules + chiffres + caractères spéciaux
4	immédiat	immédiat	immédiat	immédiat	immédiat
6	immédiat	immédiat	immédiat	3 secondes	5 secondes
8	immédiat	5 secondes	22 minutes	1 heure	5 heures
10	immédiat	58 minutes	1 mois	2 mois	5 ans
12	45 secondes	3 semaines	230 ans	2 000 ans	34 000 ans
14	45 minutes	51 ans	800 000 ans	9 000 000 années	200 000 000 années

LES BONNES PRATIQUES

1. UTILISEZ UN MÉLANGE DE LETTRES, CHIFFRES ET SYMBOLES

POURQUOI C'EST IMPORTANT
L'utilisation d'une combinaison de différents types de caractères rend votre mot de passe beaucoup plus difficile à deviner ou à craquer par des attaques automatisées. Les attaquants utilisent souvent des outils qui génèrent des combinaisons basées sur des mots de passe couramment utilisés, des séquences simples ou des dictionnaires. En mélangeant les lettres (majuscules et minuscules), les chiffres et les symboles, vous créez une barrière supplémentaire contre ces méthodes d'attaque.

COMMENT PROCÉDER
Assurez-vous que chaque mot de passe contient une combinaison aléatoire de majuscules (A-Z), de minuscules (a-z), de chiffres (0-9) et de symboles spéciaux (comme !, @, #, $, etc.). Évitez les séquences prévisibles et les mots complets.

2. CHOISISSEZ UN MOT DE PASSE D'AU MOINS 12 CARACTÈRES

POURQUOI C'EST IMPORTANT
La longueur du mot de passe est un facteur crucial dans sa sécurité. Plus un mot de passe est long, plus le nombre de combinaisons possibles augmente, ce qui rend la tâche de le deviner ou de le craquer extrêmement difficile pour les attaquants.

COMMENT PROCÉDER
Pour vous aider à créer et à retenir des mots de passe longs, vous pouvez utiliser des phrases de passe, qui sont des suites de mots formant une phrase que vous pouvez facilement mémoriser, tout en étant difficile à deviner pour quelqu'un d'autre.

3. ENVISAGEZ UN GESTIONNAIRE DE MOTS DE PASSE POUR LES STOCKER DE MANIÈRE SÉCURISÉE

POURQUOI C'EST IMPORTANT
Avec le grand nombre de comptes en ligne que la plupart des gens possèdent, il devient pratiquement impossible de se souvenir de mots de passe uniques et complexes pour chacun d'eux. Les gestionnaires résolvent ce problème en stockant tous vos mots de passe dans une base de données chiffrée, accessible *via* un mot de passe principal.

COMMENT PROCÉDER
Choisissez un gestionnaire réputé qui offre un chiffrement robuste (comme AES-256). Vous aurez seulement à retenir le mot de passe principal pour accéder à votre coffre-fort de mots de passe. Assurez-vous que celui-ci est extrêmement fort et unique. Ces gestionnaires peuvent également générer des mots de passe forts et uniques pour vous, assurant que chaque compte soit sécurisé au mieux.

57 % des utilisateurs **indiquent noter leurs mots de passe sur un petit papier**

62 % ont déjà **partagé un mot de passe par e-mail**

44 % ont **« recyclé » leur mot de passe** suivant leurs données personnelles

Source : Keeper

UN PEU D'HISTOIRE…

La 1re utilisation documentée d'un mot de passe remonte à l'Antiquité, avec le cheval de Troie. Selon le récit, pour s'assurer que seuls les Grecs pouvaient entrer dans le cheval construit pour s'infiltrer dans Troie, les soldats utilisaient un mot de passe en frappant sur la structure selon un code précis.

L'INFO EN +

Et le mot de passe du Wi-Fi ?

Protéger votre réseau domestique est crucial pour la sécurité de vos dispositifs connectés. Une des règles est de **changer le nom et le mot de passe par défaut de votre réseau Wi-Fi**.

Pourquoi ? Parce que les noms (SSID) et mots de passe par défaut des réseaux Wi-Fi sont souvent génériques et peuvent être facilement devinés ou trouvés en ligne. En les modifiant, vous réduisez le risque d'accès non autorisé à votre réseau.

Comment ? C'est très simple :

- Accédez à l'interface administrateur de votre routeur, généralement *via* une adresse IP indiquée sur le routeur ou dans le manuel d'utilisation.
- Recherchez les paramètres Wi-Fi pour changer le SSID (nom du réseau). Choisissez un nom qui ne révèle pas directement votre identité ou votre emplacement.
- Modifiez le mot de passe du Wi-Fi en suivant les bonnes pratiques de création de mots de passe forts et uniques.

ADOPTEZ LES BONS REFLEXES !

Sessions de surf, attention !

On ne le dira jamais assez : quand vous naviguez sur le web, évitez certains comportements qui vous exposent à des **risques importants**, comme utiliser des mots de passe faibles ou identiques, mais aussi **partager des informations personnelles sur des réseaux non sécurisés**. Lorsque vous utilisez des réseaux Wi-Fi publics ou non sécurisés, vos données ne sont pas chiffrées et des individus malintentionnés peuvent potentiellement intercepter les informations que vous envoyez ou recevez, comme vos mots de passe !

Ainsi, il faut :

- Éviter d'utiliser des réseaux Wi-Fi publics pour des transactions ou communications sensibles. Si vous devez absolument vous connecter, envisagez d'utiliser des données mobiles pour des tâches impliquant des informations confidentielles.
- Utiliser un VPN (*virtual private network*) lorsque vous accédez à Internet *via* un réseau public. Voir page suivante.
- Vérifier les paramètres de sécurité du réseau avant de vous connecter. Optez pour des réseaux qui exigent un mot de passe et offrent un chiffrement.

LES MISES À JOUR

COMMENT CONTRIBUENT-ELLES À MA SÉCURITÉ ?

Les mises à jour des appareils contiennent souvent des correctifs pour les vulnérabilités de sécurité récemment découvertes.

LES BONNES PRATIQUES

1. ACTIVEZ LES MISES À JOUR AUTOMATIQUES POUR VOTRE SYSTÈME D'EXPLOITATION ET VOS APPLICATIONS

POURQUOI C'EST IMPORTANT
Les mises à jour des logiciels incluent souvent des correctifs de sécurité pour les vulnérabilités récemment découvertes qui pourraient être exploitées par des cybercriminels. En activant les mises à jour automatiques, vous vous assurez que votre système d'exploitation et vos applications bénéficient des dernières protections sans délai.

COMMENT PROCÉDER
- Pour le système d'exploitation, accédez aux paramètres de mise à jour de votre système. Sur Windows, vous pouvez trouver cette option dans « Paramètres » puis « Mise à jour et sécurité ».
- Sur macOS, recherchez « Réglages Système » puis « Mise à jour logicielle ». Activez l'option pour installer automatiquement les mises à jour du système.
- Pour les applications sur PC, vérifiez les préférences ou les paramètres de chacune pour activer les mises à jour automatiques.
- Pour les applications mobiles, vous pouvez généralement configurer cela dans le magasin d'applications de votre appareil (comme l'App Store pour iOS ou Google Play pour Android), leur permettant ainsi de se mettre à jour automatiquement lorsqu'une nouvelle version est disponible.

2. REDÉMARREZ RÉGULIÈREMENT VOS APPAREILS POUR APPLIQUER LES MISES À JOUR

POURQUOI C'EST IMPORTANT
Bien que certaines mises à jour puissent être appliquées en arrière-plan sans nécessiter de redémarrage, de nombreuses mises à jour importantes, en particulier celles du système d'exploitation, requièrent de redémarrer l'appareil pour finaliser leur installation. Cela assure qu'elles sont toutes correctement appliquées et que les correctifs de sécurité prennent effet immédiatement.

COMMENT PROCÉDER
- Planifiez des redémarrages réguliers en définissant une routine pour redémarrer vos appareils, par exemple une fois par semaine. Cela peut être particulièrement pertinent pour les ordinateurs que vous utilisez quotidiennement. Pour les appareils mobiles, profitez des redémarrages suggérés par les mises à jour du système ou redémarrez-les manuellement de temps en temps.
- N'ignorez pas les notifications ! Lorsque votre système d'exploitation indique qu'un redémarrage est nécessaire pour appliquer une mise à jour, ne le reportez pas indéfiniment. Planifiez-le à un moment qui vous convient, ou laissez-le se faire automatiquement pendant les heures où vous n'utilisez pas activement votre appareil.

5 entreprises sur 6
déclarent **ne pas disposer de moyens spécifiques** pour la sécurité de leur système d'information.

94 %
des failles de sécurité sont le fruit d'**erreurs humaines**.

Source : BusinessDIT

DÉFINITIONS

Système d'exploitation
Aussi abrégé OS en anglais et SE en français, c'est un logiciel qui assure la gestion des ressources matérielles d'un ordinateur (processeur, mémoire, interface utilisateur, fichiers, périphériques, etc.) et permet l'exécution des programmes et des applications. C'est le pilier fondamental de tout système informatique.

VPN (*virtual private network*)
Un réseau privé virtuel renforce votre confidentialité en ligne et sécurise vos connexions. Sans VPN, vos activités en ligne peuvent être facilement suivies par les fournisseurs de services Internet, les annonceurs et même les cybercriminels, car votre adresse IP réelle est exposée. Vos données personnelles et votre historique de navigation risquent d'être compromis. En bonus : un VPN vous donne l'accès à des contenus en ligne dont certains pays ou fournisseurs de services Internet limitent l'accès, en contournant les restrictions géographiques !

L'INFO EN +

Protéger votre réseau domestique

C'est crucial pour la sécurité de vos dispositifs connectés : changer le nom et le mot de passe par défaut de votre réseau Wi-Fi (voir p. 7) est nécessaire, mais ça ne suffit pas.

1. ACTIVEZ LE CHIFFREMENT WPA3 SUR VOTRE ROUTEUR
Pourquoi ? WPA3 est la dernière norme de sécurité pour les réseaux Wi-Fi, offrant une meilleure protection contre certaines attaques par rapport aux versions précédentes comme WPA2.
Comment ?
• Vérifiez si votre routeur supporte WPA3. Pour cela, consultez la documentation de votre routeur ou recherchez son modèle en ligne.
• Accédez à l'interface administrateur de votre routeur puis aux paramètres de sécurité Wi-Fi.
• Sélectionnez WPA3 comme méthode de chiffrement. Si vos appareils ne supportent pas cette norme, vous pourriez avoir besoin d'utiliser un mode mixte (WPA2/WPA3), mais visez à ce qu'à terme, tous les appareils soient compatibles avec WPA3.

2. UTILISEZ UN RÉSEAU VPN POUR CHIFFRER VOTRE TRAFIC INTERNET
Pourquoi ? Un VPN crypte votre trafic Internet, empêchant ainsi les autres de voir les informations que vous envoyez ou recevez, même sur les réseaux Wi-Fi publics non sécurisés, vulnérables aux attaques de type « homme du milieu ».
Comment ?
• Choisissez un fournisseur VPN réputé qui respecte une politique stricte de non-conservation des journaux d'activités et offre un cryptage fort.
• Installez l'application VPN fournie par votre fournisseur sur tous vos appareils.
• Activez le VPN chaque fois que vous vous connectez à Internet, surtout si vous êtes sur un réseau Wi-Fi public. La plupart des fournisseurs proposent des options pour connecter automatiquement vos appareils lorsque vous accédez à de nouveaux réseaux Wi-Fi.

Le *Journal de la cyber* est édité par **Projet X** - N° 31 (* numéro bêta) – octobre 2024
Directeur de la publication : Samuel Cette
Comité éditorial : Jean-Christophe Arguillère, Samuel Cette, Lou Estrade, Ingrid Gautier, Martin Venzal
Rédaction, création graphique et maquette : Adonis Créative – **Impression :** Techni Print imprimerie
PEFC 10-31-1286
projet X
Cyber TOUR
Flashez-moi pour la version numérique !