PROSELIS
L'INFORMATIQUE À LA DEMANDE

Guide de la cybersécurité

Prévention et bonnes pratiques

Microsoft 365

STORMSHIELD

eset
Digital Security
Progress. Protected.

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

La cybersécurité : un enjeu majeur pour toutes les entreprises

Christophe Dupont-Huin,

Administrateur et président de Proselis

L'évolution croissante des besoins en ressources numériques des entreprises accélérée par la période de crise sanitaire et l'avènement de technologies IoT a profondément accru les risques cyber.
Identifier la menace, anticiper et prévenir par la mise en place d'une politique de cybersécurité robuste et agile est dorénavant indispensable pour toute entreprise, quelle que soit sa taille et son domaine d'activité.

Depuis 20 ans, Proselis accompagne les entreprises dans la conception, le maintien et la sécurisation de leurs infrastructures informatiques. Notre expertise et nos compétences sont reconnues par l'obtention du label ExpertCyber de l'AFNOR.
Accompagner les entreprises dans leur stratégie de cybersécurité, c'est aussi communiquer, informer et partager les bonnes pratiques afin de mieux prévenir les risques ; c'est l'objet de ce livre blanc !

LES 3 PILIERS DE LA CYBERSÉCURITÉ 01

1 Conformité IT :

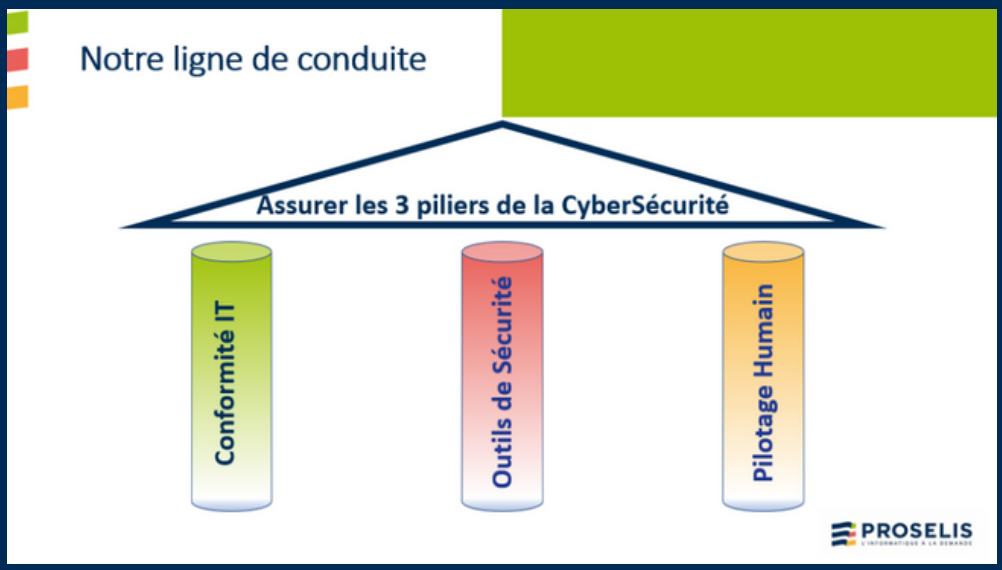
Il y a plusieurs façons d'installer un serveur, mais il n'y en a qu'une qui respecte ‘'les règles de l'art'' et qui garantit au client de ne pas avoir un serveur qui soit une faille de sécurité à lui seul

2 Outils de sécurité :

Ils sont importants pour la sécurisation des infrastructures de nos clients : antivirus, EDR, Firewall, Sauvegarde, Supervision, …

3 Pilotage Humain :

Sans pilotage humain, les outils de sécurité ne peuvent pas être efficients ! le pilotage humain est essentiel (et c'est pour cela que Proselis a créé son équipe de services managés)



PROSELIS
L'INFORMATIQUE À LA DEMANDE

CYBER-RISQUES DÉFINITION

02

Les cyber risques, que l'on peut également appeler risques informatiques ou risques numériques, font référence aux menaces potentielles pour la sécurité et la confidentialité des systèmes informatiques, des réseaux et des données.

Ils englobent les vulnérabilités et les attaques telles que les cyberattaques, le vol de données, les logiciels malveillants, les attaques de phishing et autres actions malveillantes qui peuvent compromettre l'intégrité, la disponibilité et la confidentialité des informations numériques.

Pour les entreprises et organisations, la gestion des cyber risques implique la mise en place de mesures de sécurité, de stratégies de prévention et de plans de réponse pour atténuer les éventuelles conséquences négatives de ces menaces.

La cybersécurité est un enjeu majeur pour les entreprises L'avancée de la technologie élève le niveau de la menace.

PROSELIS
L'INFORMATIQUE À LA DEMANDE

LES CHIFFRES DE LA CYBERSÉCURITÉ 03

28%

Les cyberattaques ont progressé de 28 % au troisième trimestre 2022, par rapport à 2021. La tendance est à l'intensification des attaques en 2023….

52% des entreprises ont déclaré au moins une cyberattaque au cours de l'année passée.

52%

60%

60% des victimes de cyberattaques sont des TPE/PME.

385 000 attaques réussies ont touché les systèmes d'information des organisations françaises en 2022

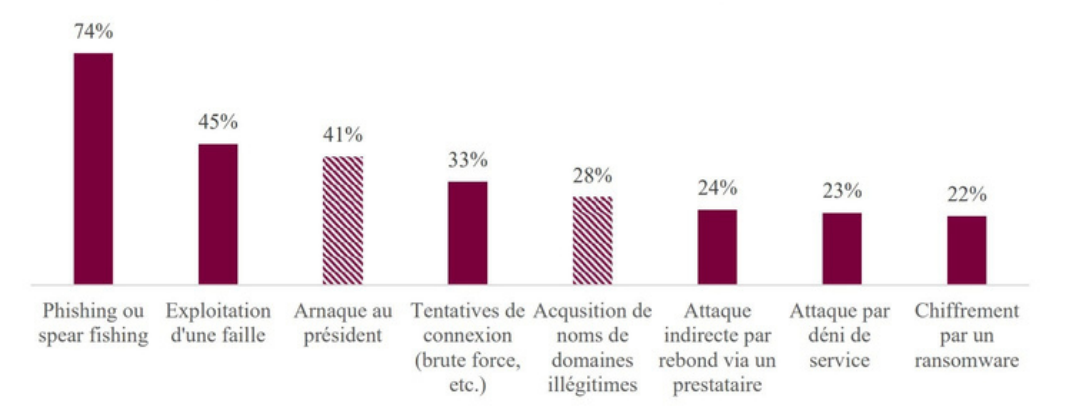
385 000
Attaques réussies

Les 5 conséquences les plus fréquentes des cyberattaques

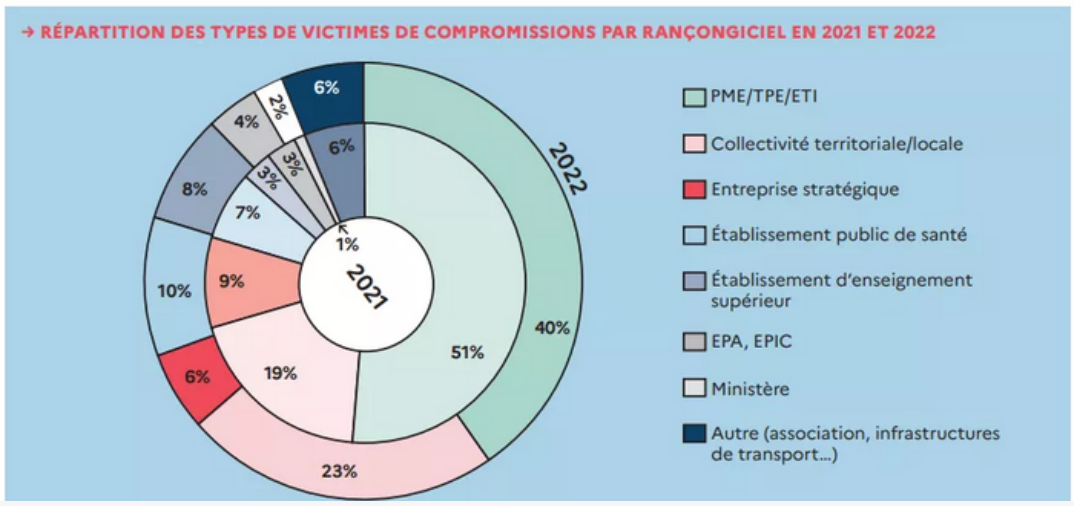
PROSELIS
L'INFORMATIQUE À LA DEMANDE

CYBERMENACES : LES TENDANCES

Les ransomwares constituent la principale menace pour les entreprises.
Les stratégies d'attaques sont de plus en plus agressives et élaborées.



Les campagnes de phishing et les escroqueries via les plateformes collaboratives comme Teams complètent le tableau attendu des cyberattaques pour 2023.
L'hypertrucage s'ajoute au panorama des nouveaux risques cyber.



04

PROSELIS
L'INFORMATIQUE À LA DEMANDE

LES CIBLES DES CYBERATTAQUANTS

Les PME en première ligne !

Les structures les plus touchées par les cyberattaques sont principalement les entreprises.
Elles représentent en effet plus de 90 % du nombre total de cyberattaques estimées au sein des organisations françaises.
Les PME qui sont particulièrement exposées (330 000 attaques recensées contre seulement 17 000 pour les grandes entreprises et ETI).

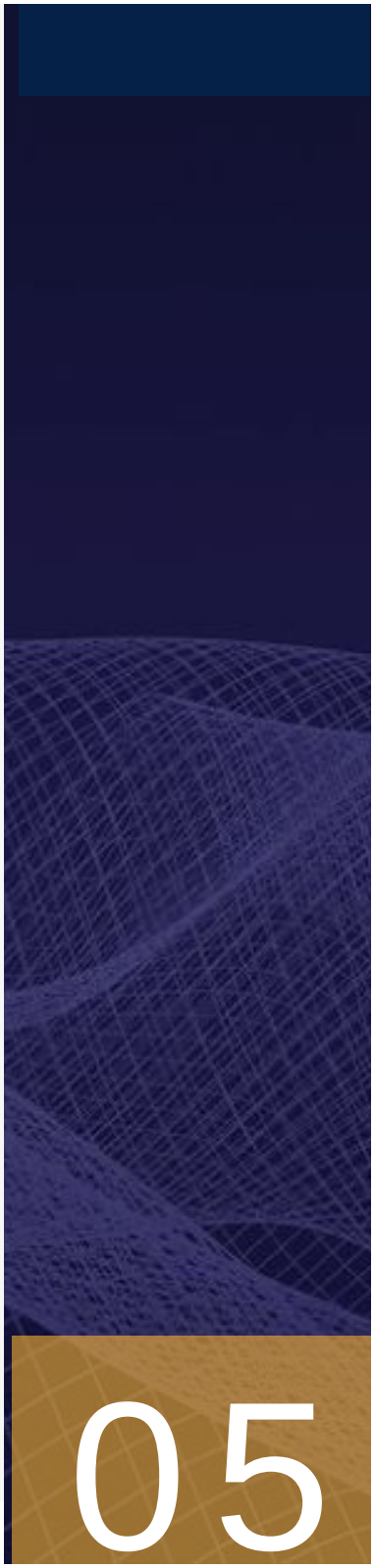
Les administrations publiques

Les administrations publiques ont essuyé 37 000 cyberattaques.
Régions, départements, communautés de communes, centres hospitaliers…
De plus en plus d'organismes publics sont touchés par des cyberattaques.
La part d'organisations publiques de 250 employés ou plus ayant été victime de cyberattaque s'élève à 51 %

Pertes de productivité et hausse des coûts de production, coût des rançons, pertes de production, dysfonctionnement des services, ralentissement de l'activité, impact sur la réputation des organisations…

Le coût d'une attaque réussie est estimé à 58 600 € en moyenne (ransmonwares inclus).

Ainsi, les cyberattaques subies en France ont généré un coût total de plus de 2 milliards d'euros en 2022 !



LES PRINCIPALES ATTAQUES 06

Le ransomware

L'attaque par ransomware est une méthode de cyberattaque où des pirates informatiques prennent en otage les données d'un ordinateur ou d'un réseau en les chiffrant. Ensuite, ils exigent une rançon, généralement en crypto-monnaie, en échange de la clé de déchiffrement qui permettra de récupérer l'accès aux données. C'est un moyen pour les cybercriminels de contraindre les victimes à payer pour récupérer leurs informations et éviter leur divulgation ou leur destruction. C’est aujourd’hui l’attaque la plus courante.

Le phishing

L'attaque par phishing est une méthode où des cybercriminels se font passer pour des entités légitimes, comme des entreprises ou des organisations connues, afin de tromper les gens et de les inciter à divulguer des informations personnelles, telles que des mots de passe, des numéros de carte de crédit ou d'autres données sensibles. Cela se fait généralement par le biais d'e-mails, de messages texte ou de sites web falsifiés qui ressemblent à ceux de sources fiables, mais qui sont en réalité conçus pour voler des informations confidentielles.

PROSELIS
L'INFORMATIQUE À LA DEMANDE

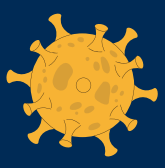
L'attaque par déni de service

L'attaque par déni de service (DDoS) est une action où des cybercriminels inondent intentionnellement un site web, un service en ligne ou un réseau avec une énorme quantité de trafic. L'objectif est de surcharger les ressources disponibles, ce qui rend le service indisponible pour les utilisateurs légitimes. Cela peut provoquer des ralentissements ou même une interruption complète du service, causant ainsi des perturbations et des problèmes d'accès pour les utilisateurs légitimes.

L'attaque de l'homme du milieu

L'attaque de l'homme du milieu est une technique où un cybercriminel s'insère discrètement entre deux parties qui communiquent, comme un utilisateur et un site web. L'attaquant intercepte et peut même modifier les informations échangées entre les deux parties, tout en faisant croire à chacune qu'elle communique directement avec l'autre. Cela permet à l'attaquant d'espionner, de voler des données sensibles ou d'altérer les communications sans que les parties impliquées ne le remarquent.

L'attaque par malware



Un malware est un logiciel malveillant, c'est-à-dire un programme informatique créé dans le but de causer des dommages à un ordinateur, un réseau ou les données qui s'y trouvent. Le terme "malware" provient de la contraction de "malicious software" (malveillant et logiciel). Les malwares incluent des types de programmes tels que les virus, les vers, les chevaux de Troie et les logiciels espions, qui peuvent infecter les systèmes informatiques et compromettre leur sécurité et leur fonctionnement normal.

L'arnaque au Président

Le principe de l’arnaque au Président est assez simple : le pirate se fait passer pour un dirigeant de l’entreprise afin d’inciter un salarié à divulguer des informations ou à réaliser une action, comme verser une somme d’argent sur le compte d’un faux client.

L'hypertrucage ou Deepfake

L'hypertrucage*, également connu sous le nom de* ***"deepfake"****, est une technique de manipulation numérique avancée qui utilise* ***l'intelligence artificielle*** *pour créer des contenus audio, vidéo ou textuels très réalistes, mais totalement falsifiés. En cybersécurité, les hypertrucages posent un risque sérieux car ils peuvent être utilisés pour créer des fausses informations, des vidéos compromettantes ou des messages trompeurs qui peuvent induire en erreur les individus ou manipuler l'opinion publique.*

Ces techniques peuvent être utilisées pour des escroqueries en ligne, des attaques de ***phishing sophistiquées,*** *des* ***campagnes de désinformation****, et même pour imiter la* ***voix ou l'apparence d'une personne*** *afin de tromper les systèmes de reconnaissance biométrique*.

L'attaque par téléchargement furtif

Cette attaque également appelée « Drive by download » consiste à diffuser un logiciel malveillant en s’insérant dans les failles de sécurité des plateformes web. Elle cible les sites insuffisamment sécurisés, les systèmes d’exploitation mal protégés, ou encore les navigateurs web qui ne sont pas à jour.

PROSELIS
L’INFORMATIQUE À LA DEMANDE

L'attaque d'authentification

Une attaque par mot de passe ou par authentification est une tentative non autorisée d'accéder à un compte, à un système informatique ou à des données en devinant ou en utilisant illégalement le mot de passe d'un utilisateur. Les attaques par mot de passe peuvent inclure des méthodes telles que le piratage par force brute (essayer de nombreuses combinaisons de mots de passe), le phishing (tromper les utilisateurs pour obtenir leurs mots de passe) ou l'utilisation de logiciels malveillants pour voler les mots de passe enregistrés sur un ordinateur. L'objectif principal de ces attaques est de prendre le contrôle du compte ou du système sans autorisation.

L'attaque par injection SQL

L'attaque par injection SQL est une technique de piratage informatique où un attaquant insère intentionnellement du code SQL malveillant dans une entrée, comme un champ de formulaire, d'une application web. L'objectif est de tromper la base de données sous-jacente pour exécuter ce code et potentiellement accéder, modifier ou supprimer des données. Cela peut permettre à l'attaquant de contourner les mécanismes de sécurité et d'obtenir un accès non autorisé aux informations stockées dans la base de données.

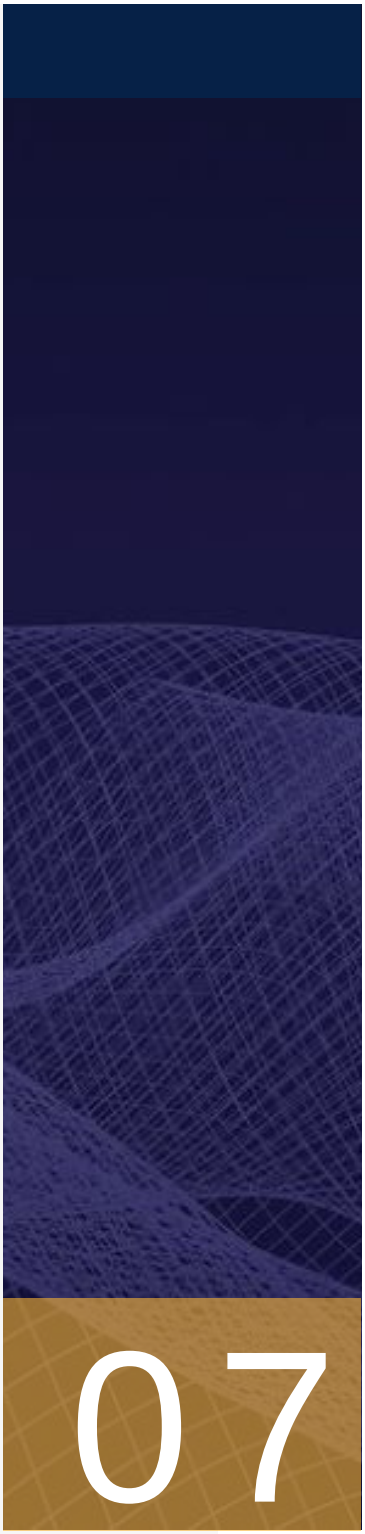
L'attaque par écoute clandestine

L’attaque par écoute illicite ou "écoute clandestine" consiste à intercepter et d'écouter des communications, telles que des appels téléphoniques, des messages texte ou des données transférées sur un réseau, dans le but d'obtenir des informations confidentielles ou sensibles.
Les pirates informatiques interceptent le trafic réseau afin d’obtenir des informations confidentielles, comme des mots de passe, des documents sensibles ou des données de paiement.

PROSELIS
L’INFORMATIQUE À LA DEMANDE

PRÉVENTION CYBER : LES BONNES PRATIQUES

La sensibilisation des collaborateurs aux bonnes pratiques en matière de numérique est indispensable pour se prémunir contre les cyber-rmenaces.
Voici quelques recommandations :



Boite mail

- N'ouvrez jamais les pièces jointes contenus dans les mails à contenu suspect (demande de virement, demande urgente…) ou provenant de destinataires inconnus
- Ne répondez jamais au mail d'un expéditeur suspect ; placez-le directement dans la corbeille
- Ne répondez jamais par mail aux demandes d'informations personnelles et confidentielles

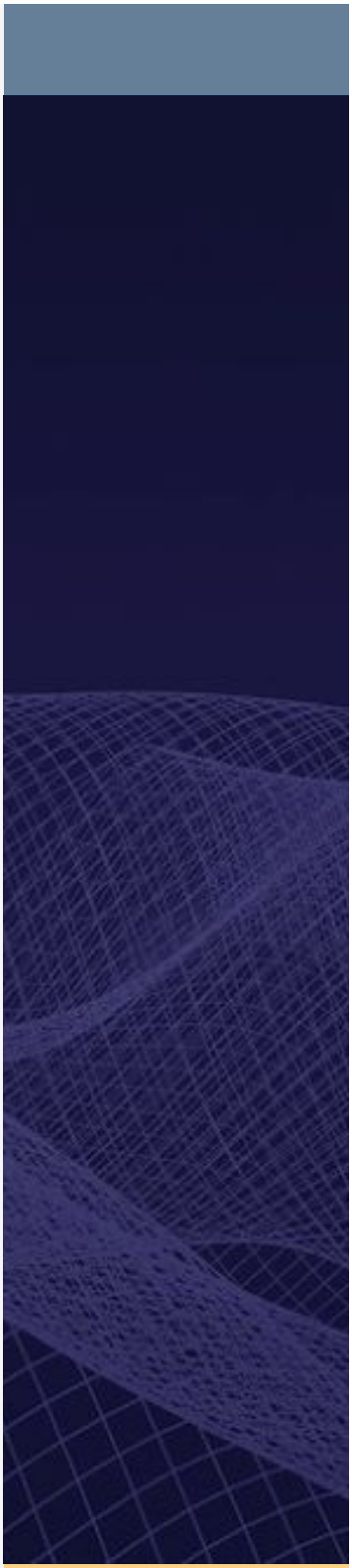
Réseaux sociaux

- Pensez à restreindre la visibilité de vos publications en modifiant la configuration de votre compte : gardez la maîtrise de votre audience en vérifiant régulièrement vos paramètres de confidentialité
- Faites preuve de discernement dans vos publications en évitant de divulguer des informations qui pourraient porter préjudice à votre entreprise
- Ne cliquez jamais sur les liens raccourcis sur les réseaux sociaux

PROSELIS
L'INFORMATIQUE À LA DEMANDE

La sauvegarde de vos données

- Effectuez régulièrement des sauvegardes de vos données en utilisant des supports externes dédiés à cet usage
- Placez tous les supports de stockage amovibles dans un coffre-fort ou dans un endroit sécurisé.
- Externalisez vos sauvegardes en ligne pour automatiser la sécurisation de vos données.
- Une sauvegarde doit être :
- Quotidienne
- Externalisée (supports externes et/ou hébergement en ligne)



Préserver ses données

Contrairement à ce que l'on pourrait penser, le recours à la solution **Microsoft 365** ne constitue en rien une garantie de sauvegarde de données.
Si Microsoft assure le bon fonctionnement de l'infrastructure, il n'est en rien responsable des données qui appartiennent à l'entreprise.
Il est donc essentiel de prendre des mesures pour préserver et sauvegarder les données de son entreprise.
Optez pour une solution qui permet de gagner du temps et de sécuriser le processus de sauvegarde des données en l'automatisant, et éliminant toute défaillance humaine.
Proselis Backup est la solution pour assurer la pérennité de votre entreprise et gagner en sérénité !

PROSELIS
L'INFORMATIQUE À LA DEMANDE

Logiciels et dispositifs techniques

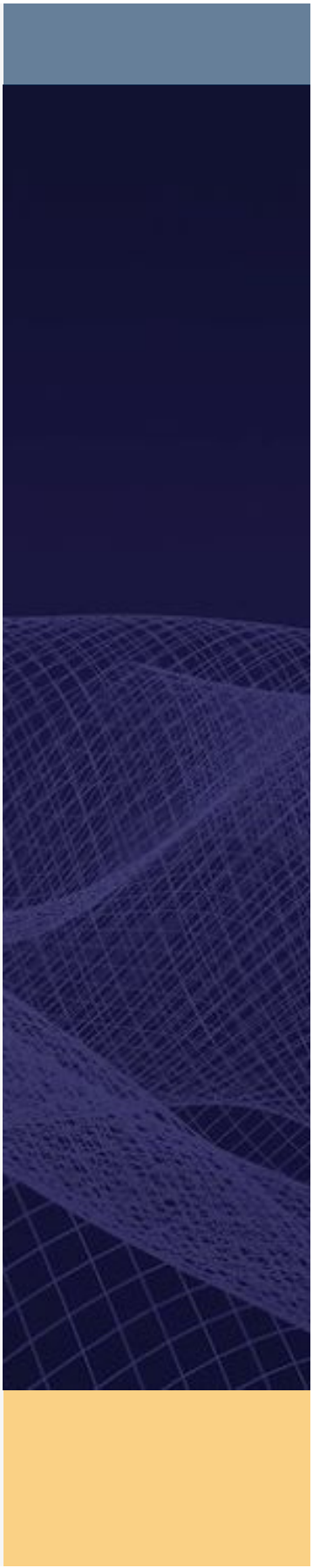
- Installez et mettez à jour régulièrement votre antivirus

  L'antivirus est un logiciel de sécurité informatique qui est conçu pur détecter, prévenir et éliminer les logiciels malveillants tels que les virus, les vers, les chevaux de Troie, les ransomwares et autres programmes malveillants susceptibles d'endommager ou perturber le fonctionnement de votre système informatique.

- Installez un pare-feu sur votre poste de travail et maintenez-le à jour

  le pare-feu ou Firewall est un dispositif de sécurité informatique qui agit comme un bouclier pour filtrer les informations qui entrent ou sortent de votre réseau informatique

- Mettez à jour votre système d'exploitation et les applications

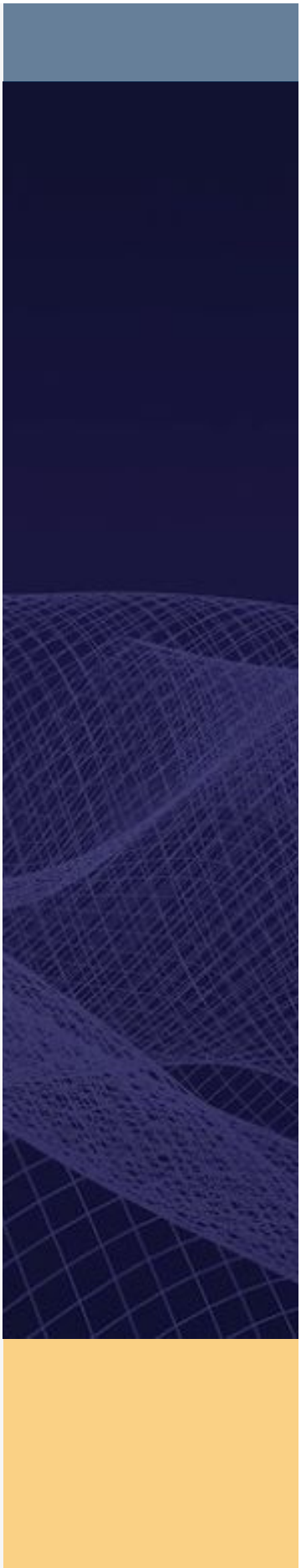


⋗ L'importance des mises à jour

La mise à jour des logiciels permet de réduire les vulnérabilités en apportant des correctifs de sécurité développés à la suite d'attaques éprouvées par l'éditeur. En effet, à chaque nouvelle version du système d'exploitation, l'éditeur corrige les éventuelles lacunes augmentant ainsi les chances d'empêcher les cybercriminels de s'introduire dans les appareils de l'entreprise. Elle permet également de renforcer les défenses en intégrant de nouvelles fonctionnalités notamment en matière d'Antivirus ; à noter que cette évolutivité est l'un des points fort des solutions **Eset** proposées par **Proselis**.

Mots de passe et gestion des accès

- Renouvelez vos mots de passe régulièrement (tous les 90 jours)
- Choisissez une combinaison d'au moins 12 caractères
- Utilisez des caractères spéciaux (majuscules, minuscules, chiffres, signes de ponctuation)
- Ne faites pas référence à vos données personnelles (date de naissance, noms et prénoms…)
- Optez pour des mots de passe différents pour chaque application ou site.
- Refusez systématiquement la mémorisation de votre mot de passe sur les sites
- Sécurisez l'accès à votre wifi via l'utilisation d'un mot de passe complexe
- Utilisez l'authentification à facteurs multiples



L'authentification multifacteur

À l'ère de la transformation numérique et du déploiement de nouveaux modes de travail plus nomades, **l'authentification multifacteur** constitue pour les organisations une solution idéale pour garantir efficacité, flexibilité et sécurité dans l'utilisation des ressources numériques par les salariés.
Selon Microsoft, l'authentification multifacteur MFA bloque en effet plus de 99,9% des attaques de compromission de compte.

PROSELIS
L'INFORMATIQUE À LA DEMANDE

*Proselis vous accompagne dans la **définition** et la **mise en œuvre** d'une stratégie de **cybersécurité** efficace !*

Proselis vous guide dans la conception et la réalisation de vos projets à travers un accompagnement personnalisé : Conseil, Installation, Maintenance, Assistance, Infogérance (dont la Supervision).

Nos équipes prennent en compte vos enjeux et vos besoins pour vous apporter des solutions adaptées et sur-mesure : Matériels, Logiciels, Hébergement.

Proselis protège votre réseau, vos données, vos flux et votre fonctionnement informatique. N'attendez pas le pire pour avoir le meilleur.

PROSELIS
L'INFORMATIQUE À LA DEMANDE

Un projet, besoin d'un conseil ou d'un accompagnement ? Contactez-nous :

ZA Porte Estuaire
44750 CAMPBON/SAVENAY

contact@proselis.com

02 40 56 29 00

PROSELIS
L'INFORMATIQUE À LA DEMANDE