# La Cybersécurité

Les bons réflexes de la Cybersécurité

ALSACE DIGITALE
CONSTRUIRE L'ÉCOSYSTÈME NUMÉRIQUE EN ALSACE

# Introduction

# La Cybersécurité

## Qu’est-ce que c’est ?

### Cyber

Tout ce qui se rapporte au réseau internet .

|

### Sécurité

Action de protéger ou défendre quelque chose .

# La Cybersécurité ?

C’est la mise en œuvre d’un ensemble de techniques et de solutions de sécurité pour protéger la confidentialité, l’intégrité et la disponibilité des informations.

Cette protection doit couvrir tout le cycle de vie des données, de leur génération et traitement, à leur transfert, stockage et élimination.

# La cyberattaque

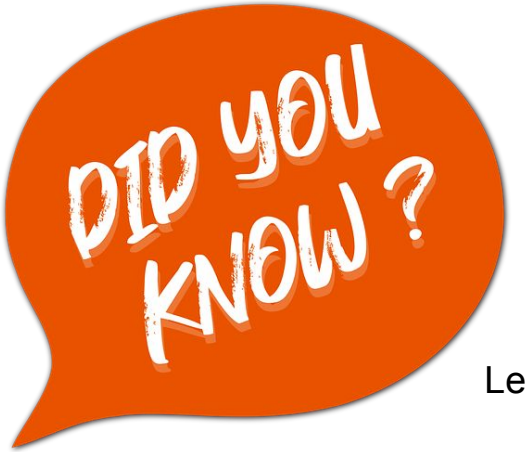
## Qu’est-ce que c’est ?

une attaque menée via **Internet** ou un autre **réseau** sur des **systèmes informatiques**, des serveurs, des réseaux ou des appareils.

Des personnes ou groupes malveillants (pirates, hackers ou cybercriminels) exploitent des failles pour perturber, accéder ou endommager des systèmes à distance.

**Leur but ?**

Voler des informations pour les effacer ou les échanger contre de l’argent.



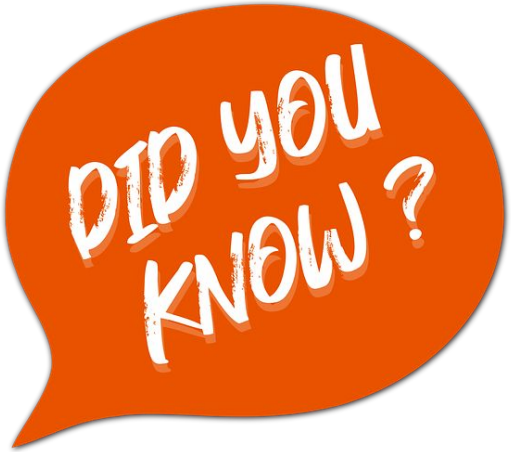

Une hausse de +400% de cyberattaques depuis le début de la crise sanitaire

Le coût des cyberattaques en France est estimé à 2 milliards d'euros en 2022

Une entreprise française sur deux est victime d’une cyberattaque

94% des logiciels malveillants sont délivrés par e-mail

# Cybersécurité en France, quelques statistiques clés !



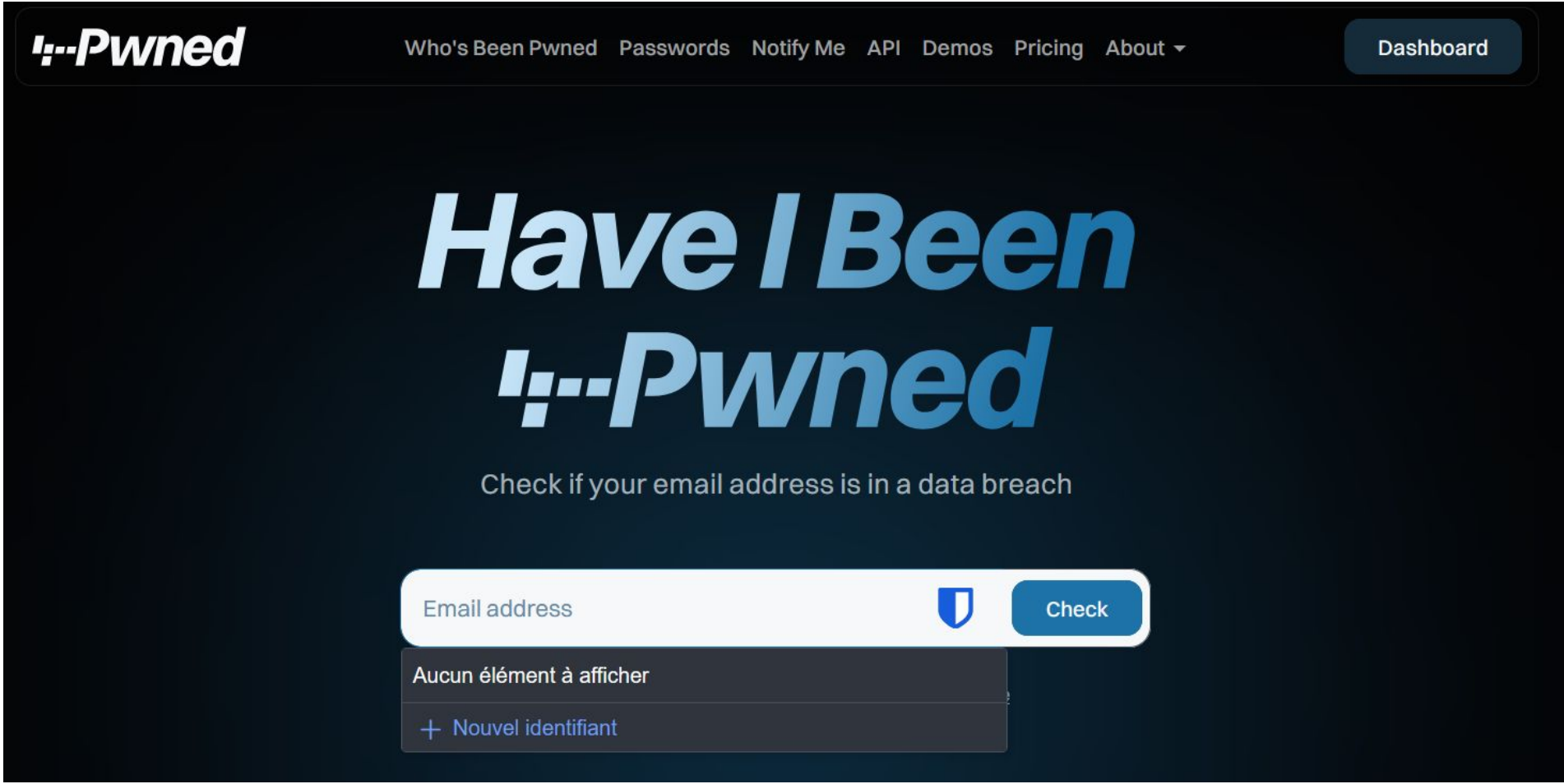

**Premier League (Angleterre)** : un dirigeant de club a failli perdre 1 million de livres après avoir saisi ses identifiants sur une fausse page email imitant un outil professionnel.

**Lazio Rome (Italie**) : le club a perdu environ 2 millions d'euros à la suite d'une fraude par email se faisant passer pour un partenaire légitime.

**Clubs européens (Espagne, etc.)** : des serveurs de clubs ont été piratés, exposant les données personnelles de membres et de supporters.

**Fédérations sportives françaises** : plusieurs millions de données de licenciés ont été volées lors de cyberattaques, puis revendues et utilisées pour du phishing ciblé.

## Chiffres


Pwned
Who's Been Pwned
Passwords
Notify Me
API
Demos
Pricing
About
Dashboard
Have I Been
Pwned
Check if your email address is in a data breach
Email address
Check
Aucun élément à afficher
Nouvel identifiant

# Les Virus

# Les Virus ?

Les Virus sont des programmes malveillants qui cherchent à perturber le fonctionnement normal d'un appareil à l'insu de son propriétaire ou à porter atteinte à ses données :

- Vol ou destruction d'informations
- Espionnage ou chantage
- Utilisation de sa machine pour en attaquer d'autres…

# Comment les virus peuvent s'infiltrer dans un système informatique ?

- En naviguant sur Internet
- En cliquant sur un lien frauduleux (Mail, MMS, Chat, SMS…)
- En ouvrant une pièce-jointe d'un message
- En branchant une clé USB…

# Les Symptômes d'une infection par un virus ?

- Des courriels étranges sont envoyés à vos contacts depuis vos compte
- Un ralentissement ou un blocage anormal de l'appareil
- Des fenêtres popup ou des messages d'erreur qui s'affichent sans raison
- La page d'accueil de votre navigateur a été modifiée etc...

# Quelques types de logiciels malveillants (malwares) informatiques ?

# Rançongiciel - (Ransomware)

Il encrypte vos fichiers,

de sorte que vous ne puissiez pas les ouvrir,

jusqu'à ce que vous payez une rançon (en général par cryptomonnaie)

# Le cheval de Troie

La machine peut être infectée :

- Après l'ouverture d'une pièce jointe
- Après avoir cliqué sur un lien malveillant reçu dans des courriels,
- En naviguant sur des sites compromis
- Installer un programme gratuit cracké

## Son objectif ?

Voler vos coordonnées bancaires, espionner, Installer d'autres malwares (ransomware, spyware...)

## Un cheval de Troie peut réaliser de nombreuses actions malveillantes :

- Télécharger d'autres virus,
- Créer des copies de lui-même pour vous faire croire que vous l'avez supprimé avec succès,
- Prendre le contrôle de votre souris,
- Voler des fichiers,
- Vous espionner à travers votre appareil photo et microphone,
- Enregistrer ce que vous tapez sur votre clavier,

**En gros, toutes les actions que vous faites sur votre ordinateur sont surveillées**

# Antivirus

# Antivirus ?

## Qu’est-ce qu’un antivirus ?

C’est un programme informatique, ou une application, qui a pour principale vocation d’identifier, de neutraliser, voire d’éliminer les virus informatiques.

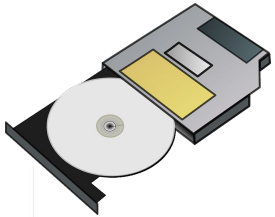
## Faut-il utiliser un antivirus ?

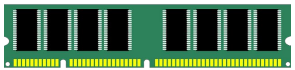
Oui.

# Comment fonctionne un antivirus ?

Après l'installation, l'antivirus se greffe sur le système d'exploitation de l'appareil.

Il permet de rechercher les virus dans ce qui peut y être stocké, y entrer ou en sortir :



## Pour cela :

L'antivirus s'appuie sur des « bases de signatures » qui contiennent des définitions ou empreintes de virus régulièrement actualisées

# Quel est le meilleur antivirus ?

Les performances et fonctionnalités des principaux antivirus du marché sont assez similaires et aucun ne peut se prévaloir d'apporter une protection à 100% efficace.




# Le Phishing

# Hameçonnage - (Le Phishing)

C’est quand quelqu’un essaie de se faire passer pour :

- Une personne que vous connaissez
- Un organisme
- Une société

**une usurpation d'identité**

# Pourquoi ?

Pour vous forcer à donner des informations personnelles :

- Votre identité
- Vos coordonnées

**Ou encore plus grave :**

- Vos coordonnées bancaires
- Votre numéro de sécurité sociale.

# Comment se protéger ?


Tout le monde peut recevoir des tentatives d’arnaques

Le plus important est de savoir reconnaître ces arnaques

Il faut faire attention aux **SMS** et **mails** que vous recevez

**Surtout**, si il y a des liens vers des sites web ou des pièces jointes.

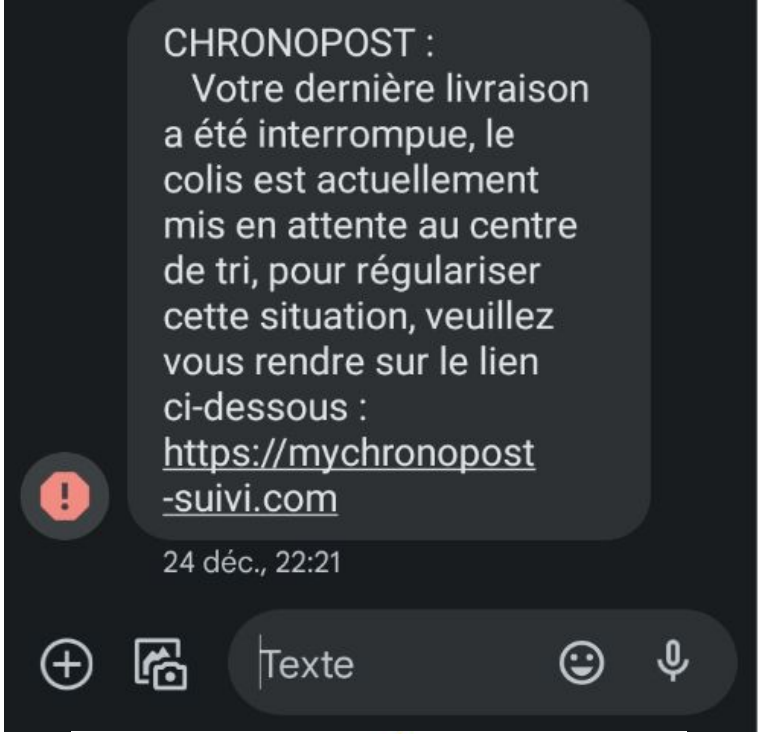
# 5 signes qui doivent vous alerter

# 1 : On a besoin d'informations

Les pirates essaient de récupérer le plus d'informations personnelles sur vous :

votre nom, prénom, date de naissance, lieu de naissance, adresse, email, numéro de téléphone.

**Ne donnez jamais d'informations personnelles lorsque la demande vient d'un mail ou d'un SMS.**




Exemple d'une tentative d'arnaque

# 2 : « Cliquez sur le lien suivant »

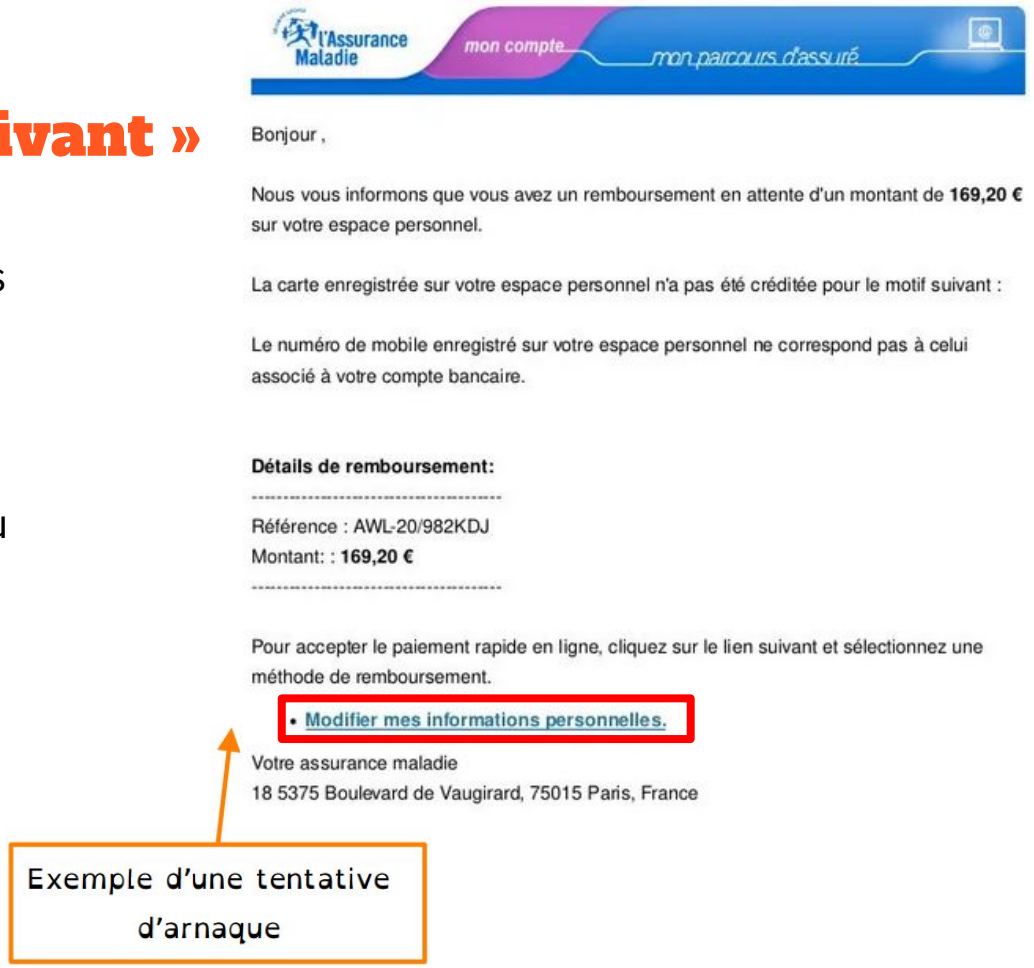
Vous devez cliquer sur un lien qui vous envoie sur un site internet.

**Attention**, ce lien est TOUJOURS faux !

Le nom du site sera presque celui du vrai site.

amelimoncomptes.fr au lieu de ameli.fr

**Ne cliquez pas sur les liens que vous recevez par mail ou SMS.**



# 3 : « Vous avez 48h »

Si vous ne répondez pas rapidement, quelque chose va se passer.

Pour l'arnaqueur, vous devez réagir vite.

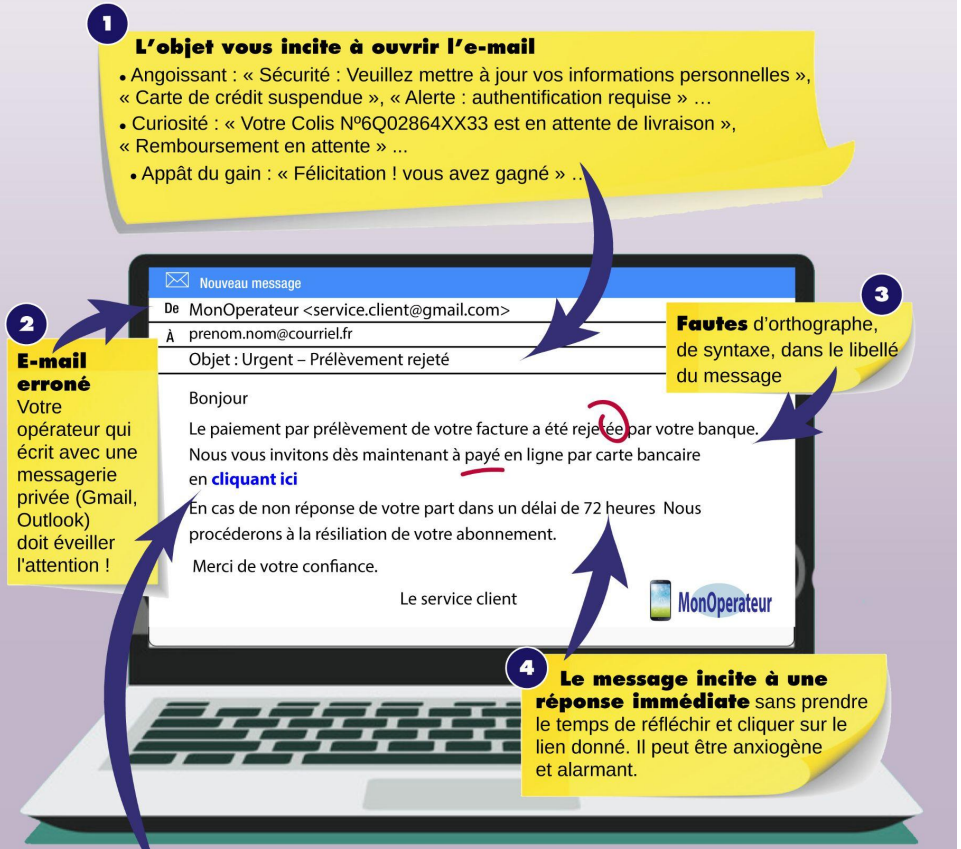
**Ne cliquez pas dans l'urgence**

# 4 : « Vous nous devez 500€ » OU « Un cadeau exceptionnel vous attend »

On vous menace de :

- Supprimer votre compte
- Vous prélever de l'argent
- Vous risquez de perdre un superbe cadeau si vous ne répondez pas

**Prenez le temps de réfléchir**


1
L'objet vous incite à ouvrir l'e-mail
• Angoissant : « Sécurité : Veuillez mettre à jour vos informations personnelles », « Carte de crédit suspendue », « Alerte : authentification requise » …
• Curiosité : « Votre Colis Nº6Q02864XX33 est en attente de livraison », « Remboursement en attente » ...
• Appât du gain : « Félicitation ! vous avez gagné » ..
Nouveau message
De MonOperateur <service.client@gmail.com>
À prenom.nom@courriel.fr
Objet : Urgent – Prélèvement rejeté
Bonjour
Le paiement par prélèvement de votre facture a été rejetée par votre banque.
Nous vous invitons dès maintenant à payé en ligne par carte bancaire
en cliquant ici
En cas de non réponse de votre part dans un délai de 72 heures Nous procéderons à la résiliation de votre abonnement.
Merci de votre confiance.
Le service client
MonOperateur
2
E-mail erroné
Votre opérateur qui écrit avec une messagerie privée (Gmail, Outlook) doit éveiller l'attention !
3
Fautes d'orthographe, de syntaxe, dans le libellé du message
4
Le message incite à une réponse immédiate sans prendre le temps de réfléchir et cliquer sur le lien donné. Il peut être anxiogène et alarmant.
5
Un lien à cliquer trompeur
Pour connaître la destination réelle du lien, passez le curseur de la souris sur le lien sans cliquer pour qu'il s'affiche. Rendez-vous ensuite sur le site officiel de l'organisme prétendument expéditeur de l'e-mail, en passant par un moteur de recherche et comparez les deux adresses. La différence peut être infime, juste une lettre qui change.

# Les mesures essentielles pour assurer votre cybersécurité

# 1. Protégez vos accès avec des mots de passe solides

**Qu’est-ce qu’un mot de passe ?**

Un mot de passe est comme une clé, qui sécurise vos espaces personnels sur internet. Il est donc personnel et confidentiel !

## Différent pour chaque service

## Suffisamment long et complexe

des majuscules **ABC**

des minuscules **abc**

des chiffres **123**

des caractères spéciaux **_?*/!**

minimum 12 caractères

## un gestionnaire de mots de passe

Keepass

Bitwarden

## impossible à deviner

123456

azerty

abcdef

**Changez votre mot de passe au moindre soupçon**

**N’utilisez pas vos mots de passe sur un ordinateur partagé**


**Ne communiquez jamais vos mots de passe à un tiers**

**Activez la « double authentification » lorsque c’est possible**

# Comment créer un mot de passe solide ?

# Première technique : les mots choisis au hasard

1. Choisir 2 ou 3 mots sans rapport
2. Mettre la première lettre en majuscule
3. Séparer les mots d'un caractère spécial
4. Ajouter un chiffre

bicyclette lionceau

**B**icyclette **L**ionceau

**B**icyclette**?L**ionceau

**B**icyclette**?L**ionceau**4**

# Deuxième technique : la phrase facile à retenir

1. Trouver une phrase longue facile à retenir

**J'ai deux enfants qui s'appellent Laura et Tom**

2. Garder uniquement la première lettre de chaque mot et les chiffres

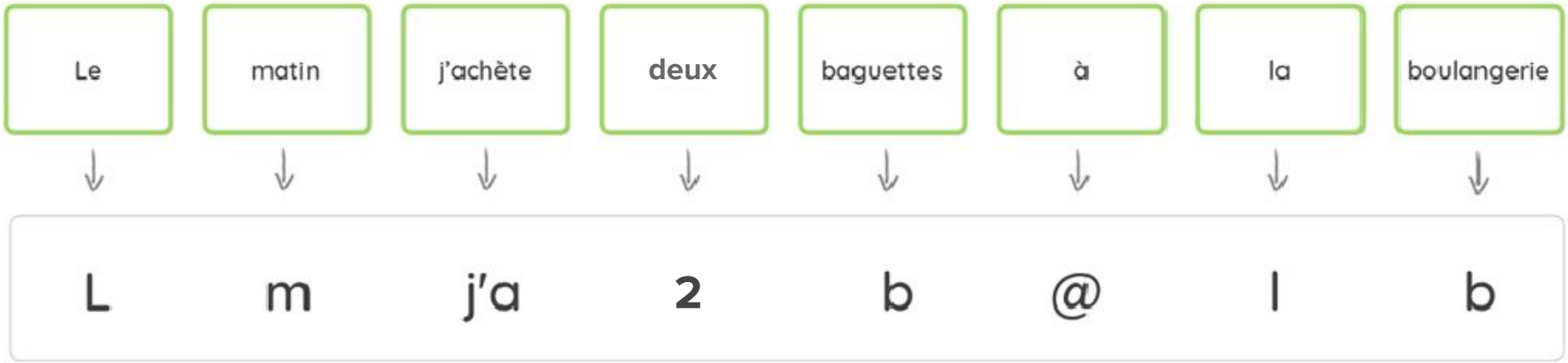
**Ja2eqsaLeT**

3. Ajouter un caractère spécial s'il n'y en a pas encore

**Ja2eqsaLeT@**

Lmj'a2b@lb

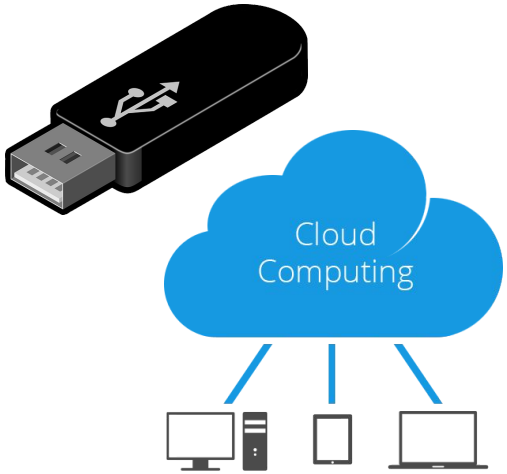
Lmj'a2b@lb



# 2. Sauvegardez vos données régulièrement

En cas :

- de piratage,
- de panne,
- de vol,
- de perte de votre appareil




**Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes**

**Conservez une copie sur un support externe (clé ou disque USB)**

# 3. Appliquez les mises à jour de sécurité

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner

# 4. Utilisez un antivirus

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus.

# 5. Téléchargez vos applications uniquement sur les sites officiels

- Microsoft Store,
- Apple App Store,
- Google Play Store

Pour limiter les risques d'installation d'une application piégée pour pirater vos équipements.

# 6. Méfiez-vous des messages inattendus

En cas de réception d’un message inattendu ou alarmiste par :

- email
- SMS
- chat

Demandez toujours confirmation à l’émetteur par un autre moyen s’il vous semble connu et légitime.

Il peut en effet s’agir d’une attaque par **(Le Phishing)**

# 7. Vérifiez les sites sur lesquels vous faites des achats

Il existe de nombreux sites de vente douteux, voire malveillants.

Avant d'acheter sur Internet : Vérifiez

- que vous n'êtes pas sur une copie frauduleuse d'un site officiel,
- la crédibilité de l'offre,
- consultez les avis


# 8. Séparez vos usages personnels et professionnels

Il est important de **séparer** vos usages numériques :

- Personnelle
- Professionnelle

**Afin que :**

- le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement,
- la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles

# 9. Évitez les réseaux WiFi publics ou inconnus

En mobilité ?

Connexion de votre abonnement téléphonique (3G, 4G, 5G) aux réseaux WiFi publics.

Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates pour capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire…).

Si vous n’avez d’autre choix que d’utiliser un WiFi public ?

Veillez à ne jamais y réaliser d’opérations sensibles.

# Le Cloud - Google Drive


**Le Drive : Notre coffre-fort partagé**

Points clés :

- **Sécurité** : Protège contre les virus qui bloquent les ordinateurs (Ransomwares).
- **Recherche** : Tapez un mot-clé, retrouvez le document (plus besoin de demander le lien 10 fois).
- **Contrôle** : On partage un lien, on n'envoie pas le fichier. On peut couper l'accès quand l'éducateur quitte le club.

# Le site Pix :

**Cultivez vos compétences numériques :**

**Pix** est le service public en ligne pour évaluer, développer et certifier ses compétences numériques.

https://pix.fr/

# Quelques Sites :

- https://www.cybermalveillance.gouv.fr/

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

- https://www.ssi.gouv.fr/

Agence nationale de la sécurité des systèmes d'information (**ANSSI**)