



La Cybersécurité

en Collectivité Territoriale

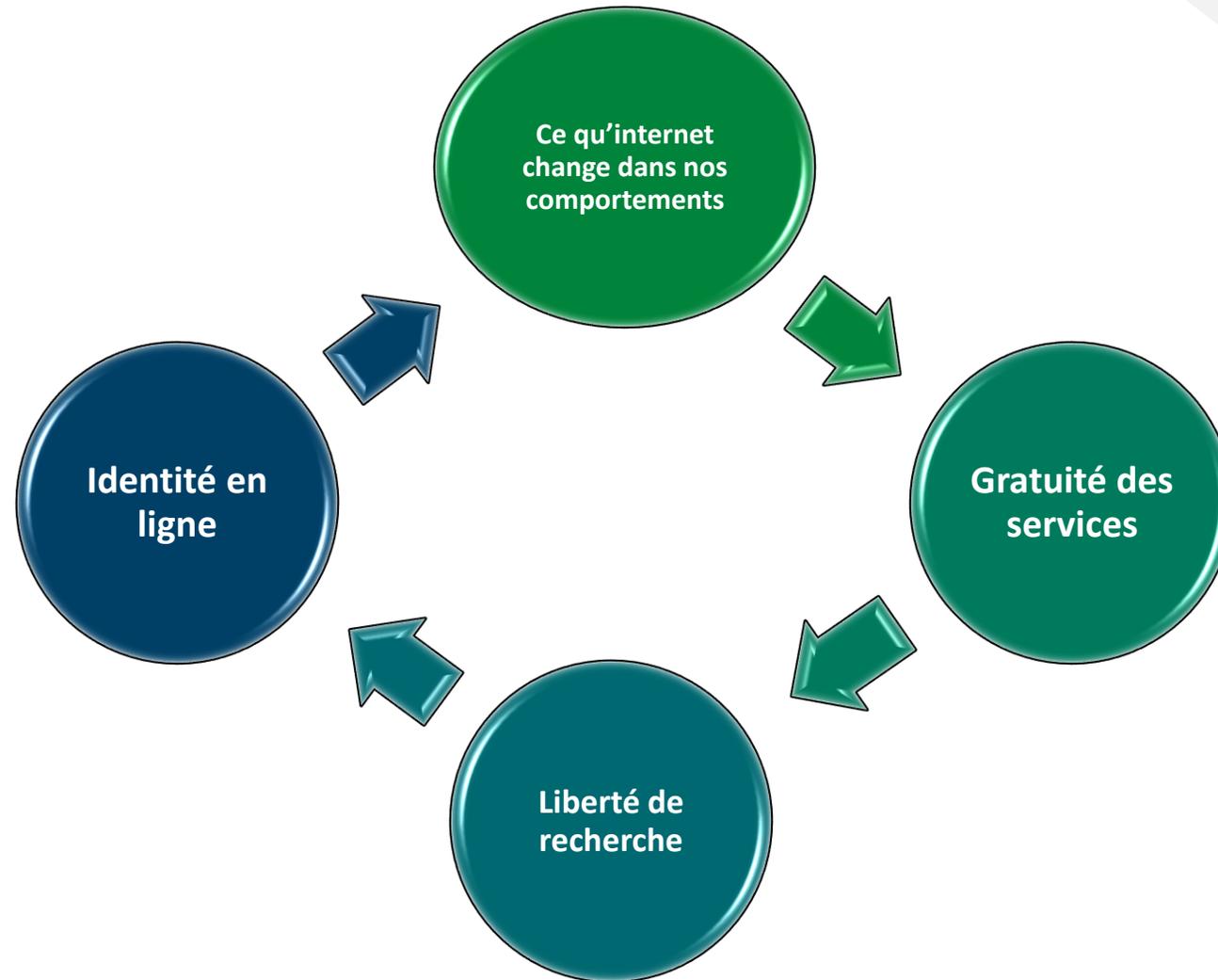




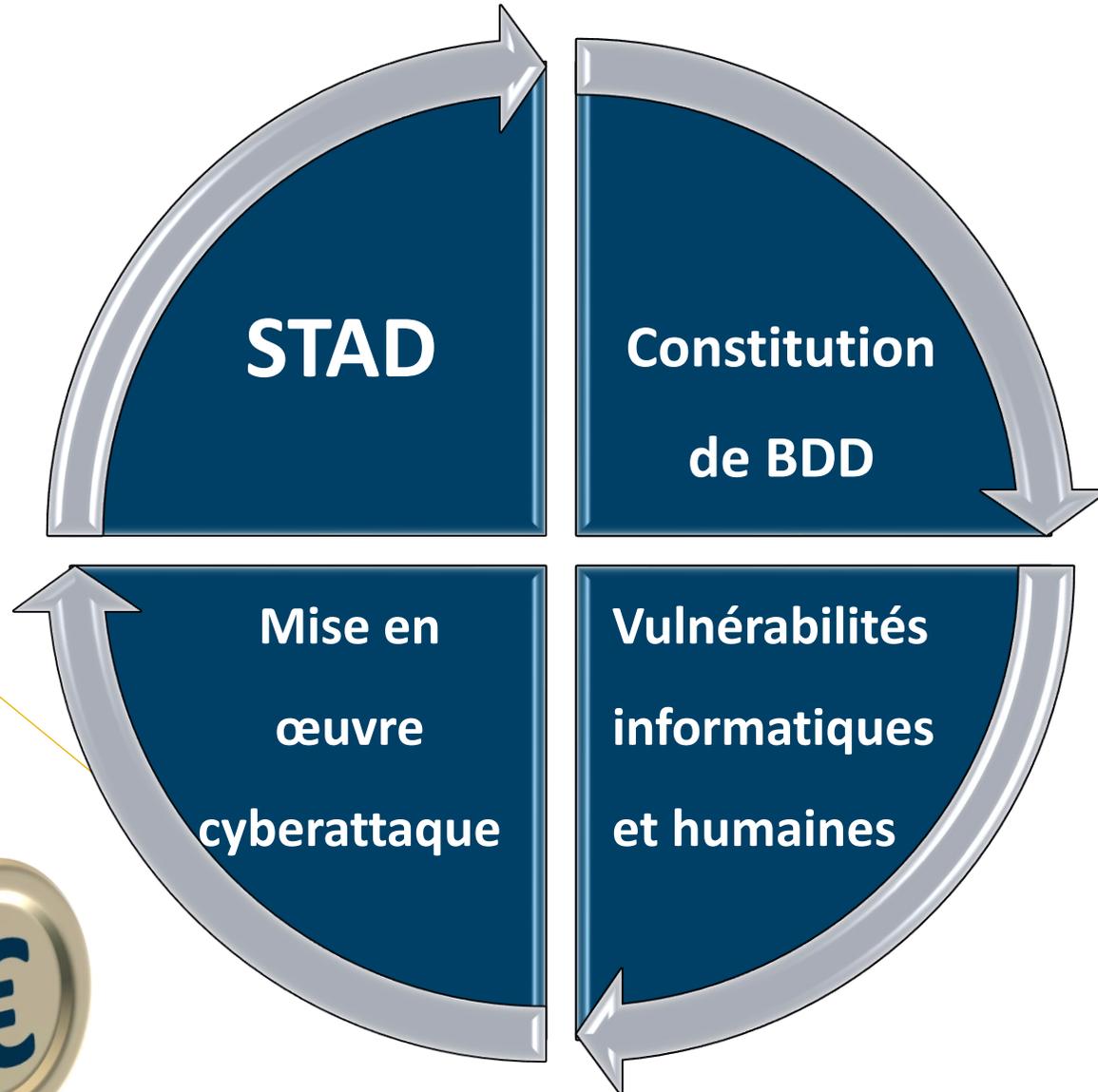
Plan de la séance

- Introduction
- Les grandes menaces cyber
- Les 10 bonnes pratiques

Internet en toute conscience



La fuite de donnée : la boucle est bouclée!



Nom	Taille	Pr
<input checked="" type="checkbox"/> twitch-leaks-part-one	125,89 Gio	N
<input checked="" type="checkbox"/> twitch-payouts	4,88 Gio	N
<input checked="" type="checkbox"/> 3rdparty.zip	15,1 Kio	N
<input checked="" type="checkbox"/> abuse.zip	3,9 Mio	N
<input checked="" type="checkbox"/> admin-services.zip	37,2 Mio	N
<input checked="" type="checkbox"/> ads.zip	1,14 Gio	N
<input checked="" type="checkbox"/> ags-sonic.zip	544,8 Mio	N
<input checked="" type="checkbox"/> amzn.zip	44,6 Mio	N
<input checked="" type="checkbox"/> andaries.zip	22,1 Kio	N
<input checked="" type="checkbox"/> archive.zip	73,2 Mio	N
<input checked="" type="checkbox"/> astith.zip	810,3 Kio	N
<input checked="" type="checkbox"/> availability.zip	239,0 Mio	N

* Have i been pwned?

RANÇONGIERE

Arnaque CPF CRYPTOJACKING piratage compte ASTAD ESCROQUERIE

Swatting FAUX SUPPORT TECHNIQUE

ARNAQUE Revenge Porn ROMANCE

SLUT SHAMMING

TROLLING FOSSE DOXING

DDOS FOVI CONVOCATION CYBER-HARCÈLEMENT

DÉNI DE SERVICE DISTRIBUÉ Défacement

ARNAQUE À LA



I. Les menaces

- 1.1 L'hameçonnage
- 1.2 Le rançongiciel
- 1.3 Le piratage de compte et l'usurpation d'identité
- 1.4 L'arnaque au faux support technique

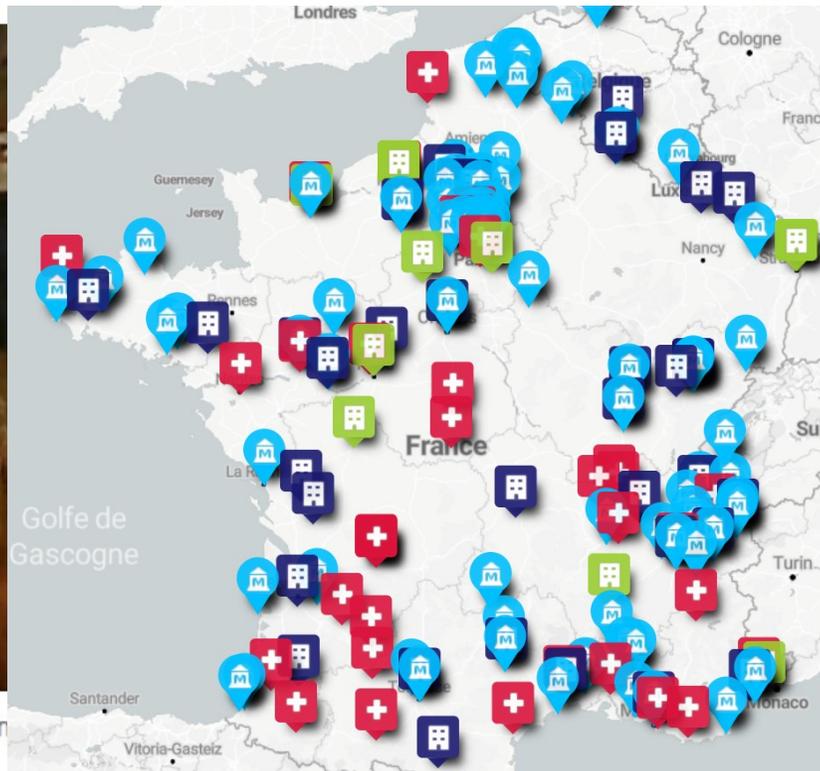
TÉMOIGNAGE. À Ploërmel, leur entreprise a subi une Elven. La commune a subi un piratage informatique

En 201
cybera
jeudi 2
d'entre

Ouest-Fran
Publié le 31/08

À Vannes, une plainte déposée après le piratage des panneaux du tunnel de Kérino

Publié le 24 janvier 2023 à 11h10 Modifié le 24 janvier 2023 à 15h26



Sur les par

Le groupe Eureden victime d'une cyberattaque

Publié le 18 mars 2022 à 10h26



nvrier 2020. (FRANÇOIS DESTOC/LE TÉLÉGRAMME)



Fuite de données clients d'Océalab



Le laboratoire Océalab va déposer plainte, par le biais de son avocat parisien, Me Gérard Haas, spécialisé dans la cybercriminalité. | OUEST-FRANCE

Hameçonnage (Phishing)

Premier vecteur pour une attaque ultérieure

The image shows a composite of three phishing messages. On the left is an email from 'Crédit Mutuel' with the subject 'AMELI - Remboursement'. The email body contains a warning about a blocked account and a link to 'Espace Client'. In the center is an SMS from 'Crédit Agricole' claiming the account is blocked and providing a link to a fake website. On the right is another SMS from 'Crédit Agricole' claiming a parcel delivery failed and providing a link to a fake website. The email header includes the Crédit Mutuel logo and the recipient's name 'AMELI - Remboursement'. The SMS messages include sender names, phone numbers, and timestamps.

Crédit Mutuel
AMELI - Remboursement

Madame, M
Vous devez connaître les conditions de votre Assurance Maladie. Avec cette assurance, vous êtes admissible à recevoir un remboursement d'un montant de 1000€.

De : **Votre Assurance Maladie** (ez895qs+eds4596s@i...)
indésirable.

Crédit Agricole
Urgent CA >

Message
Aujourd'hui 10:15

Crédit Agricole
Votre Compte a été bloqué par notre service.
Débloquez votre compte en cliquant sur le lien ci-dessous : [http://bit.do/fnw5X](#)

+33 6 17 07 70 50 >

Message
samedi 10:08

Nous avons essayé de livrer votre colis 00073679039, mais il n'y a aucun affranchissement. Suivez les instructions ici : <http://bit.do/fnw5X>

Nous vous invitons à consulter les démarches à suivre en [cliquant ici](#).

Cordialement

Ameli.fr - assurance maladie ameli 2016 France

But recherché

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...

Technique

Voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Hameçonnage (Phishing)

Premier vecteur pour une attaque ultérieure



Le rançongiciel (ransomware)

Extorsion de fonds par voie numérique



But recherché

Réclamer le paiement d'une rançon pour restaurer l'accès aux données.

Technique

Suite à un hameçonnage réussi ou par intrusion sur le système, un logiciel malveillant chiffre les données, ce qui les rend inaccessibles.



Corbeille

Vos dossiers personnels sont encryptés par le



**Vos dossiers personnels sont encryptés par le
CTB-Locker.**

Vos documents, vos photos, vos données et d'autres dossiers importants ont été encryptés avec un encodage plus fort et une clé unique, générés par cet ordinateur.

La clé privée pour décrypter est gardée dans un serveur d'Internet secret et personne ne peut décrypter vos dossiers jusqu'à ce que vous payez et obteniez la clé privée.

Vous n'avez que 96 heures pour envoyer le paiement. Si vous n'envoyez pas l'argent dans le temps limite, tous vos dossiers resteront encryptés pour de bon et personne ne sera capable de les récupérer.

Appuyez sur 'Vue' pour visionner la liste de dossiers qui ont été encryptés.

Appuyez sur 'Suivant' pour passer à la page suivante.



ALERTE! N'ESSAYEZ PAS DE VOUS DÉBARRASSER DU PROGRAMME PAR VOUS-MÊME. TOUTE ACTION ENTRAÎNERA LA DESTRUCTION DE LA CLÉ DE DÉCRYPTAGE. VOUS PERDREZ VOS DOSSIERS POUR TOUJOURS. LA SEULE FAÇON DE CONSERVER VOS DOSSIERS EST DE SUIVRE LES INSTRUCTIONS.

Vue

95:57:20

Suivant >>

Suivez les instructions sur le serveur.

Ces instructions sont aussi gardées dans un dossier appelé Decrypt-All-Files.txt dans le dossier Documents. Vous pouvez l'ouvrir et utiliser le copié-collé pour les adresses et la clé.

Le piratage de compte et l'usurpation d'identité

Particuliers comme entreprises sont concernés



But recherché

Dérober des informations confidentielles (personnelles / professionnelles / bancaires) pour en faire un usage frauduleux.

Technique

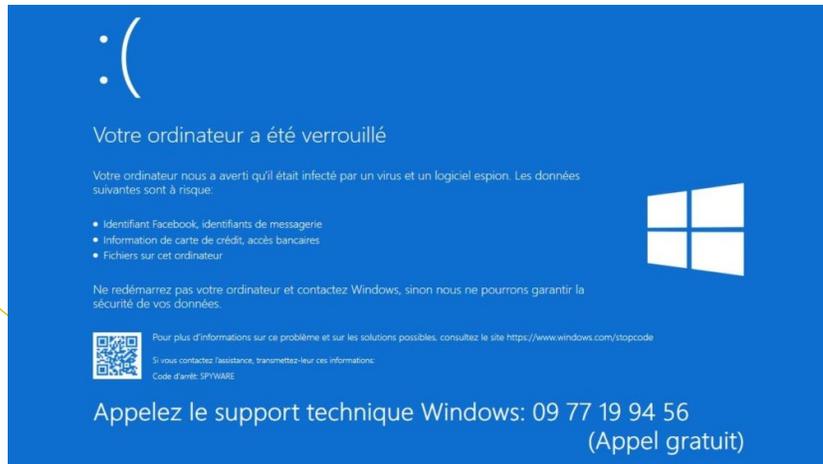
Prise de contrôle d'un ou plusieurs comptes en ligne et / ou usurpation de l'identité numérique.

Les causes probables:

- mot de passe trop simple
- hameçonnage réussi
- BDD d'un site cyber-attaqué



Arnaque au faux support technique



But recherché

Inciter la victime à **payer** un pseudo-dépannage informatique et / ou la **faire souscrire** à des abonnements payants.

Technique

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.)

Comment réagir si on est victime?

- **En cas d'infection, débranchez** la machine **d'Internet** ou du **réseau informatique**
- **En cas de vol de coordonnées bancaires faites opposition** immédiatement
- Conservez les **preuves** (courriels, captures d'écran, photos etc.)
- **Déposez plainte**
- Faites une **analyse antivirusale complète** de votre appareil
- **Changez** immédiatement vos **mots de passe**
- **Signalez** tout message ou site douteux à [Signal Spam](#)
- **Signalez** l'adresse d'un site d'hameçonnage à [Phishing Initiative](#)
- **Signalez les faits** sur la plateforme PHAROS: [Internet-signalement.gouv.fr](https://internet-signalement.gouv.fr)
- Besoin de plus de conseils ? contactez la plateforme [Info Escroqueries](#)



guide pour les collaborateurs



diagnostic en ligne

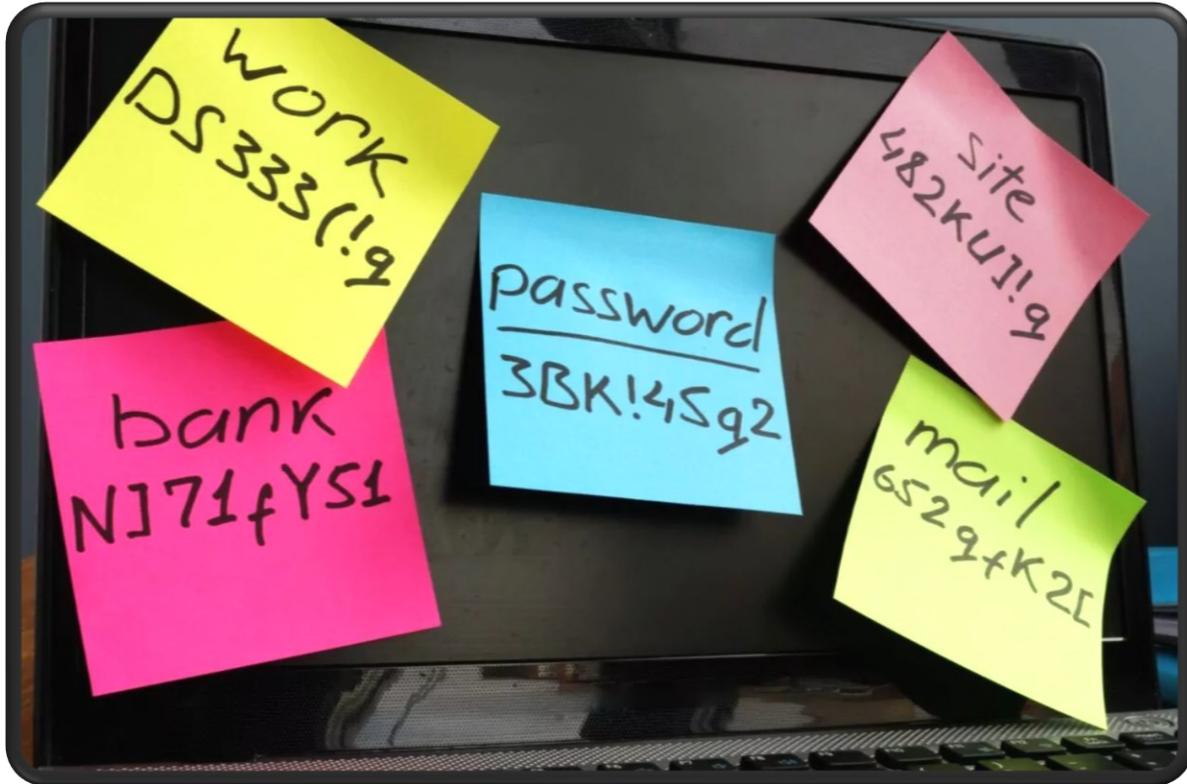




II. Les bonnes pratiques

10 mesures essentielles pour
une bonne hygiène numérique

Protéger vos accès avec des mots de passe solides



- 🔒 Un mot de passe différent pour chaque service
- 🔒 Robustesse = Long et complexe
- 🔒 Gestionnaire de mots de passe
 - 🔒 Activation de la double authentification
 - 🔒 Protection robuste de la messagerie

security.org

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombre minimum	Lettres minuscules	Lettres majuscules et minuscules	Chiffres, lettres minuscules et symboles	Chiffres, lettres minuscules et symboles
4	instantané	instantané	instantané	instantané	instantané
5	instantané	instantané	instantané	instantané	instantané
6	instantané	instantané	instantané	instantané	instantané
7	instantané	instantané	1 seconde	2 secondes	4 secondes
8	instantané	instantané	20 secondes	2 minutes	8 heures
9	instantané	3 minutes	24 heures	2 jours	6 semaines
10	instantané	1 semaine	21 heures	3 jours	2 semaines
11	instantané	22 heures	1 mois	31 jours	3 ans



KeePass



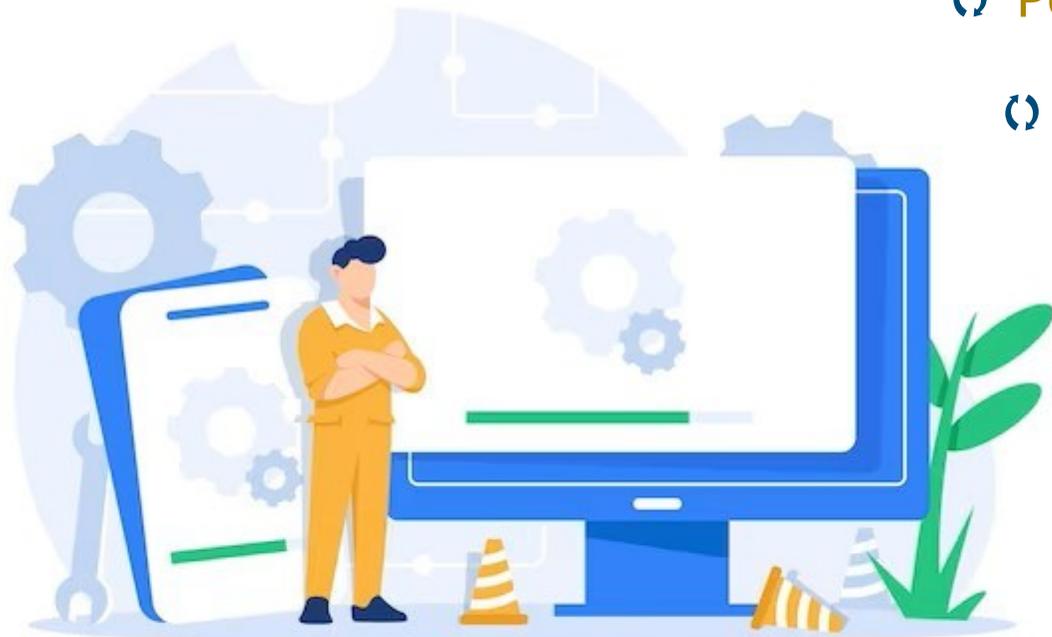
Sauvegardez vos données



- 📁 Sauvegardes régulières
- 📁 Identifiez les données à sauvegarder
- 📁 Déconnectez la sauvegarde
- 📁 Testez vos sauvegardes
- 📁 Protégez vos sauvegardes (vol, casse, perte...)



Appliquez les mises à jours proposées



- 🕒 Pensez aux mises à jours de vos logiciels ET appareils
- 🕒 Téléchargez sur les sites officiels uniquement
- 🕒 Activez les mises à jour automatiques
- 🕒 Identifiez vos appareils et logiciels



Sécurité sur les réseaux sociaux



- 🌐 Protéger l'accès à vos comptes
- 🌐 Maîtrisez vos publications
- 🌐 Vérifiez vos paramètres de confidentialité
- 🌐 Attention à l'authentification via votre compte
- 🌐 Supprimez votre compte si vous ne l'utilisez pas



Séparez vos usages personnels et professionnels



- 📖 Mots de passe différents
- 📖 Séparez vos messageries pro et perso
- 📖 Méfiez vous des supports USB
- 📖 Maîtrisez votre usage d'internet



Utilisez un antivirus



Téléchargez vos applications sur les sites officiels



Méfiez-vous des messages inattendus



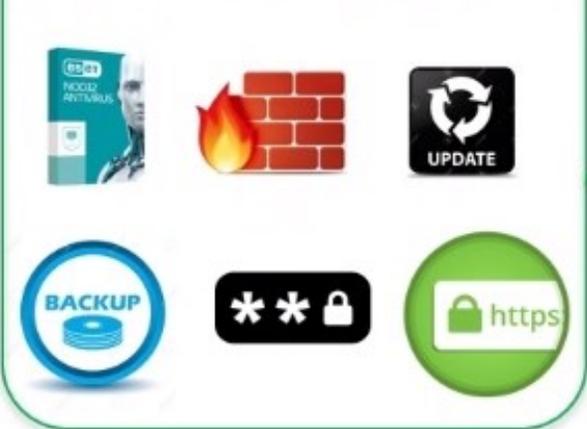
Vérifiez les sites d'achats



Évitez les réseaux Wi-Fi publics ou inconnus



Mesures de sécurité techniques



Politiques et procédures



Individus non sensibilisés





Groupement de Gendarmerie du Morbihan



Presansce-56@gendarmerie.interieur.gouv.fr



La **Cyber** est ton affaire !



#CyberResponsable Du **2** au **31** octobre 2023

cybermois.cybermalveillance.gouv.fr

