ACTECIL

RGPD SOLUTIONS

Sensibilisation à la cybersécurité

1 Introduction

A. Le cadre légal
B. Les acteurs de la cybersécurité

A. Le cadre légal et règlementaire

- **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
  - Encadre les traitements des données personnelles en France
  - Mise à jour avec l'entrée en application du **RGPD**

- **Loi n° 88-19 du 5 janvier 1988, dite loi Godfrain**
  - Infractions liées à la fraude informatique

- **Code Pénal Français :**
  - Articles 323-1 à 323-8
    - 2 à 7 d'emprisonnement (ou jusqu'à 10 ans !)
    - 60 000 € à 300 000 € d'amende
  - Articles 226-16 à 226-24
    - Protection des données à caractère personnel

- **Pour aller plus loin au niveau Européen : le RGPD et le *Cybersecurity Act***
  - Le Règlement Général sur la Protection des Données (RGPD),
  - Le *Cybersecurity Act*, adopté le 12 mars 2019 : renforce le mandat de l'ENISA et donne un cadre de certification de cybersécurité

ACTECIL RGPD SOLUTIONS

B. Les acteurs de la cybersécurité

Commission Nationale de l'Informatique et des Libertés

→ Contrôle de l'application du RGPD en France ;
→ Sanctionne les organismes non conformes ;

https://www.cnil.fr/

Agence Nationale de la Sécurité des Systèmes d'Information

→ Autorité nationale sur la sécurité et la défense des systèmes d'information

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

B. Les acteurs de la cybersécurité

CERT-FR (Equipe de Réponse au Urgences Informatiques)

→ Alertes et réactions aux attaques informatiques

https://cert.ssi.gouv.fr/

Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information

→ Chargée de la coordination de la cybersécurité dans l'Union Européenne

https://www.enisa.europa.eu/

2. Les principales menaces

A. Objectifs et acteurs des principales menaces
B. Les impacts et les risques

A. Objectifs et acteurs des principales menaces

Acteurs

- Réseaux organisés
- Hacktivistes
- Individus
- Groupes Etatiques

	Réseaux organisés	Hacktivistes	Individus	Groupes Etatiques
Sabotage				
Cybercriminalité				
Déstabilisation				
Espionnage				

Classement des types d'attaques en fonction des acteurs

B. Les impacts et les risques

- Disponibilité, intégrité et confidentialité

Disponibilité

Intégrité

Confidentialité

Preuve / Traçabilité

Types	Conséquences	Exemples d'impacts
Impacts sur le fonctionnement	Impacts sur les missions	• Incapacité à fournir un service • Conséquences sur la production ou la distribution de biens ou de services
Impacts humains	Impacts sur les personnes	• Perte de vies humaines • Mises en danger de personnes
Impacts sur les biens	Impacts sur le patrimoine culturel et intellectuel	• Perte de savoir-faire • Perte de mémoire de l'organisme
Impacts financiers	Conséquences pécuniaires directes ou indirects	• Perte de chiffre d'affaire • Pénalité
Impacts sur l'image	Notoriété, renommée, éthique	• Perte de crédibilité • Perte de confiance
Autres	Impacts de non-conformité	• Perte de labels, certifications, etc.
	Impacts juridiques	• Procès, sanctions de l'organisme, sanctions des dirigeants, etc.
	Impacts sur l'environnement	• Chimique, radiologique, sonore, visuel, etc.

Les « risques » sont évalués sur une échelle de 1 à 4
1 = risque négligeable
4 = risque maximal

ACTECIL RGPD SOLUTIONS

3. Les e-mails

A. Les arnaques les plus fréquentes
B. Reconnaître une tentative de hameçonnage

A. Les arnaques les plus fréquentes

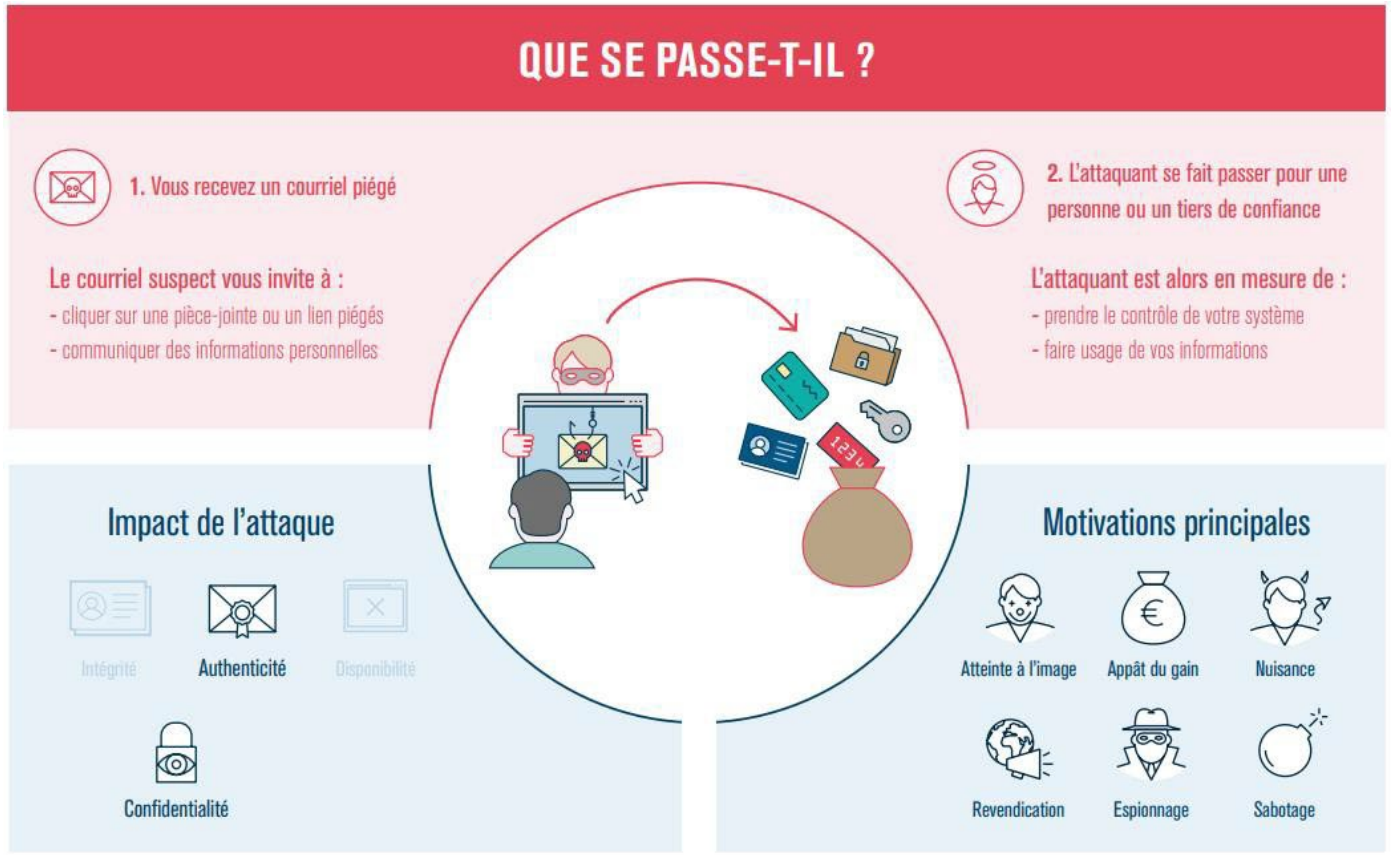
- Les e-mails

95 % des cyberattaques commencent par un mail malveillant.

Connaissez-vous l’arnaque la plus fréquente ?

A. Les arnaques les plus fréquentes

- Les e-mails



Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage

B. Reconnaître une tentative de hameçonnage

- Les e-mails

→ Une **notification de la messagerie** ou de **l'antivirus**

→ Un email d'un service ou d'une société dont **vous n'êtes pas client**

→ Un nom d'**expéditeur inhabituel**

→ Une **adresse d'expédition fantaisiste**

→ Un objet d'email **trop alléchant ou alarmiste**

→ Une **apparence suspecte**

→ Une **absence de personnalisation**

→ Une **demande inhabituelle**

→ Une **demande d'informations** confidentielles

→ Un **message aguicheur** ou **inquiétant**

→ Des **fautes de français** surprenantes

→Une **incitation à cliquer** sur un **lien** ou une **pièce-jointe**

Mise en situation

- Les e-mails

Exercice proposé par Google pour s'entrainer à détecter un courriel malveillant

https://phishingquiz.withgoogle.com/?hl=fr

4. Les déplacements

A. Comment éviter les risques liés aux déplacements

A. Comment éviter les risques liés aux déplacements

→L'utilisateur devrait :

- Rester vigilant de son entourage ;
- Mettre un filtre de confidentialité ;
- Désactiver les systèmes Bluetooth et Wi-Fi lorsque non utilisés ;
- Signaler tout vol ou comportement suspect à son équipe informatique.

→L'entreprise devrait :

- Banaliser les équipements d'entreprise ;
- Chiffrer les disques durs ;
- Avoir une politique d'entreprise adaptée aux terminaux nomades (charte télétravailleur, charte informatique, etc.)

Les déplacements

- Les bons réflexes

LES 9 BONNES PRATIQUES EN UN COUP D'ŒIL

Source : ANSSI
https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

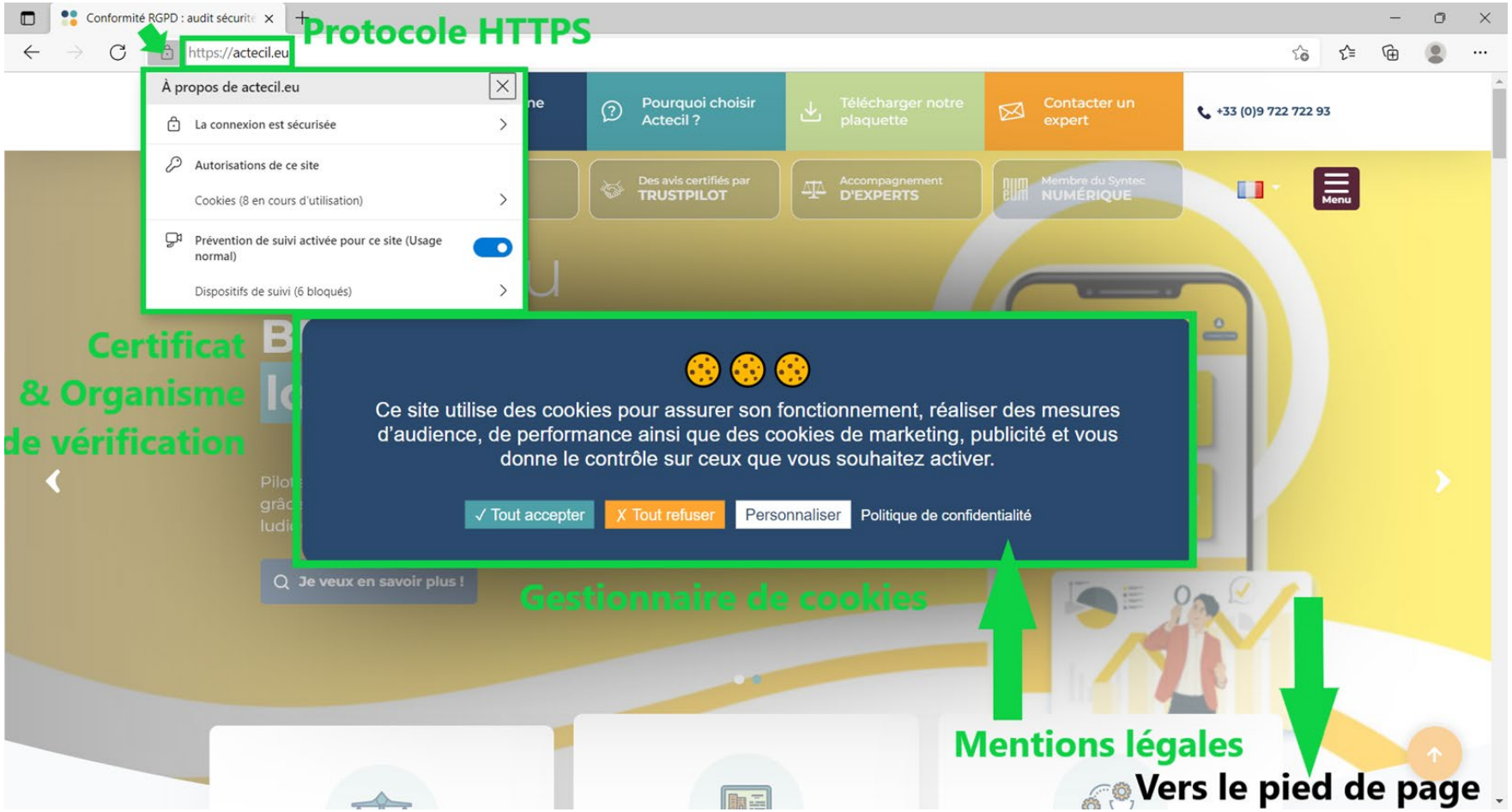
5. La navigation sur internet

A. Les bonnes habitudes du netizen

5. La navigation sur internet

Savez-vous comment reconnaître un site de confiance ?

5. La navigation sur internet



5. La navigation sur internet

- Les bonnes habitudes du Netizen

→ Il navigue sur des **sites de confiances**.
  - La règle s'applique aussi pour le travail !

→ Il arrive à identifier les liens douteux.

→ Il télécharge uniquement depuis des sites fiables.

→ Il préfère la double vérification.

→ Il donne les sources de ce dont il discute.

→ Il reste courtois et poli.

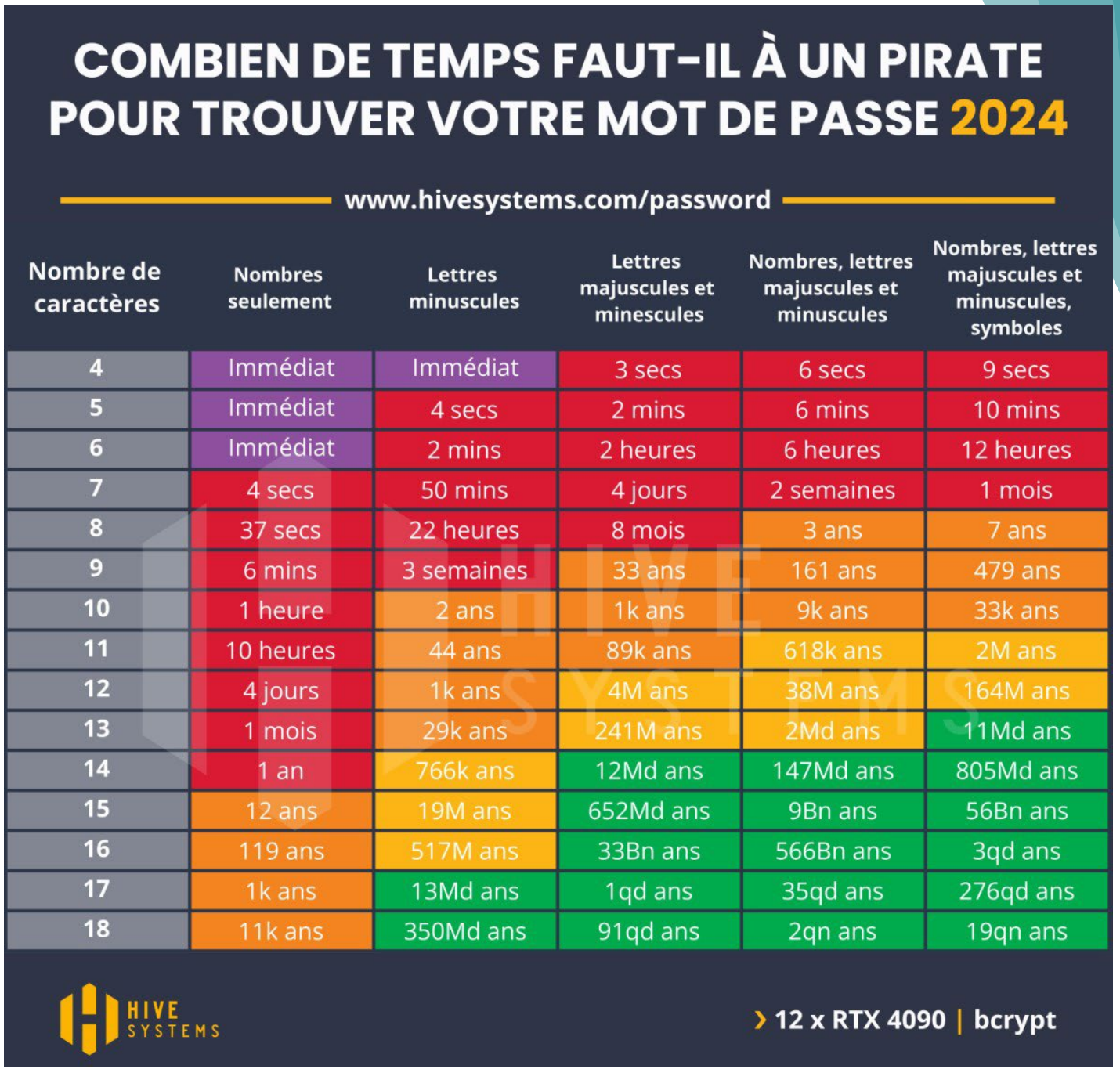
6. Les mots de passe

A. Quelques chiffres
B. Un bon mot de passe
C. Les gestionnaires de mots de passe

6. Les mots de passe

A. Quelques chiffres... en 2024...

- **65%** des mot de passe utilisés pour s'identifier sont réutilisés
- **81%** des accès aux données d'entreprises sont causés par des mots de passe faibles
- Plus de **3 milliards** de mots de passe uniques ont été exposés en 2023



COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

www.hivesystems.com/password

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

HIVE SYSTEMS

› 12 x RTX 4090 | bcrypt

6. Les mots de passe

B. Un bon mot de passe

- Contenir au moins **12 caractères** ;
- Contenir les **4 types** : des lettres **minuscules**, **majuscules**, des **chiffres** et des **caractères** spéciaux ;
- **Ne doit pas pouvoir être deviné** ;
- **Être différent pour chaque compte** utilisé ;
- Peut être enregistré dans un **gestionnaire de mot de passes**.

6. Les mots de passe

C. Les gestionnaires de mot de passe

→ Gestion des mots de passes sécurisés

- 1 seul mot de passe Maître pour tous vos mots de passe
- Possibilité de générer des mots de passes
- Versions gratuites et en sources ouvertes
- **Validé par des audits de sécurité reconnus**

→ Trois grands types de gestionnaires

- Les gestionnaires intégrés aux navigateurs
- Les gestionnaires hébergés
- Les gestionnaires locaux

https://keepass.fr/ ------ https://bitwarden.com/
https://www.dashlane.com/fr/ ------ https://www.lastpass.com/fr

6. Les mots de passe

Mise en situation

Quel(s) mot(s) de passe vous semble(nt) le(s) plus « fort(s) » ?

Réponse A AZERTYUIOP	Réponse B 28071994
Réponse C J’4lC&lpGdM!	Réponse D 1234

7. Le système

A. Règles d’or sur les sauvegardes et les mises à jour

A. Comprendre la règle d'or concernant les sauvegardes

3

Disposer de trois copies de vos données au moins

2

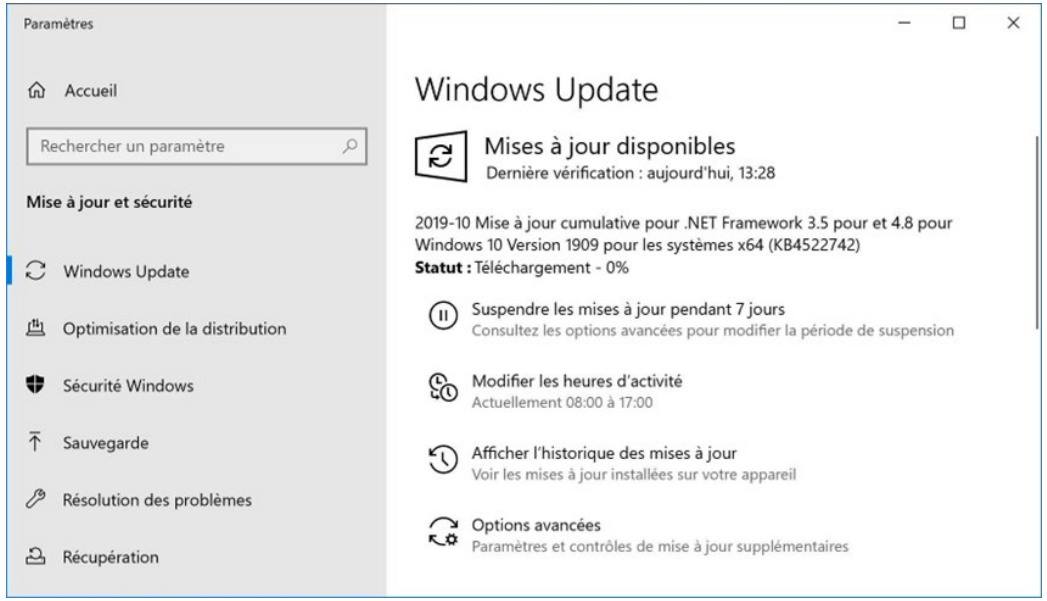
Stocker ces copies sur deux supports différents

1

Conserver une copie de la sauvegarde hors-site (hors-réseau)

A. Comprendre l'importance des mises à jour

1. **Mettre à jour sans tarder**
2. Télécharger uniquement depuis les **sites officiels**
3. Identifier l'ensemble des appareils et logiciels
4. Activer l'**option de mise à jour automatique**
5. Connaissez la **politique de mise à jour** de votre entreprise
6. Planifiez les périodes d'inactivité
7. **Méfiez-vous des faux sur internet**
8. Vérifier si la solution continue d'être mise à jour
9. **Protégez autrement les appareils qui ne peuvent pas être mis à jour**



Article de Cybermalveillance :
Bonnes pratiques de mises à jour

Merci de votre attention

Des questions

A. Bonus - Comprendre quelques méthodes d'attaques

Hameçonnage / Phishing

- Technique d'Ingénierie Sociale
- But : récolter des informations et/ou des identifiants
- > Partie 4 : les e-mails

Arnaque au faux président / support technique

- Technique d'Ingénierie Sociale
- But : effrayer la victime pour la forcer à réaliser des actions

Cryptojacking

- Implantation d'un malware
- But : miner des cryptomonnaies à l'insu de la victime

Rançongiciels / Ransomware

- Technique de pression, finalité de l'attaque
- Note : l'intrusion est déjà effectuée, c'est la dernière action de l'attaquant
- But : brouiller les pistes, faire perdre du temps, se faire connaître, récolter un peu plus d'argent

Pour aller plus loin : https://www.cybermalveillance.gouv.fr/cybermenaces

ACTECIL RGPD SOLUTIONS