

SAE11 – Hygiène informatique et sécurité



Les mots de passe

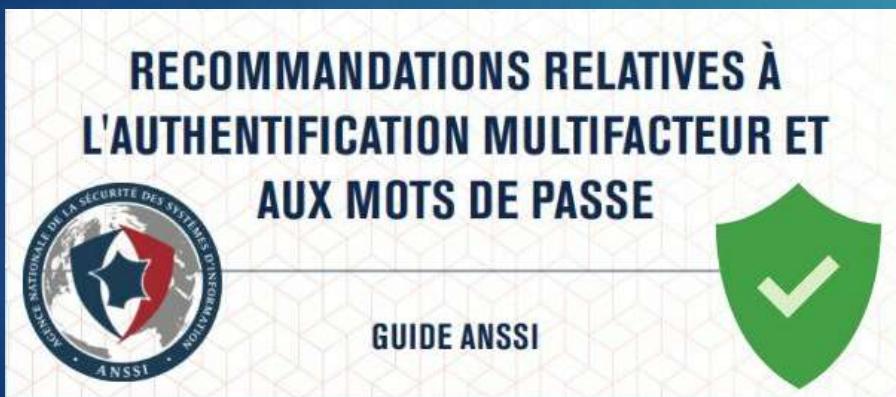
S1G4

LUCAS PECOUT
ALAN SALMON
JOSHUA KEELY

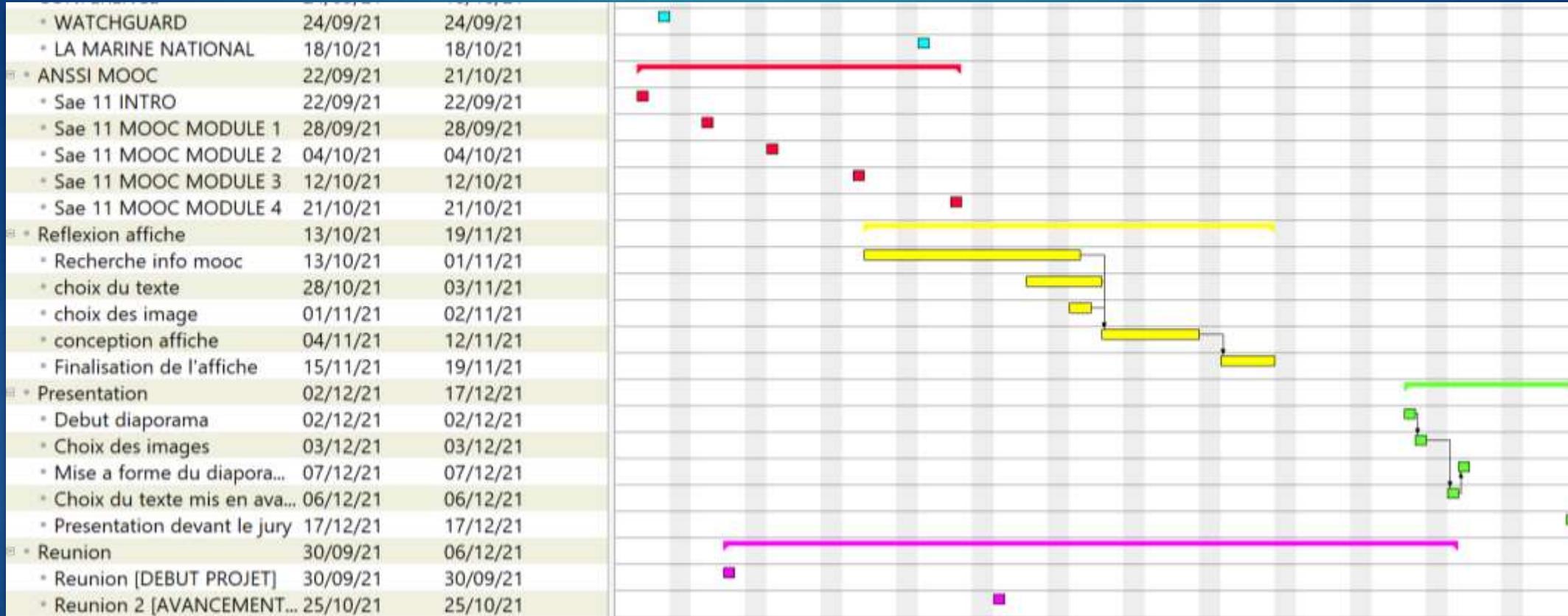
Le thème : Les mots de passe



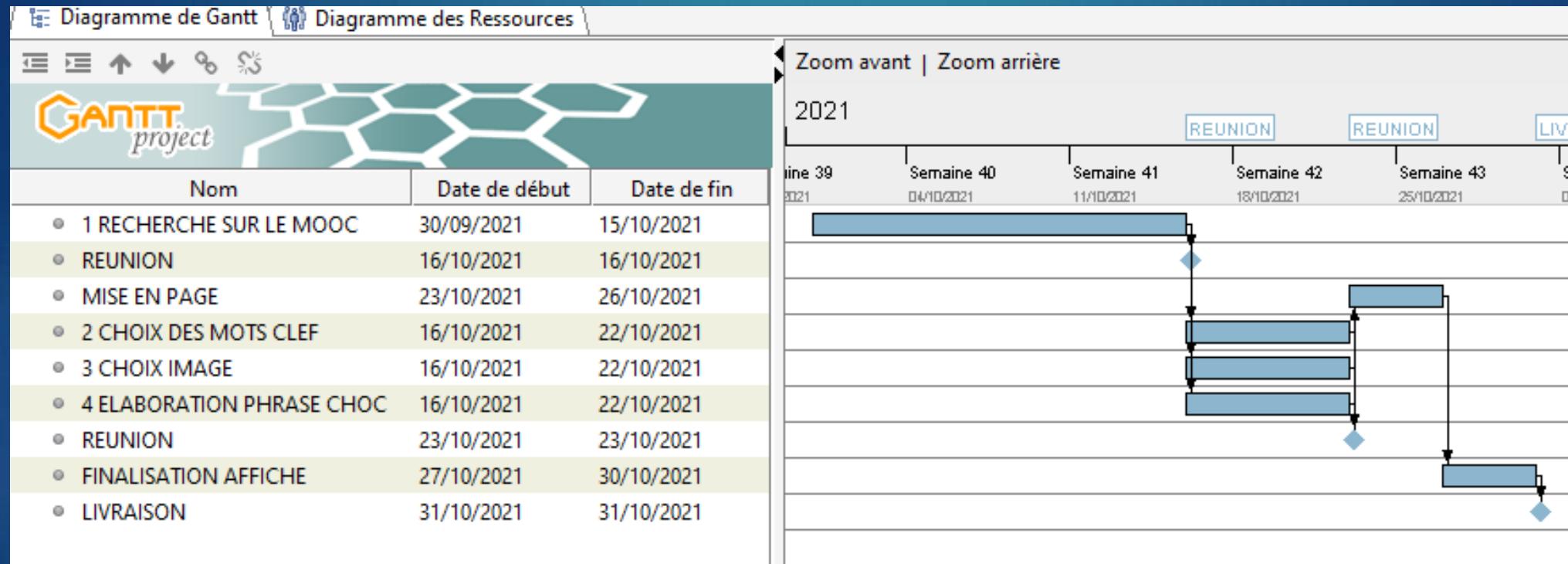
L'ANSSI



Gantt



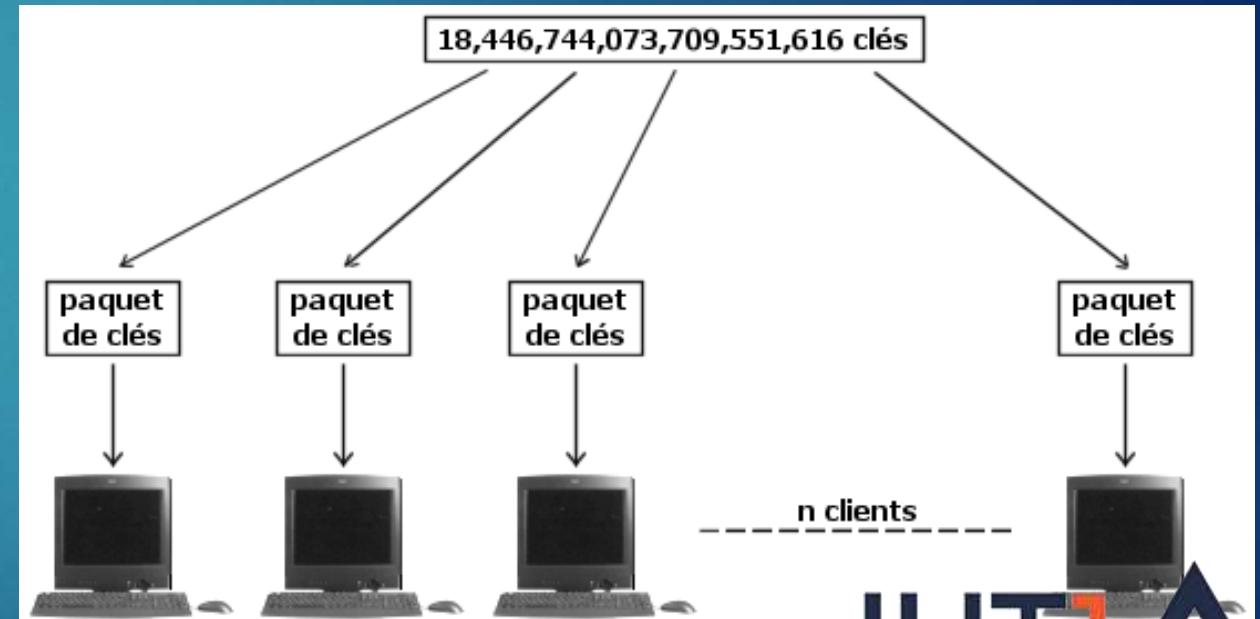
Gantt de base



Attaques par ingénierie sociale:



Attaque par dictionnaire ou force brute



Example d'attaque

N°4 : Marriott

En Avril, grâce à l'utilisation des identifiants de deux employés pour accéder à l'application de fidélisation, ce sont **les données personnelles de quelques 5,2 millions de clients qui ont été subtilisées**. Le groupe en est à sa **deuxième cyberattaque en seulement 3 ans...** La première ayant donné lieu à une fuite de données ayant affecté **339 millions de clients...** Le groupe Marriott avait alors dû régler **une amende de 18,4 millions de livres**. Cette sanction était diligentée par le gendarme britannique de la protection des données : ICO. Ce dernier avait alors prononcé cette peine au nom de l'Union Européenne. A noter que cette cyberattaque a eu lieu en 2014 et que les contenus sensibles ont été compromises jusqu'à ce que le piratage soit détecté... en 2018 !



Risques et conséquences des attaques informatiques

- Pertes financières
- Vol de données
- Nuisance à la sécurité (parfois nationale)
- Usurcation d'identité



58%
des victimes de violation de données en 2017 sont des petites entreprises



81%
des violations exploitent des mots de passe volés ou trop simples.
****mot de passe ****

Les recommandations

NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	1 sec	5 sec
8	IMMÉDIATEMENT	5 sec	22 min	1 heure	9 heures
10	IMMÉDIATEMENT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

*source : SCSP Community (Seasoned Cyber Security Professionals)

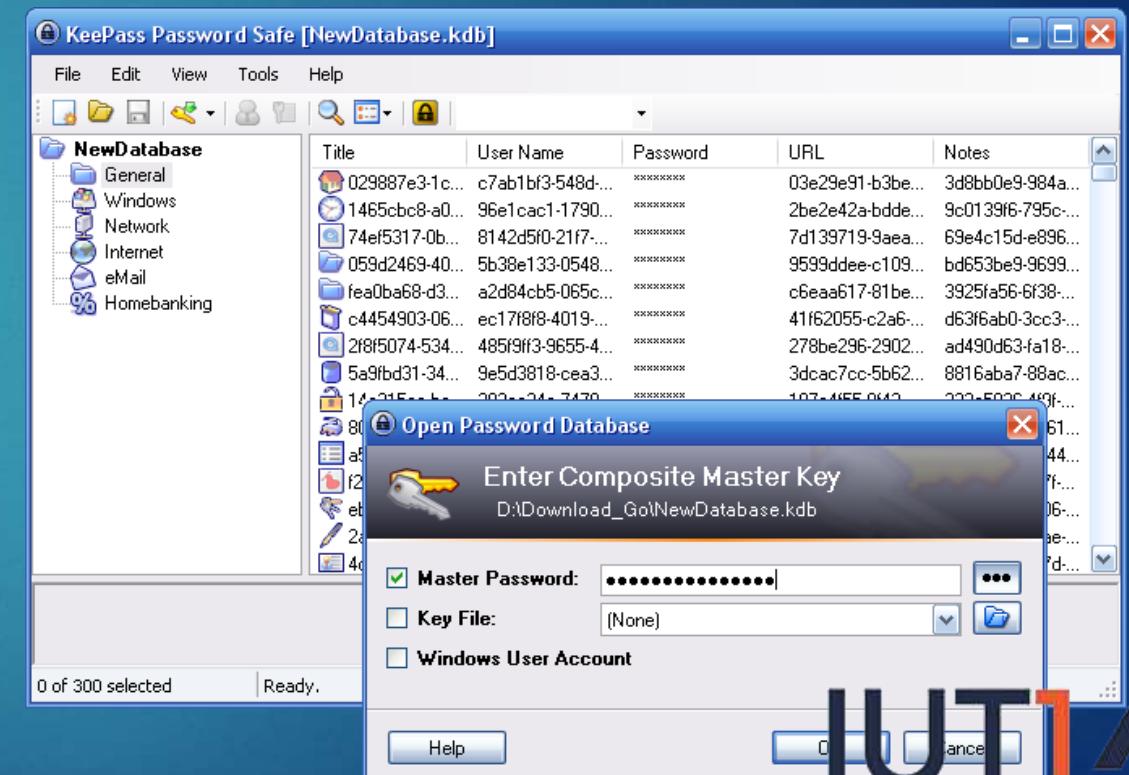
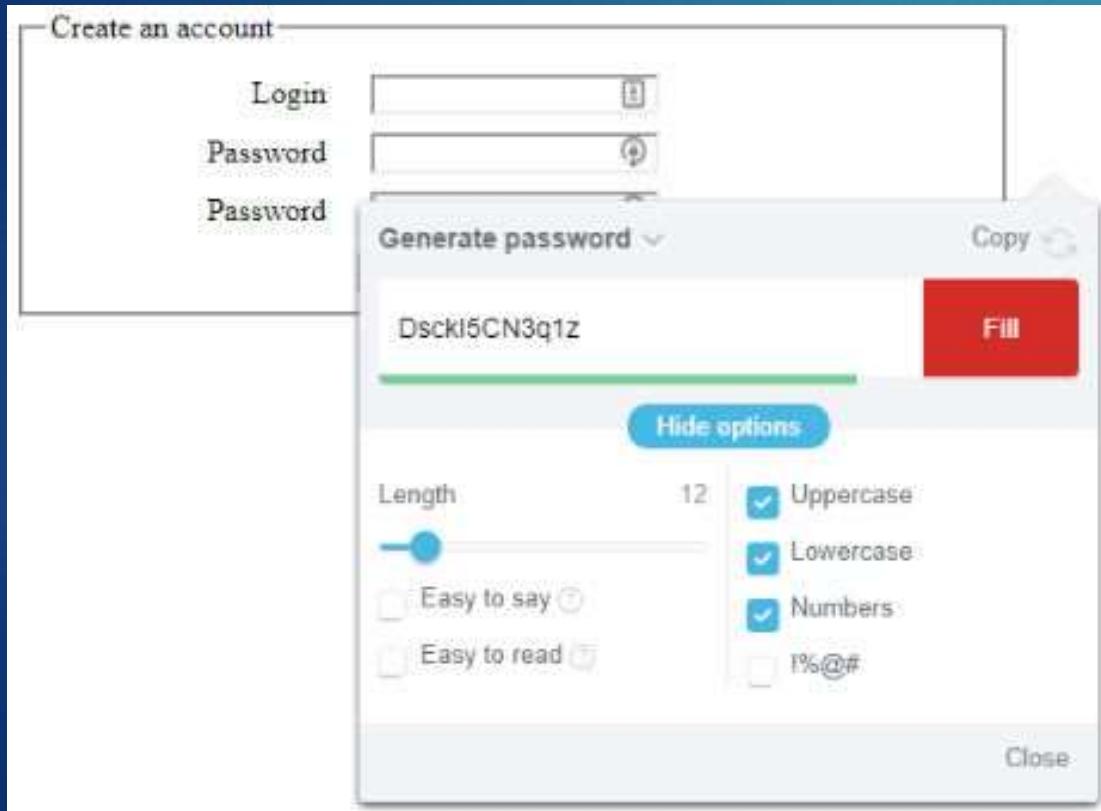
MOTS DE PASSE

Les bons réflexes à adopter pour une sécurité maximale

Recommandations :

- N'envoyez aucun mot de passe par mail ou SMS et ne les conservez pas dans un fichier texte
- Modifiez systématiquement les mots de passe par défaut et renouvez-les fréquemment
- Ne les enregistrez pas dans le navigateur d'un ordinateur partagé
- Activez la double authentification lorsqu'elle est proposée
- Stockez-les tous dans un gestionnaire de mots de passe sécurisé

Les recommandations



Présentation affiche

Les dangers d'un mot de passe faible



⚠️ Les risques:

Vol d'information

Lorsqu'un compte est piraté, des informations sensibles (bancaires, médicales, confidentielles) sont compromises. Elles peuvent fuiter sur internet ou être revendue à des fins malveillantes.



Usurpation d'identité

La simple compromission d'un mot de passe permet à une personne mal intentionnée de se faire passer pour quelqu'un d'autre. De grandes décisions peuvent être prises sans consentement.



Les types d'attaques

Attaques par ingénierie sociale: E-mails, SMS, clé USB, envoyés pour amener l'utilisateur à fournir ses identifiants, à cliquer sur un lien qui installe un logiciel malveillant, ou à site Web factice

Indispensables dans la vie de tous les jours, pour se connecter à tous les services du quotidien (mail, banque, réseaux sociaux), voici quelques dangers auxquels vos mots de passe sont confrontés tous les jours et comment éviter ces menaces.

Les solutions:

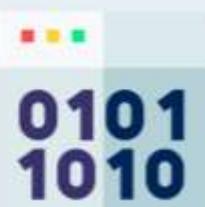
Changer les mots de passe régulièrement

Inconsciemment, les gens utilisent leur environnement immédiat pour créer leurs mots de passe. Le changer régulièrement est un bon moyen pour se protéger des attaques par force brute ou ingénierie sociale.



Utiliser un gestionnaire de mots de passe

Un gestionnaire de mots de passe sauvegarde chaque mot de passe d'un utilisateur dans un coffre-fort, facilitant leur sécurité.



Les types d'attaques

Attaques par ingénierie sociale:
E-mails, SMS, clé USB, envoyés pour amener l'utilisateur à fournir ses identifiants, à cliquer sur un lien qui installe un logiciel malveillant, ou à site Web factice



Attaque par dictionnaire:
Une attaque qui teste les mots courants

Force brute:
Utilisation d'un programme pour générer des mots de passe potentiels ou même des caractères aléatoires.

Pour limiter les risques, ne jamais utiliser ces mots de passe:

password azerty
123456 admin iloveyou
toto



- 77% UTILISENT LES MÊMES MOTS DE PASSE SUR DE NOMBREUX SITE
- 37% DES FRANÇAIS ESTIMENT QUE LEURS MOTS DE PASSE NE SONT PAS SÉCURISÉS
- 24% ESTIMENT QU'AU MOINS UN DE LEURS COMPTES A DÉJÀ ÉTÉ PIRATÉ

LES ATTAQUES ONT CONNU UNE HAUSSE DE 325 % PAR RAPPORT À 2020

Sources: ANSSI, Canva, Freepik
Production: Lucas Picard, Joshua Keely, Alan Salmon



sauvegarde chaque mot de passe d'un utilisateur dans un coffre-fort, facilitant leur sécurité.

1010

Un bon mot de passe

L'ANSI[®] recommande un mot de passe :

- D'au moins 12 caractères
- Différent pour chaque site internet
- Sans information personnelle
- Sans mot du dictionnaire explicite
- Contenant tout type de caractères



[®]Agence nationale de la sécurité des systèmes d'information (anssi)

RETOUR D'EXPERIENCES

- ▶ Points Positifs :
 - Création et gestion d'un projet
 - Apprentissage des bonnes pratiques sur la sécurité informatique
 - Réalisation d'un projet concret en équipe
 - Sensibilisation à la sécurité des mots de passe
 - Travail en collaboration et partage d'information
 - suivi de projet
 - Gestion du temps et de l'équipes

Bibliographie

<https://secnumacademie.gouv.fr/>

<https://www.canva.com/>

<https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-10530-violation-de-donnees-le-groupe-hotelier-marriott-face-a-un-recours-collectif-d-envergure.html>

<https://theconversation.com/les-mots-de-passe-entre-securite-vulnerabilite-et-contraintes-87886#:~:text=Le%20risque%20principal%20est%20le,l'usurcation%20d'identit%C3%A9.>