Plan :

- intro + histoire + définition

-firewall : ploquer les access non autoriser

Dmz

- gestionnaire de mot de passe

double authentification

- anti-virus

- protection de materieelle (switch, router, auter)

- charte de sécuriter

- politique de sécuriter(désactiver les roote)

- voir les évolution

- INTRO

- **La Sécurité informatique dans une petite entreprise**

Aujourd'hui les entreprises sont obligées d'avoir un réseau pour la communication et pour l'échange de données. Elles sont sujets à des attaques informatiques de plus en plus fréquente ce qui fait qu'il est impératif de sécuriser le réseau ou de mettre en place des mesures de sécurité.

Il y a plusieurs possibilités de sécuriser le réseau d'une entreprise, chaque entreprise choisit son système selon son besoin et son activité. Il est possible de faire l'installation d'un pare-feu qui bloque les requêtes non autorisées ou de mettre en place des VLAN pour séparer les réseaux ce qui permet de sécuriser le réseau des entreprises.

Historiquement les réseaux téléphoniques ont été les premières infrastructures à être piraté par des hackers. Les hackers sont à la base des personnes passionnées d'informatique et d'électronique qui s'amusent à modifier les programmes ou à remanier le matériel informatique, pour les détourner de leur utilisation première, mais aussi pour les rendre plus performant.

Ci-dessous les liens vers des articles sur les hackers :

https://blog.planethoster.com/le-hacking-une-histoire-de-revolutionnaires/

https://encyclopedia.kaspersky.fr/knowledge/a-brief-history-of-hacking/

- Cybersécurité :
  - Définition :

- Cyber : le monde du numérique d'internet
- Sécurité : protéger une entité contre une menace ou une attaque d'une personne malveillante.

Sur Wikipédia :

https://fr.wikipedia.org/wiki/Cybers%C3%A9curit%C3%A9

Le mot **cybersécurité** est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation)

- FIREWALL

Le pare-feu

concerne les petits fails de sécurité ou d'administrateur ou les 2 rencontrés dans notre quotidien.

DMZ = En informatique, une zone démilitarisée, ou DMZ est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

NAT (Network Address Translation) et PAT (Port Address Translation)
https://fr.wikiversity.org/wiki/NAT_%26_PAT/Introduction

- LES MOT DE PASSE

Les mot de passe permet de protéger un systéme pour que seul se qui connaisee le MDP puise si connecter

La régle de basse pour un bon mot de passe :

Deux méthodes simples peuvent vous aider à définir vos mots de passe :

• La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » :

• ght5CDs%E7am

• La méthode des premières lettres : « Allons enfants de la patrie, le jour

de gloire est arrivé » :

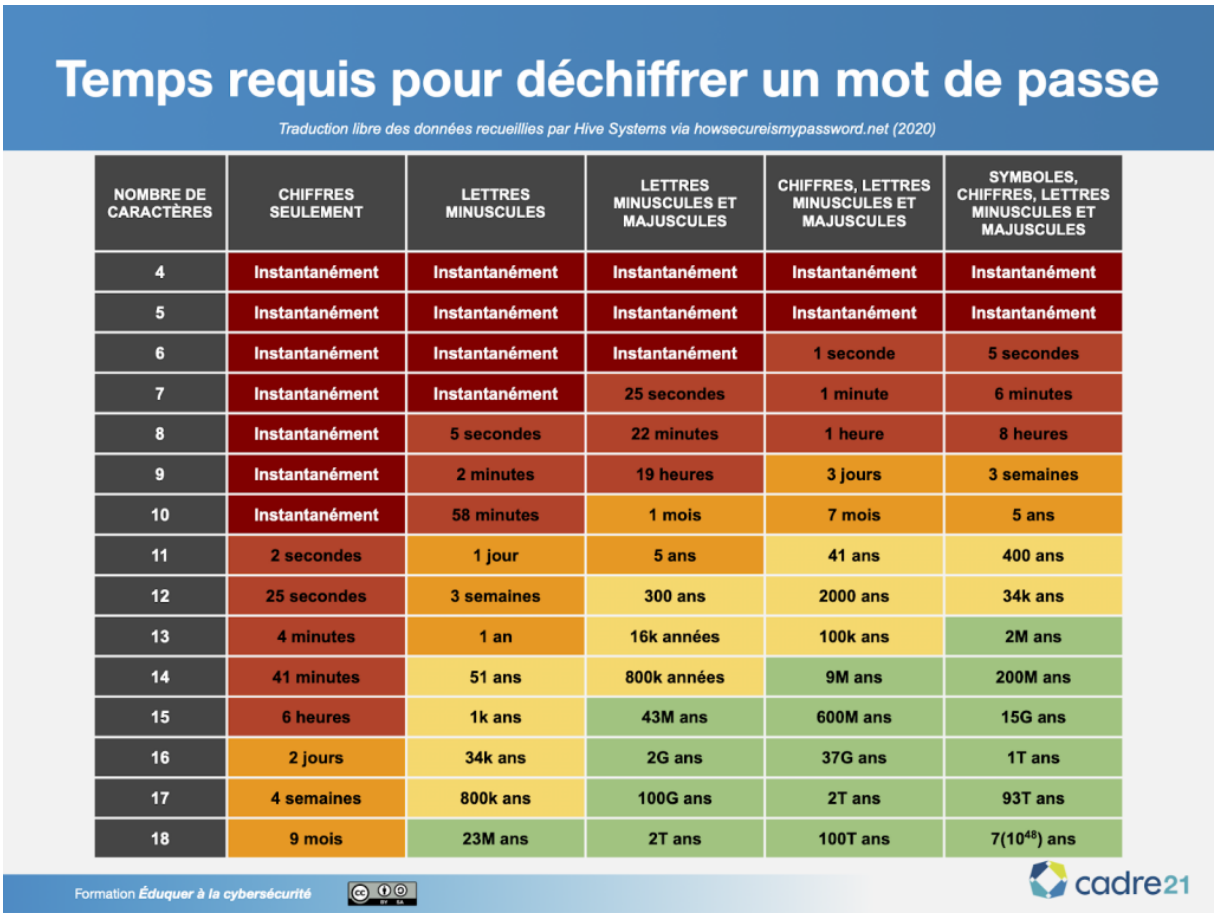
• aE2lP,lJ2Géa!

mot de pass nule

https://www.bhmag.fr/actualites/le-top-25-des-pires-mots-de-passe-utilises-sur-internet-en-2019-45241

Mais aujourd'hui a puissance de calcule permet de casser

https://www.journaldunet.com/solutions/dsi/1441966-52-secondes-le-temps-necessaire-pour-pirater-le-mot-de-passe-d-un-employe-et-entrer-dans-le-reseau-de-son-entreprise/



Temps requis pour déchiffrer un mot de passe

Traduction libre des données recueillies par Hive Systems via howsecureismypassword.net (2020)

NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	7(10^{48}) ans

Formation *Éduquer à la cybersécurité*

cadre21

Solution un gestionnaire de mot de passe + double authentification

Les 8 meilleurs gestionnaires de mots de passe :

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwipuqmnn8X0AhUOyIUKHZ4_CkQQFnoECDEQAw&url=https%3A%2F%2Fwww.codeur.com%2Fblog%2Fmeilleurs-gestionnaires-mots-de-passe%2F&usg=AOvVaw2wSV9y5rgs9i2O6s9VhJUo

clée yubico

https://www.yubico.com/la-cle-yubikey/?lang=fr

activer la double authentification

https://www.youtube.com/watch?v=ezEftyrKNOQ