Cybercafé

Comment le sécurisé ?

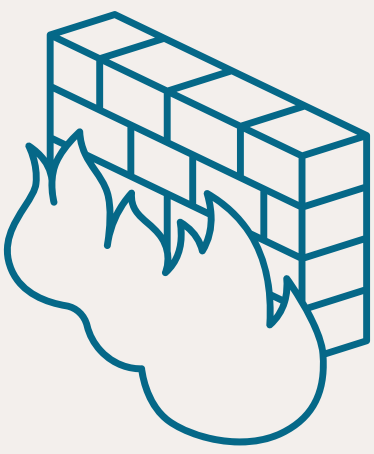
Une grande partie des connexions en ligne est dangereuse.

Il est donc important de se protéger !

À travers ce guide, vous allez découvrir et comprendre comment vous protéger des menaces internes à votre cybercafé !

Par Axel Hespel SIO 1

FireWall



USB

Mise A jour

Un pare-feu / Fire-Wall

C'est quoi ?

Un pare-feu est un dispositif de protection du réseau qui surveille le trafic entrant et sortant, et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

Pourquoi ?

Pour vous protéger des connexions à des sites étrangers ou bloquer certains ports !

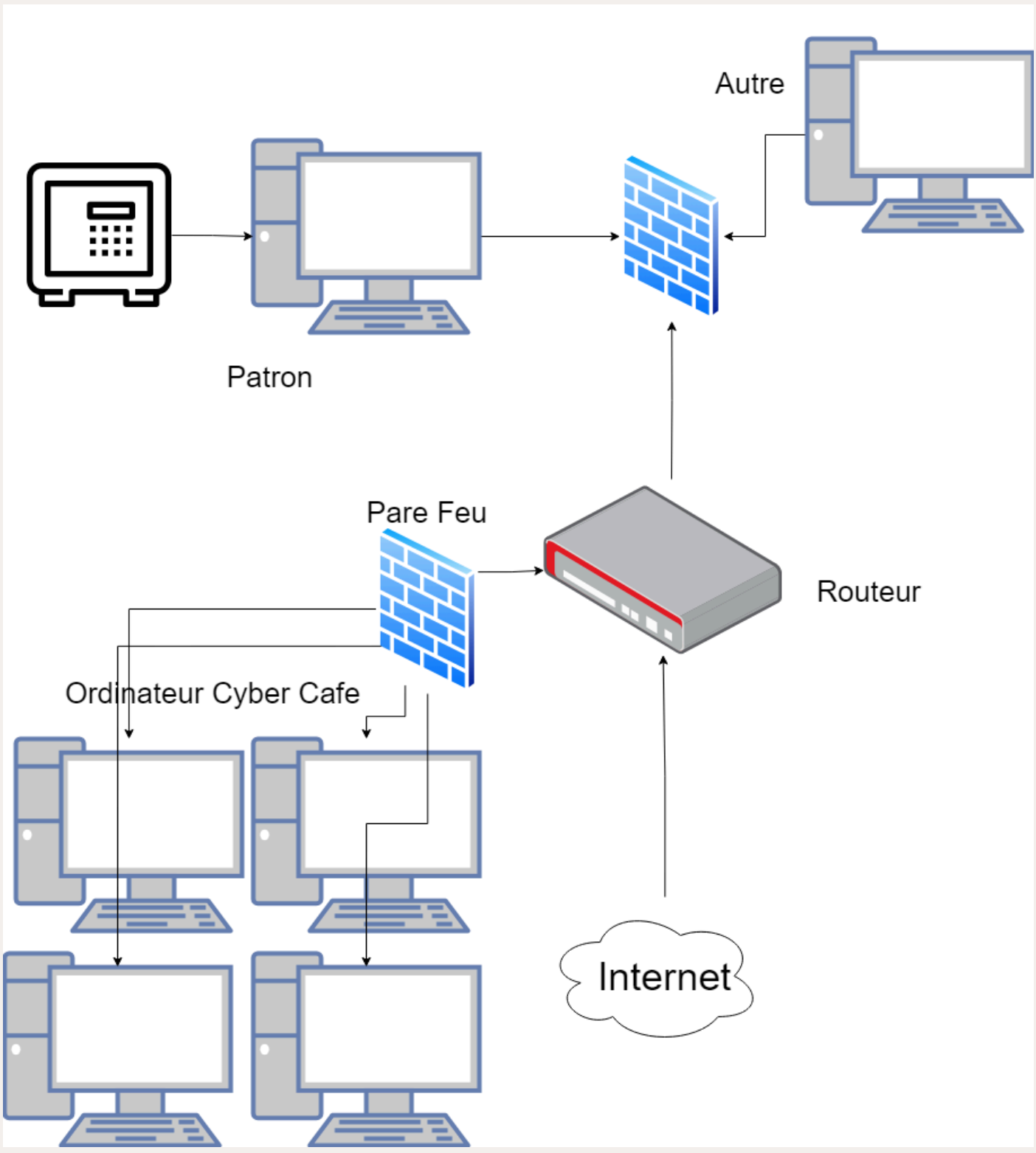
Pare Feu

Ou ? Comment ?

Ou ?

Un pare-feu est un outil qui vous permet de connecter vos ordinateurs à ce boîtier, qui sera ensuite relié à votre box. Selon les règles définies sur le pare-feu, les connexions, qu'elles soient entrantes ou sortantes, seront bloquées. Il sera donc, par exemple, impossible d'accéder au reste de vos équipements informatiques.

Exemple



Par Axel Hespel SIO 1

Pare Feu

Ou ? Comment ?

Comment ?

Par analogie, dans la sécurité du réseau, un pare-feu est un système logiciel ou matériel qui agit comme un contrôleur d'accès entre les réseaux fiables et ceux non approuvés.

A quoi ca ressemble ?

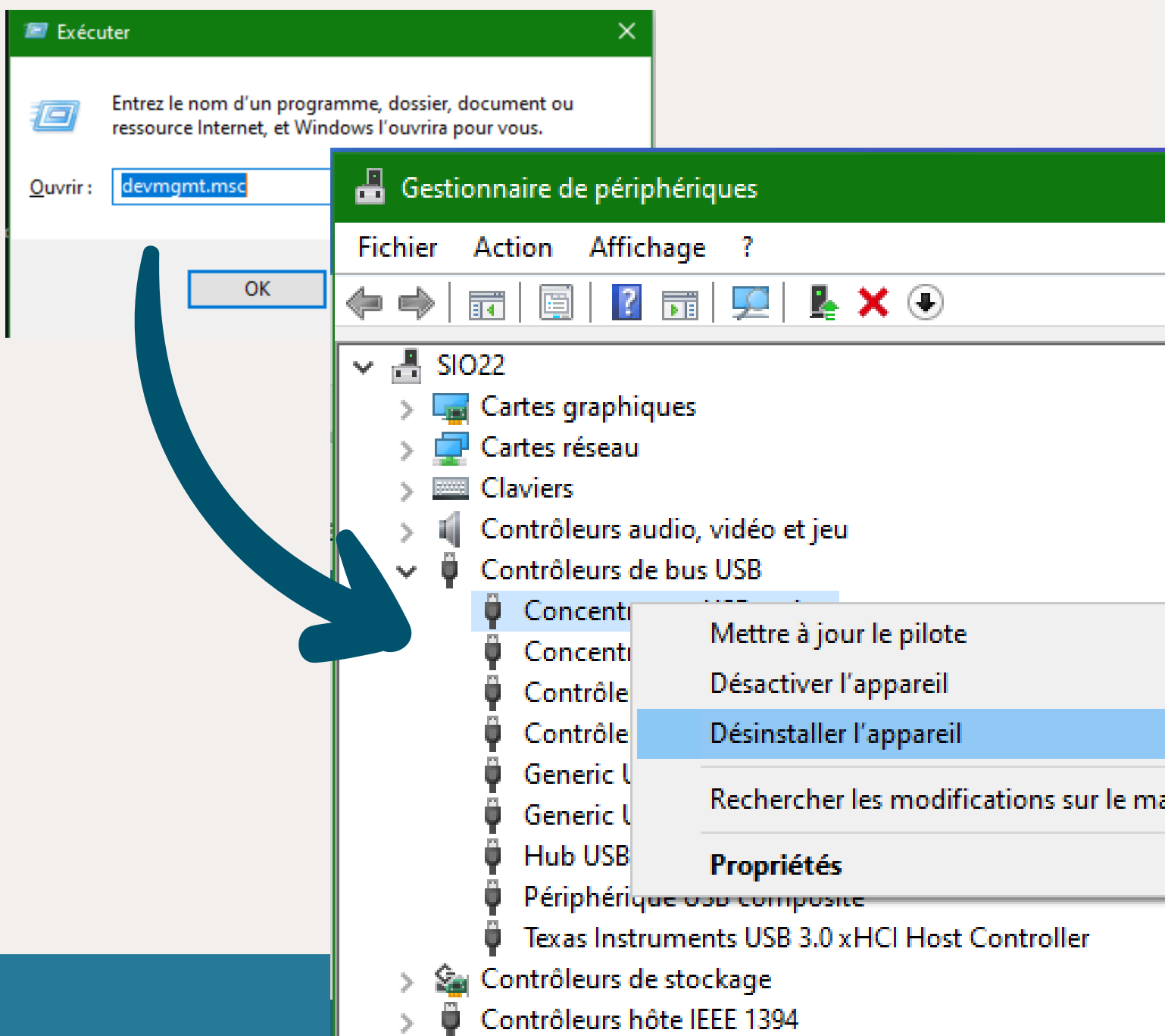
Port USB

Les désactivez

Les ports USB représentent une véritable menace pour votre système d'information, il est donc très important de les désactiver.

Comment ?

- Appuyez simultanément sur Windows+R
- cherchez devmgmt.msc
- Une fois dedans cliquer sur controlleur de bus USB
- Désinstallez tout les pilotes de tout les ports USB (Bien les désinstallez et non désactivez !)

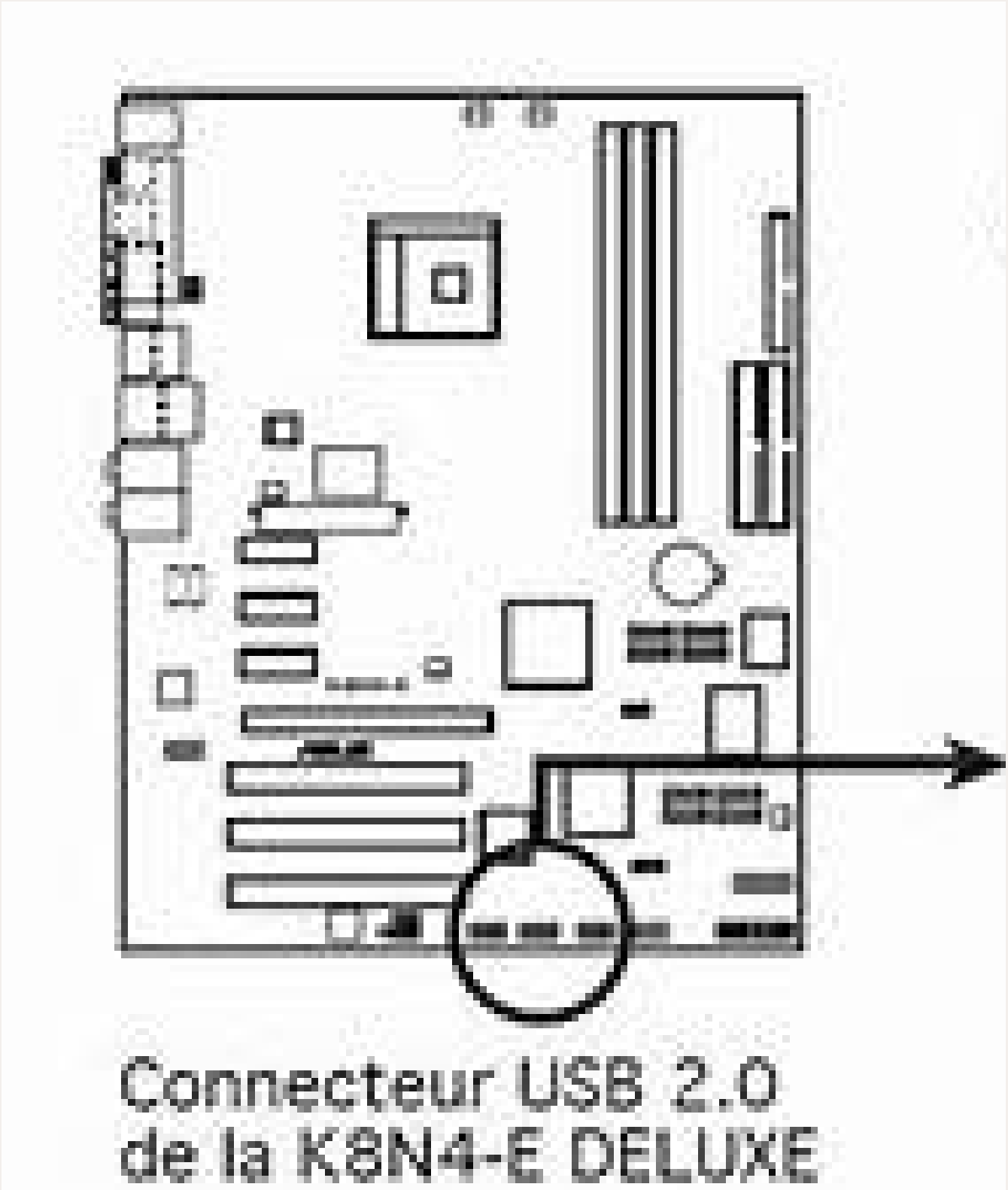


Port USB

Les désactivez

Comment ?

Il est également possible de ne pas brancher les ports USB sur la carte mère ou de les débrancher facilement !



Connecteur USB 2.0
de la K8N4-E DELUXE

Port USB

Les désactivez

Réalisez des testes !

Pour vérifier la pérennité des groupes, je ne peux que vous encourager à réaliser des tests, ainsi que des audits ou du pentesting pour évaluer l'état de votre parc et identifier les éventuelles failles potentielles.

Mise a Jour

De facon fiable !

Facon 1
Windows Update

Sur Windows, les mises à jour se font grâce à Windows Update. Elles s'effectuent automatiquement lors du démarrage de l'ordinateur. Il est donc important de redémarrer vos machines au moins une fois par jour. Vous pouvez également vérifier si les mises à jour ont été effectuées via Windows Update.

Facon 2
wsus update

Si vous disposez d'un parc connecté à un serveur Windows, vous pouvez alors effectuer les mises à jour directement grâce à leur service WSUS. Ce service vous permet de télécharger une seule fois les mises à jour depuis Internet, puis de les répliquer ensuite sur vos différentes machines, plutôt que de les télécharger X nombre de fois.

Mise a Jour

Pourquoi ?

Pourquoi ?

Il est très important de réaliser ces mises à jour, car si des failles sont découvertes sur votre système d'exploitation, même si elles sont identifiées, si vous ne réalisez pas les mises à jour, vous resterez quand même vulnérable et exposé aux attaques !

Les dangers

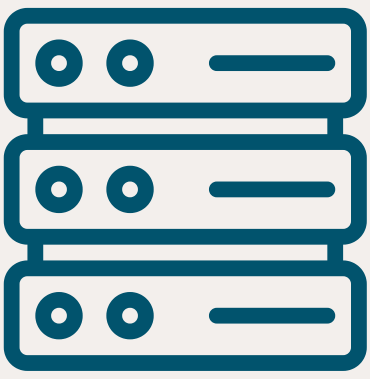
Différentes failles sur windows sont découvertes **toute les semaines**

- Des failles dite “day-0” qui sont des failles plus au moins sensible exploitabe sur tout les Systémes.
- Des problémes de performance ou d’instabilité peuvent également etre corrigé

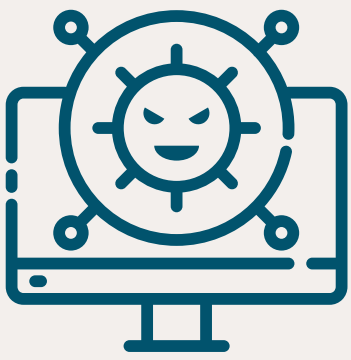
Outils en plus

Quelles outils ?

DHCP



ANTI-VIRUS



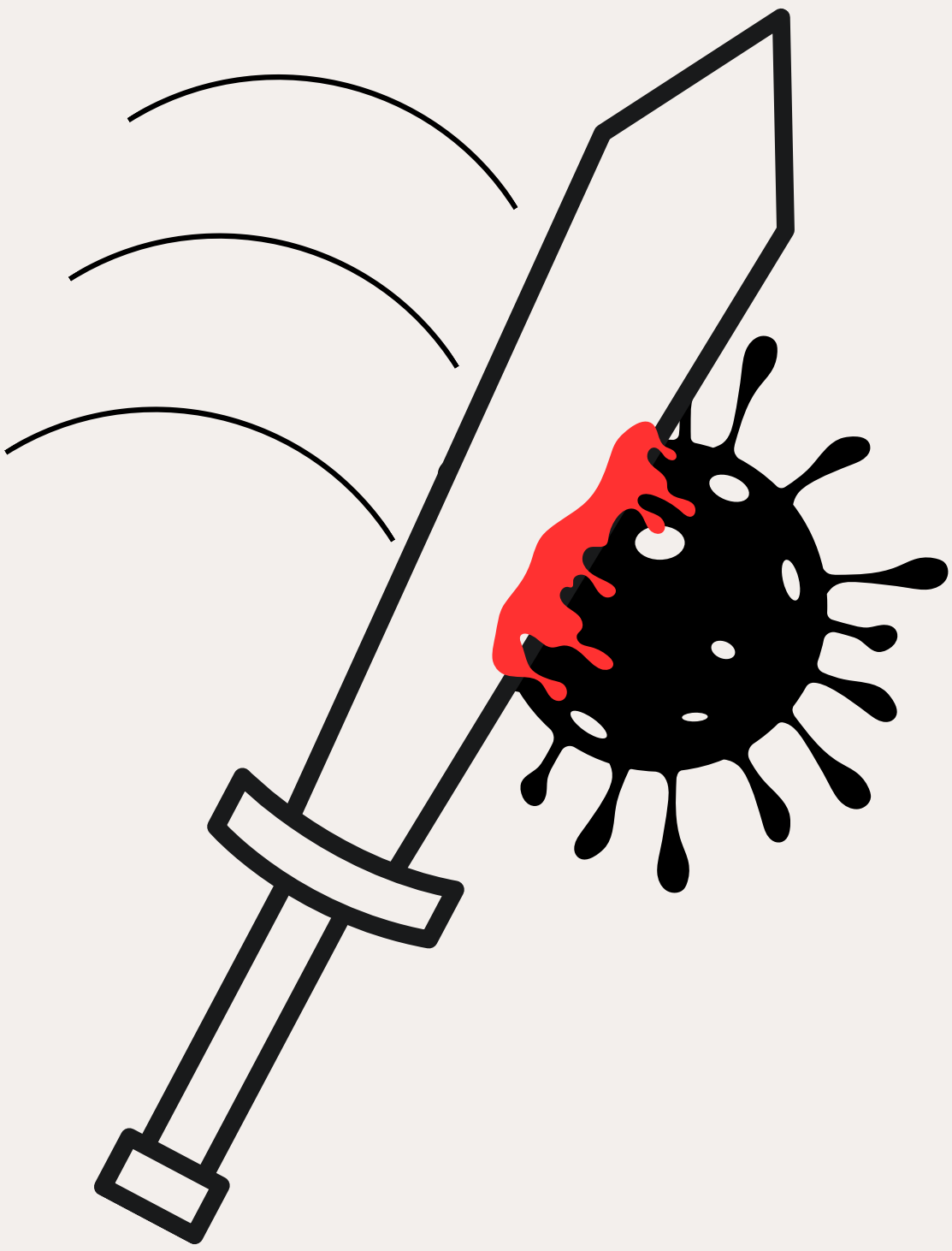
DHCP

Pour des raisons de sécurité, je vous conseille de configurer correctement votre serveur DHCP. Une configuration adéquate permettra d'empêcher les connexions étrangères non autorisées. Par exemple, vous pouvez limiter le nombre de connexions ou restreindre les connexions par adresse MAC afin de mieux contrôler l'accès au réseau.

Outils en plus

ANTI-VIRUS

Pour des raisons de sécurité, je vous conseille de configurer correctement votre serveur DHCP. Une configuration adéquate permettra d'empêcher les connexions étrangères non autorisées. Par exemple, vous pouvez limiter le nombre de connexions ou restreindre les connexions par adresse MAC afin d'avoir un meilleur contrôle de l'accès au réseau.



II-Lycée

Gestion des mots de passe

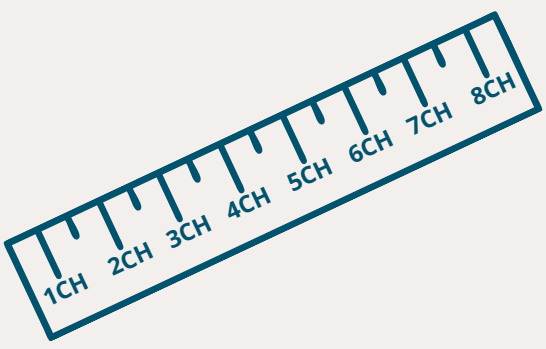
Le mot de passe est la première couche de sécurisation.

Il est donc important d'en avoir de solides !

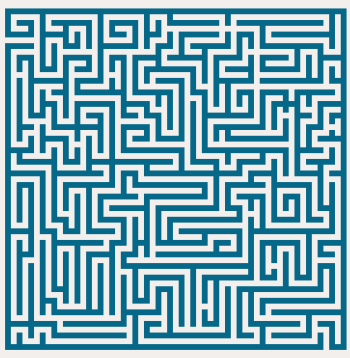
Comment rédiger un guide des bonnes pratiques ?

Par Axel Hespel SIO 1

Long



Complexe



Renouveler

Source

Un mot de passe

C'est quoi ?

Il s'agit d'une chaîne de caractères permettant de protéger l'accès à certains endroits.

Les mots de passe

Premières connexions

Politique de sécurité des mots de passe

Une politique de sécurité de mots de passe est caractérisée par la définition de certains éléments associés à la gestion des mots de passe (liste non exhaustive) :

- catégorie de mots de passe ;
- longueur des mots de passe ;
- règles de complexité des mots de passe (c.-à-d. les types de caractères utilisables) ;
- délai d'expiration des mots de passe ;
- mécanismes de limitation d'essais d'authentification (cf. la recommandation R10) ;
- mécanismes de contrôle de la robustesse des mots de passe ;
- méthode de conservation des mots de passe ;
- méthode de recouvrement d'accès en cas de perte ou de vol des mots de passe ;
- mise à disposition d'un coffre-fort de mots de passe.

vVoici une liste de tous les éléments que vous devez prendre en compte pour la création de votre politique de mot de passe liée à la création de mots de passe.
Les plus importants etant:

- Complexité (37CA différent)
- Taille (14CA)
- Délai d'expiration des mots de passe
- Trouvabilité (Element connue de la personne)

Les mots de passe

Gestion pendant le BTS

Pendant votre BTS, il est recommandé de changer vos mots de passe plusieurs fois et d'en avoir de distincts selon les sites ou le niveau de gravité en

Création PASSPHRASE

Si vous n’arrivez pas a retenir tout vos de passe vous pouvez créez des passphrase: Exemple

- Votre tortue s’appelle Georgette et vous habitez en Charente-Maritime. Préférez VOILÀ_LA_TORTUE_DU17 plutôt que GEORGETTE

Les mots de passe

Création PASSPHRASE

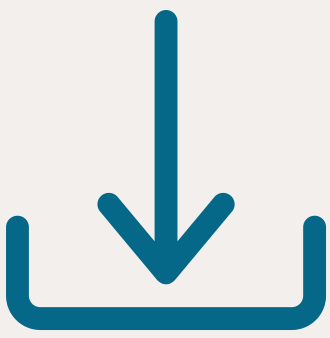
Le mieux est de créer des passphrases originales à chaque fois, mais vous pouvez par exemple choisir les paroles d'une musique (même si une personne proche de vous peut donc déduire le mot de passe). Si vous utilisez la passphrase, il est important de modifier certains caractères.

Element non recommander lors de la navigation

Compte inutile

Enregistrer son mot de passe

Télécharger



Les mots de passe

Rôles différentes stratégies

- Conserver l'historique
  - Nombre de mots de passe stockés par le serveur (éviter la réutilisation
- Durée de vie maximale
  - Nombre de jours avant changement de mot de passe obligatoire
- Durée de vie minimale
  - Nombre de jours avant changement de mot de passe minimum
- Enregistrer les mots de passe
  - Possibilité d'enregistrer les mots de passe dans Windows
- Exigences de complexité
  - Exiger le respect des règles de complexité des mots de passe
- Longueur minimale du mot de passe
  - Nombre de caractères minimum

Les mots de passe

Keepass

+	-
• Open source • facile d'utilisation • Pratique • Fiabe • Recommander par la CNIL	• Si une faille est publique mot de passe exploitable ! • Lors de changement de PC, il faut l'application

Les mots de passe

Keepass

A quoi ca ressemble ?