

# SAE-101

Se sensibiliser   l'hygi ne informatique et   la cybers curit 

# Table des matières

## 1. Introduction

## 2. Contenu

- 1) Les cyberattaques et les vecteurs de menace
- 2) Solutions de protection
- 3) Sécurisation des mots de passe et des communications
- 4) Chiffrement des communications
- 5) Usage personnel des ordinateurs de l'entreprise
- 6) Sauvegardes régulières et formation des employés

# Introduction

1. Aperçu des différentes menaces
2. Mesure pour limiter ces menaces
3. Les différents outils pour contrer les attaques
4. Des actions du quotidien simples pour réduire les risques

# 1. Les différentes menaces

Le Phishing

Les Malware

# Le Phishing

C'est l'une des menaces les plus fréquentes. Cette attaque a pour but de récupérer des données personnelles, comme des identifiants et des mots de passe, ou des informations bancaires. Généralement, la victime est contactée par e-mail, SMS ou appel téléphonique.

# Le Phishing

C'est l'une des menaces les plus fréquentes. Cette attaque a pour but de récupérer des données personnelles, comme des identifiants et des mots de passe, ou des informations bancaires. Généralement, la victime est contactée par e-mail, SMS ou appel téléphonique.



Chère cliente, Cher client,

Lors de votre dernière opération bancaire, nous avons remarqué une activité inhabituelle sur votre compte.

Pour réactiver votre compte Vous devez mettre à jour vos informations, une fois ces dernières validées, le compte fonctionnera normalement.

L'ensemble du processus ne prendra que 5 minutes. Vous devez agir maintenant pour résoudre le problème le plus rapidement possible.

Suivez le lien ci-dessous pour finaliser le processus et régler l'état de votre compte

[Accéder à votre espace sécurisé](#)

Nous vous remercions de votre confiance

Cordialement,

Arnaud Le Roux  
Direction Qualité

# Le Phishing

C'est l'une des menaces les plus fréquentes. Cette attaque a pour but de récupérer des données personnelles, comme des identifiants et des mots de passe, ou des informations bancaires. Généralement, la victime est contactée par e-mail, SMS ou appel téléphonique.



Chère cliente, Cher client,

Lors de votre dernière opération bancaire, nous avons remarqué une activité inhabituelle sur votre compte.

Pour réactiver votre compte Vous devez mettre à jour vos informations, une fois ces dernières validées, le compte fonctionnera normalement.

L'ensemble du processus ne prendra que 5 minutes. Vous devez agir maintenant pour résoudre le problème le plus rapidement possible.

Suivez le lien ci-dessous pour finaliser le processus et régler l'état de votre compte

[Accéder à votre espace sécurisé](#)

Nous vous remercions de votre confiance

Cordialement,

Arnaud Le Roux  
Direction Qualité

**De :** E-service Clients BRED <BRED\_secureID9593.noreply@zwina.com>

**Envoyé :** Thursday, October 29, 2020 9:51:42 AM

**À :** prenom.nom@courriel.fr

**Objet :** Au sujet de la sécurité de votre compte! #Re-664366

nom d'expéditeur inhabituel

# 1. Les différentes menaces

Le Phishing

Les Malware

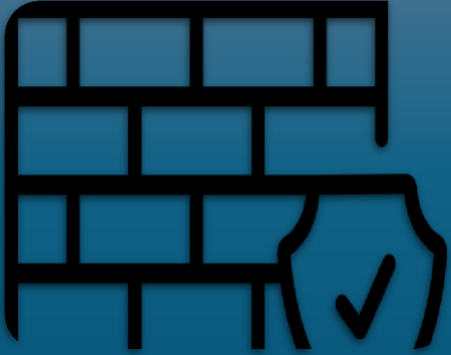


Les malwares, ou logiciels malveillants, sont des programmes créés pour nuire aux systèmes informatiques et en compromettre la sécurité. Ils se présentent sous plusieurs formes, chacun ayant un mode d'attaque spécifique. Par exemple :

- **Virus** : s'infiltrer dans des programmes légitimes et se propage d'un fichier à l'autre, souvent pour détruire ou corrompre des données.
- **Cheval de Troie** : se fait passer pour un programme inoffensif pour inciter l'utilisateur à le télécharger, permettant ensuite aux attaquants d'accéder au système.
- **Logiciels de ransomware** : bloque l'accès aux fichiers ou à l'ordinateur, exigeant une rançon pour les débloquent.
- **Logiciels espions** : surveille les activités de l'utilisateur à son insu, collectant des informations sensibles.

Les malwares se diffusent souvent par des pièces jointes d'email, des sites infectés, des liens non sécurisés ou des téléchargements douteux. Les conséquences peuvent aller du vol de données à la prise de contrôle complète d'un système, impactant à la fois les individus et les entreprises.

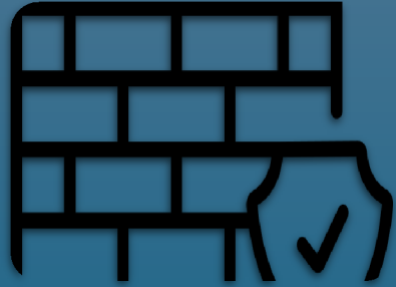
## 2. Solutions de protection



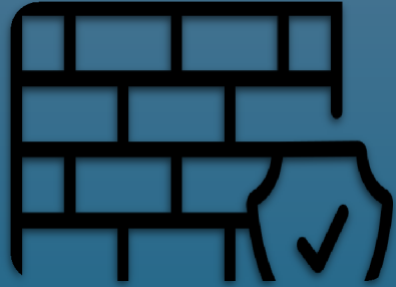
Pare-feu



Mises à jour et correctifs réguliers

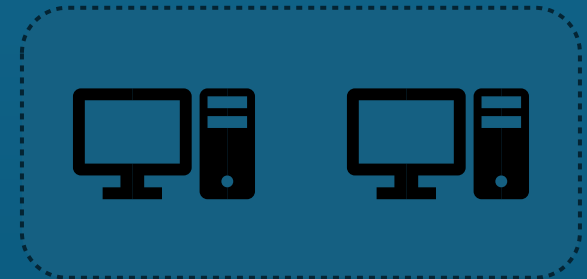


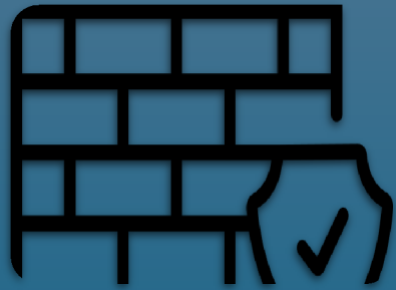
Le pare-feu a pour but de filtrer le trafic réseau, bloquant l'accès, par exemple, à des sites. Il fonctionne comme une barrière entre un réseau interne sécurisé et un réseau externe non sécurisé.



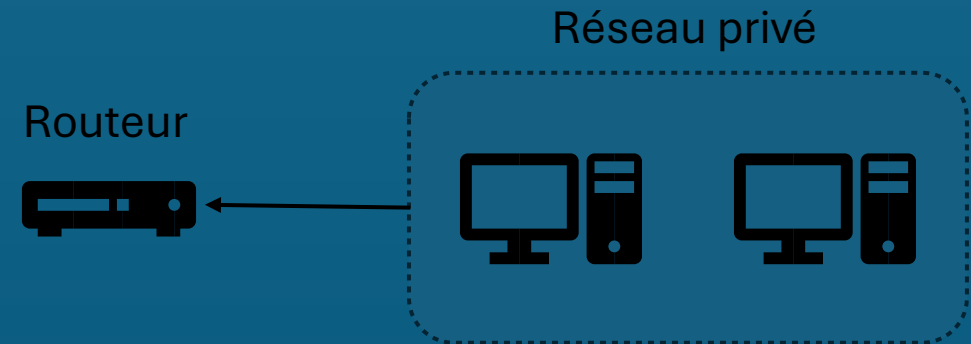
Le pare-feu a pour but de filtrer le trafic réseau, bloquant l'accès, par exemple, à des sites. Il fonctionne comme une barrière entre un réseau interne sécurisé et un réseau externe non sécurisé.

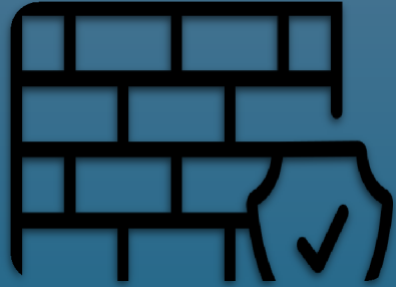
Réseau privé



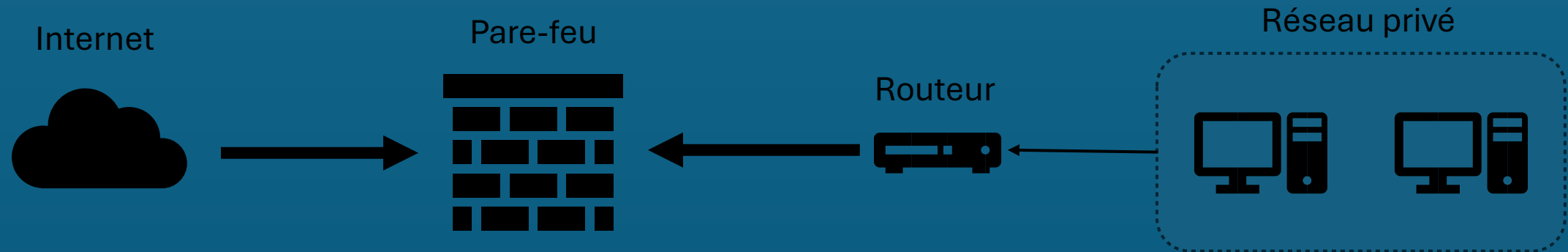


Le pare-feu a pour but de filtrer le trafic réseau, bloquant l'accès, par exemple, à des sites. Il fonctionne comme une barrière entre un réseau interne sécurisé et un réseau externe non sécurisé.

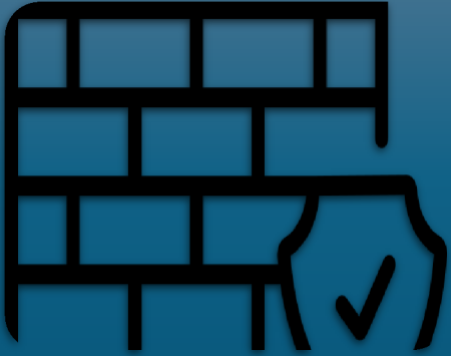




Le pare-feu a pour but de filtrer le trafic réseau, bloquant l'accès, par exemple, à des sites. Il fonctionne comme une barrière entre un réseau interne sécurisé et un réseau externe non sécurisé.



## 2. Solutions de protection



Pare-feu



Mises à jour et correctifs réguliers



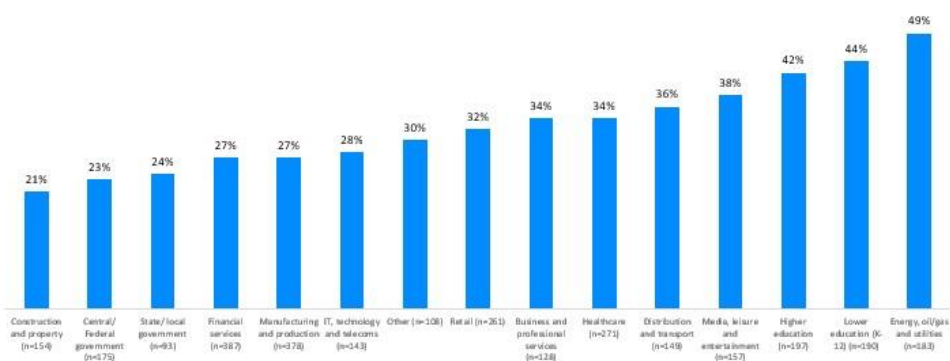
Il est primordial de mettre à jour son ordinateur, et les logiciels contenus dans ce dernier. Cela permet en effet de contrer une partie des attaques informatiques, et ainsi maintenir une certaine sécurité sur le réseau de l'entreprise.





Il est primordial de mettre à jour son ordinateur, et les logiciels contenus dans ce dernier. Cela permet en effet de contrer une partie des attaques informatiques, et ainsi maintenir une certaine sécurité sur le réseau de l'entreprise.

Percentage of ransomware attacks that started with exploited vulnerability



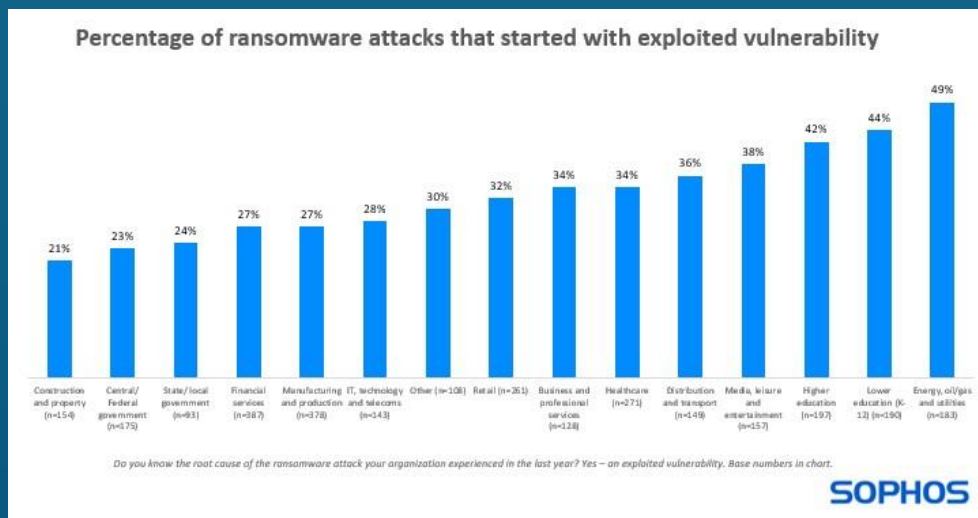
*Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes – an exploited vulnerability. Base numbers in chart.*

SOPHOS



Il est primordial de mettre à jour son ordinateur, et les logiciels contenus dans ce dernier. Cela permet en effet de contrer une partie des attaques informatiques, et ainsi maintenir une certaine sécurité sur le réseau de l'entreprise.

« Un tiers des attaques de ransomware commencent avec une vulnérabilité non corrigée »

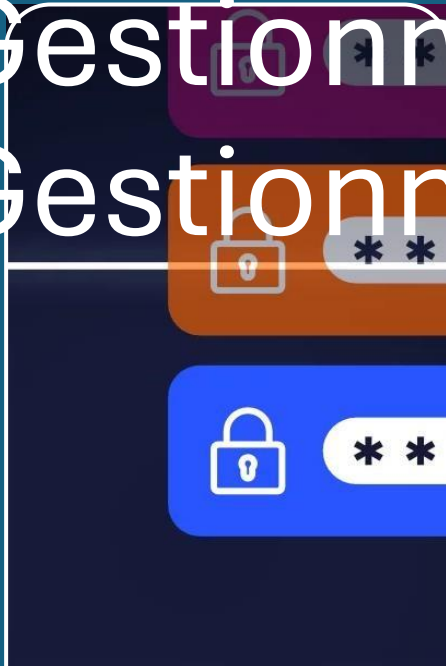


### 3. Sécurisation des mots de passe et des communications

HEURTEBISE JOHAN

### 3. Sécurisation des mots de passe et des communications

#### Gestionnaire de mot de passe



Pour protéger vos comptes personnels, mais surtout les comptes de l'entreprise, nous vous recommandons d'utiliser un gestionnaire de mot de passe. Néanmoins, il est préférable de ne pas utiliser les gestionnaires de mot de passe intégrés dans les navigateurs. L'utilisation d'un gestionnaire de mot de passe permet de mettre un

### 3. Sécurisation des mots de passe et des communications



Ne jamais partager son mot de passe



Éviter de réutiliser des mots de passe d'un service à un autre

## 4. Chiffrement des communications

La confidentialité des communications de l'entreprise est primordiale.

1. Des données sensibles sont traitées en permanence Il

est donc important de chiffrer les données.

## 4. Chiffrement des communications

### Chiffrement de bout en bout

- Seul l'expéditeur et le destinataire peuvent lire les messages.

### Chiffrement des connexions via VPN

- Le VPN crée un tunnel sécurisé et chiffré entre un appareil et un réseau privé.

### chiffrement sur les sites web

- Les sites utilisant le protocole HTTPS sont sécurisés

# Chiffrement de bout en bout

- Seul l'expéditeur et le destinataire peuvent lire les messages.



Ordi A

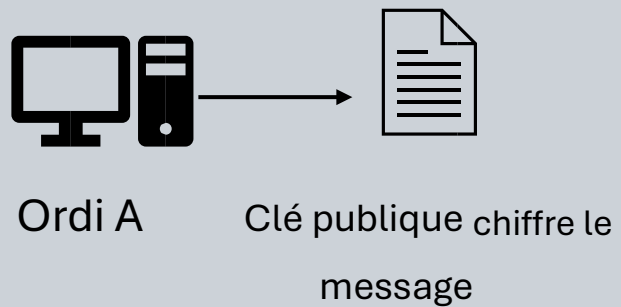


Ordi B



# Chiffrement de bout en bout

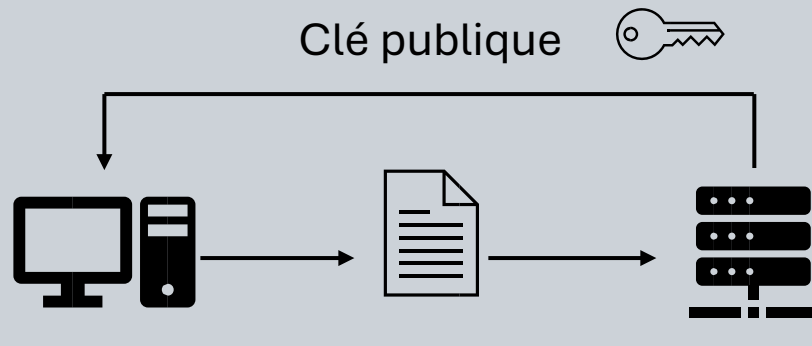
- Seul l'expéditeur et le destinataire peuvent lire les messages.



Ord B

# Chiffrement de bout en bout

- Seul



l'expéditeur et le destinataire peuvent lire les messages.

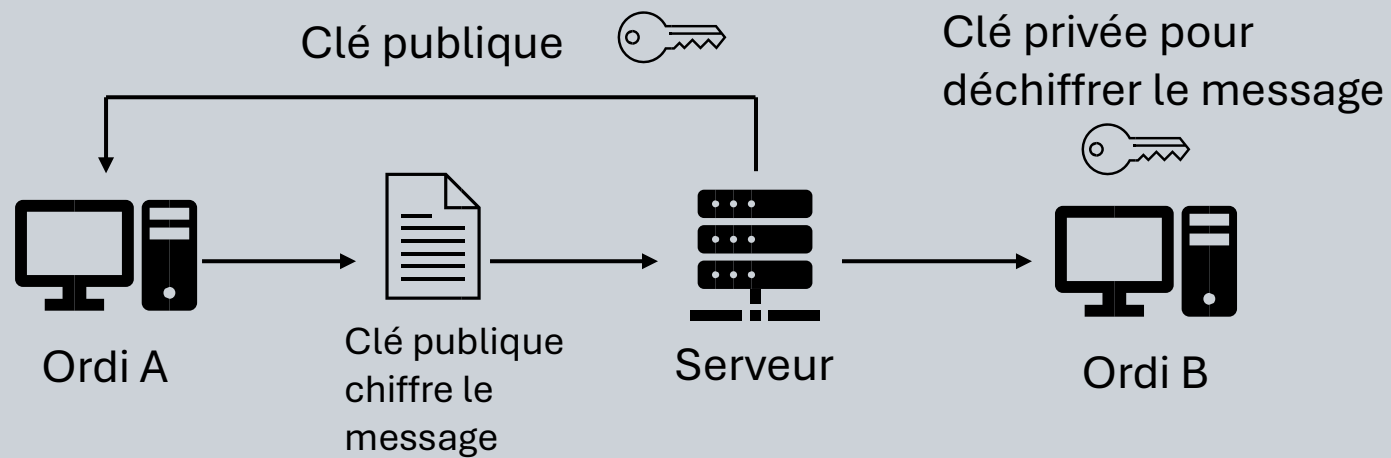


Ordre A

Clé publique chiffre le Serveur Ordre B

# Chiffrement de bout en bout

- Seul l'expéditeur et le destinataire peuvent lire les messages.



## 4. Chiffrement des communications

### Chiffrement de bout en bout

- Seul l'expéditeur et le destinataire peuvent lire les messages.

### Chiffrement des connexions via VPN

- Le VPN crée un tunnel sécurisé et chiffré entre un appareil et un réseau privé.

### chiffrement sur les sites web

- Les sites utilisant le protocole HTTPS sont sécurisés

## Chiffrement des connexions via VPN

- Le chiffrement par VPN est une technologie qui sécurise la connexion internet d'un utilisateur en créant un tunnel chiffré entre son appareil et un serveur VPN.

# Chiffrement des connexions via VPN

- Le chiffrement par VPN est une technologie qui sécurise la connexion internet d'un utilisateur en créant un tunnel chiffré entre son appareil et un serveur VPN.



Client

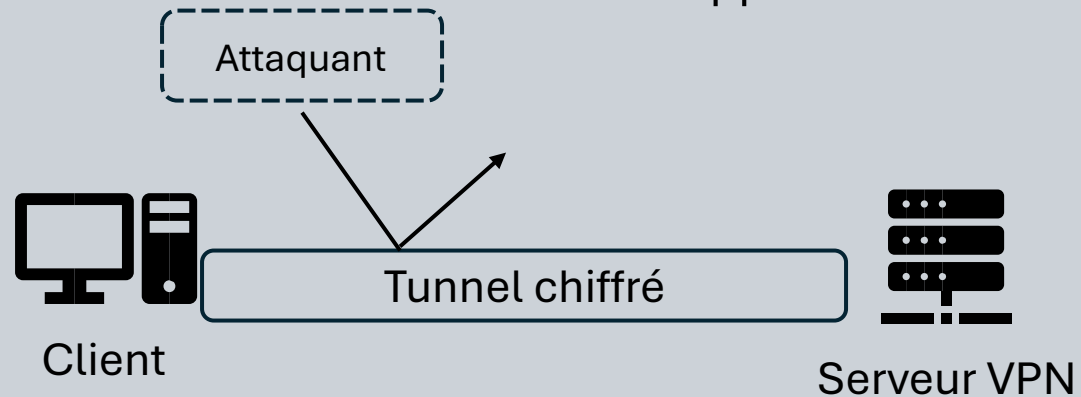
# Chiffrement des connexions via VPN

- Le chiffrement par VPN est une technologie qui sécurise la connexion internet d'un utilisateur en créant un tunnel chiffré entre son appareil et un serveur VPN.



# Chiffrement des connexions via VPN

- Le chiffrement par VPN est une technologie qui sécurise la connexion internet d'un utilisateur en créant un tunnel chiffré entre son appareil et un serveur VPN.





## 4. Chiffrement des communications

### Chiffrement de bout en bout

- Seul l'expéditeur et le destinataire peuvent lire les messages.

### Chiffrement des connexions via VPN

- Le VPN crée un tunnel sécurisé et chiffré entre un appareil et un réseau privé.

### chiffrement sur les sites web

- Les sites utilisant le protocole HTTPS sont sécurisés

# Protocoles de chiffrement sur les sites web

- Le protocole HTTPS est un protocole qui permet de sécuriser les communications sur le web, il permet de garder une certaine confidentialité des données. Il faut bien différencier le protocole HTTPS, qui est sécurisé, et le protocole HTTP qui ne l'est pas. Le protocole HTTPS offre un niveau de protection beaucoup plus élevé.

# 5. Usage personnel des ordinateurs de l'entreprise

L'utilisation des équipements de l'entreprise pour la navigation personnelle possède des risques importants.

Ex : Ne pas ouvrir des mails personnels

Ces pratiques augmentent le risque d'infection par des logiciels malveillants, phishing, etc.

## 6. Sauvegardes régulières et formation des employés

### Sauvegardes Fréquentes

- Les sauvegarde fréquentes sont importante en cas d'attaque.

### Formation et Vigilance

- La meilleure défense reste la vigilance de chacun.

## Sauvegardes Fréquentes

- Les sauvegardes fréquente sont importantes en cas d'attaque. Car en cas d'attaque, nous pouvons récupérer les données de l'entreprise. Ces données sont sauvegardées de manière sécurisée.

## 6. Sauvegardes régulières et formation des employés

### Sauvegardes Fréquentes

- Les sauvegarde fréquentes sont importante en cas d'attaque.

### Formation et Vigilance

- La meilleure défense reste la vigilance de chacun.

## Formation et Vigilance

- La meilleure défense reste la vigilance de chacun. Bien que les outils technologiques soient essentiels, la vigilance est indispensable pour créer une sécurité fiable et durable. Un utilisateur conscient et prudent est l'une des premières lignes de défense contre les cyberattaques.

# Conclusion

Se sensibiliser   l'hygi ne informatique et   la cybers curit 



# Bibliographie

- MOOC de l'ANSII
- Cisco
- <https://news.sophos.com/en-us/2024/04/03/unpatched-vulnerabilities-the-most-brutal-ransomwareattack-vector/>
- <https://www.malekal.com/le-chiffrement-bout-en-bout-quest-ce-que-cest-et-comment-ca-marche/>