

REPUBLIQUE DU SENEGAL



Un peuple-Un but-Une foie

Ministère de l'enseignement supérieur, de la recherche et de l'innovation

Direction de l'Enseignement Supérieur Privé



**Exposé sur la sensibilisation à l'hygiène
informatique et à la cybersécurité**

Présenté par:

Mouhamadou Lamine Dieng

Fatimata Zahra Lo

Athoumani Chaarani

Encadré par:

Mr ismaïla Fall

Année académique: 2023-2024

13/03/2024

Partie 1: Notions d'hygiène informatique et Panorama des Menaces.....	3
Introduction.....	3
Contexte de la sensibilisation.....	3
Politiques de sécurité.....	4
L'importance d'une politique de sécurité informatique.....	8
Pratiques d'hygiène informatique.....	9
Rôles et responsabilités.....	13
Outils et technologies de sécurité.....	14
Panorama des menaces.....	18
Conclusion.....	21
Partie 2: Applications Pratiques.....	21
Intégrité, confidentialité et gestionnaire de mots de passe.....	21
1. Objectif.....	21
2. Intégrité des données.....	21
3. Chiffrement des données sensibles.....	23
★ Le chiffrement symétrique.....	23
★ Le chiffrement asymétrique.....	24
• Générez une paire de clés de chiffrement RSA.....	25
• Chiffrer et déchiffrer les données sensibles.....	26
• Signez numériquement des données et vérifiez la signature.....	27
• Générez une clé de chiffrement AES et chiffrer/déchiffrer les données sensibles.....	28
4. Utilisation d'un gestionnaire de mots de passe.....	30
• Installez le gestionnaire de mots de passe fiable et sécurisé comme Keepass 2.....	30
• Protéger l'accès au gestionnaire avec un mot de passe principal fort.....	32
• Créez des mots de passe forts et uniques pour chaque compte et service.....	35
• Copie et ouverture de la base de données dans une autre machine ou smartphone.....	37

Objectifs:

Notre rapport s'articulera autour de deux grandes parties:

Dans la première partie, nous verrons les Notions d'hygiène informatique et le Panorama des Menaces dans le système informatique actuel, en insistant sur l'usage des bonnes pratiques d'hygiène.

Dans la seconde partie, nous nous focaliserons sur des applications pratiques assurant l'intégrité et la confidentialité des données ainsi que l'utilisation d'un gestionnaire de mots de passe(keepass 2).

Partie 1: Notions d'hygiène informatique et Panorama des Menaces

Introduction

L'hygiène informatique est un ensemble de bonnes pratiques essentielles pour garantir la sécurité et la protection des données numériques. Dans un monde de plus en plus connecté, la cybersécurité est devenue une préoccupation majeure pour les individus et les organisations. Ainsi, l'hygiène informatique consiste à vous entraîner à penser de manière proactive à la cybersécurité, tout comme vous le faites avec votre hygiène personnelle quotidienne, afin de résister aux menaces et aux problèmes de sécurité en ligne. Pour mieux comprendre les enjeux liés à la sécurité informatique, il est important d'explorer le panorama des menaces qui peuvent mettre en péril la confidentialité et l'intégrité des informations.

Contexte de la sensibilisation

La sensibilisation à l'hygiène informatique et à la cybersécurité revêt une importance capitale dans le contexte actuel marqué par la prolifération des menaces numériques. En effet, avec l'évolution rapide de la technologie, l'essor du BYOD (Bring Your Own Device) qui permettent aux employés d'utiliser leurs propres appareils pour le travail, et l'interconnexion croissante des

systèmes informatiques, les cyberattaques sont devenues de plus en plus sophistiquées et répandues. De nombreuses cyberattaques profitent d'une manière ou d'une autre des employés d'une organisation, en exploitant leur négligence ou en les incitant à agir par le biais d'un hameçonnage ou d'une attaque d'ingénierie sociale. Ainsi, sensibiliser les individus et les organisations à ces enjeux permet de les préparer à faire face aux diverses menaces en ligne, telles que les logiciels malveillants, les attaques par hameçonnage, les ransomwares, etc.

En comprenant les risques associés à l'utilisation d'Internet et en adoptant de bonnes pratiques en matière de sécurité informatique, les utilisateurs peuvent contribuer à renforcer la protection de leurs données personnelles et professionnelles. La sensibilisation permet également de promouvoir une culture de la sécurité au sein des organisations, en encourageant la mise en place de mesures préventives et réactives pour contrer les cybermenaces.

Politiques de sécurité

Une politique de cybersécurité fournit des orientations aux employés d'une organisation sur la manière d'agir pour protéger les informations sensibles de l'entreprise. Les entreprises disposent généralement de plusieurs politiques de sécurité qui couvrent divers sujets, notamment la sécurité informatique, la sécurité du courrier électronique et l'utilisation d'appareils personnels pour le travail dans le cadre d'une politique. Les politiques de sécurité informatique doivent être conçues pour identifier et traiter les risques de sécurité informatique d'une organisation, selon les trois objectifs fondamentaux de la sécurité informatique (également appelés "triade de la CIA") que sont:

La confidentialité: Protection des données sensibles contre l'exposition à des parties non autorisées.

L'Intégrité: Garantir que les données n'ont pas été modifiées pendant qu'elles sont stockées ou en transit.

La Disponibilité: Fournir un accès continu aux données et aux systèmes aux utilisateurs légitimes.

❖ Politiques de mots de passe :

→ Les politiques de mots de passe exigent souvent que les employés utilisent des mots de passe complexes, comprenant une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Il existe des outils tels que kaspersky password pour vérifier la sécurité de vos mots de passe(de faible à fort).

Exemples:



FR ▼ FAQ

passer



Il est grand temps de changer de mot de passe !

- Mauvaise nouvelle
⚠ Mots fréquemment utilisés
- Ce mot de passe est apparu 14737 fois dans une base de données de mots de passe ayant fait l'objet d'une fuite.

✓ **Bon mot de passe!**

- Votre mot de passe est résistant au piratage.
- Votre mot de passe n'apparaît dans aucune base de données ayant fait l'objet d'une fuite.

Votre mot de passe peut être craqué avec un ordinateur de bureau standard en environ...

10000+ siècles

→ Il est généralement recommandé aux employés de ne pas partager leurs mots de passe avec d'autres personnes et de les changer régulièrement, par exemple tous les 90 jours.

→ L'utilisation de l'authentification à deux facteurs: Lorsqu'un utilisateur tente de se connecter à un compte protégé par l'authentification à deux facteurs, il devra fournir à la fois son mot de passe (premier facteur) et un code généré par l'application d'authentification ou envoyé par SMS (deuxième facteur). Cette combinaison de facteurs rend plus difficile pour les pirates informatiques d'accéder à un compte, même s'ils ont réussi à obtenir le mot de passe..

❖ **Politiques d'utilisation des appareils personnels sur le réseau d'entreprise :**

Les entreprises ont souvent des politiques claires concernant l'utilisation des appareils personnels sur leur réseau, tels que les ordinateurs portables, les smartphones ou les tablettes.

- ➔ Ces politiques peuvent inclure des exigences telles que l'installation de logiciels de sécurité approuvés, le chiffrement des données sensibles, et l'interdiction de certaines activités potentiellement risquées, comme le téléchargement de logiciels non autorisés.
- ➔ En outre, les employés peuvent être tenus de signaler tout incident de sécurité ou toute perte d'appareil personnel utilisé pour accéder au réseau de l'entreprise.

L'objectif est de définir clairement les règles et les procédures d'utilisation des actifs de l'entreprise. Il s'agit d'informations destinées à la fois aux utilisateurs finaux et au personnel chargé des technologies de l'information et de la sécurité.

L'importance d'une politique de sécurité informatique

Une sécurité informatique est une trace écrite des règles et politiques de sécurité informatique d'une organisation. Cela peut être important pour plusieurs raisons, notamment :

- **Protection des données sensibles** : Une politique de sécurité informatique aide à protéger les données sensibles de l'organisation, telles que les informations clients, les données financières et les secrets commerciaux, contre les accès non autorisés, les fuites et les pertes.

- **Prévention des cyberattaques** : En mettant en place des contrôles de sécurité appropriés, une politique de sécurité informatique aide à réduire les risques de cyberattaques telles que les violations de données, les ransomwares et les perturbations du réseau.
- **Préserve la réputation de l'entreprise** : Les violations de données et les cyberattaques peuvent entraîner une perte de confiance des clients, des partenaires commerciaux et du public envers l'organisation. Une politique de sécurité solide contribue à maintenir la réputation et la crédibilité de l'entreprise.
- **Réduction des risques financiers** : Les incidents de sécurité informatique peuvent entraîner des coûts importants pour une organisation, tels que les frais de récupération des données, les amendes réglementaires et les pertes financières. Une politique de sécurité efficace aide à réduire ces risques financiers.
- **Amélioration de la productivité** : En assurant la disponibilité et l'intégrité des systèmes informatiques, une politique de sécurité informatique contribue à maintenir la productivité des employés en évitant les interruptions causées par des incidents de sécurité.

- **Réponse aux incidents:** En cas de violation de données ou d'autres incidents de sécurité, il est essentiel de réagir correctement et rapidement. Une politique de sécurité informatique définit les actions à entreprendre en cas d'incident.
- **Conformité réglementaire:** De nombreuses réglementations, telles que le GDPR et l'ISO, exigent qu'une organisation dispose de politiques et de procédures de sécurité en place et documentées. L'élaboration de ces politiques est nécessaire pour atteindre et maintenir la conformité réglementaire.

Pratiques d'hygiène informatique

Voici quelques bonnes pratiques d'hygiène informatique encouragées pour assurer la sécurité des systèmes et des données :

★ Protéger vos appareils

Protéger les appareils revient à:

- à mettre en place un antivirus sur chaque poste utilisateur
- **désactiver/désinstaller** les applications et services inutilisés, pour ne pas laisser de failles potentiellement exploitables par des hackers.
- **chiffrer vos données**, afin de préserver leur confidentialité en cas de perte ou de vol de matériel.
- **désactiver les ports inutilisés de vos périphériques** (imprimantes, PC, etc...), ces derniers pouvant constituer une porte d'entrée vers votre réseau d'entreprise.
- configurer le plus finement possible les clients de messagerie pour qu'ils bloquent un maximum de courriers malveillants/indésirables.

★ sécuriser votre réseau

- déployer un pare-feu de type UTM afin de filtrer les contenus web douteux et bloquer les tentatives d'intrusion.
- Séparer par des cloison les différents réseaux, par exemple en séparant le réseau wifi « invité » du réseau interne
- utiliser des protocoles sécurisés (SSH, TLS, etc...) afin de protéger les échanges d'informations entre vos différents périphériques
- contrôler le trafic sur votre réseau
- inciter les utilisateurs à ne pas connecter d'appareils personnels au réseau de l'entreprise, pour éviter les risques d'infection par virus ou les failles de sécurité.

★ Sécurisation des réseaux Wi-Fi :

Protéger les réseaux Wi-Fi avec des mots de passe forts, chiffrer les données transmises sur le réseau à l'aide du protocole WPA2 ou WPA3, et désactiver la diffusion du nom du réseau (SSID) pour renforcer la sécurité.

★ Vérification régulière des mises à jour logicielles :

Il est essentiel de maintenir à jour les logiciels, y compris le système d'exploitation, les applications et les programmes, pour corriger les vulnérabilités connues et renforcer la sécurité du système.

★ Utilisation de logiciels antivirus et de pare-feu :

Les logiciels antivirus peuvent aider à détecter et à supprimer les logiciels malveillants, tandis que les pare-feu peuvent bloquer les tentatives d'accès non autorisées au système.

★ Contrôle d'accès :

Le contrôle d'accès logique se divise en trois éléments clés : **l'authentification, l'autorisation et la traçabilité.**

→ Authentification :

L'authentification est le processus par lequel l'identité d'un utilisateur est vérifiée pour s'assurer qu'il est bien celui qu'il prétend être. Cela peut impliquer l'utilisation de mots de passe, de codes PIN, de cartes à puce, d'empreintes digitales ou d'autres méthodes pour vérifier l'identité de l'utilisateur.

→ Autorisation :

Une fois qu'un utilisateur est authentifié, l'autorisation détermine les actions et les ressources auxquelles cet utilisateur est autorisé à accéder. Cela implique de définir les droits et les privilèges d'accès pour chaque utilisateur en fonction de son rôle ou de ses responsabilités au sein du système.

→ Traçabilité :

La traçabilité consiste à enregistrer et à suivre les activités des utilisateurs une fois qu'ils ont été authentifiés et autorisés. Cela permet de garder une trace des actions effectuées par les utilisateurs, de détecter les comportements suspects et de faciliter les enquêtes en cas d'incident de sécurité.

→ Systèmes d'exploitation :

Assurez-vous de maintenir à jour votre système d'exploitation (comme Windows, macOS, Linux) en installant les dernières mises à jour de sécurité. Les correctifs de sécurité corrigent les vulnérabilités qui pourraient être exploitées par des attaquants.

→ Logiciels et applications :

Mettez à jour régulièrement tous les logiciels et applications que vous utilisez, y compris les navigateurs web, les lecteurs PDF, les suites bureautiques, etc. Les logiciels obsolètes peuvent présenter des failles de sécurité qui pourraient être exploitées.

→ Firmware du matériel :

Assurez-vous de maintenir à jour le firmware de vos périphériques matériels tels que les routeurs, les imprimantes et les caméras de sécurité. Les mises à jour du firmware peuvent corriger des vulnérabilités de sécurité et améliorer les performances.

→ Automatisation des mises à jour :

Activez les options d'automatisation des mises à jour lorsque c'est possible. Cela garantit que les mises à jour critiques sont installées dès qu'elles sont disponibles, réduisant ainsi le risque d'exploitation des vulnérabilités.

→ Sauvegarde avant les mises à jour majeures :

Avant d'installer des mises à jour majeures, assurez-vous de sauvegarder vos données importantes pour éviter toute perte en cas de problème lors de la mise à jour.

★ anticiper les risques

En matière de cybersécurité, le risque zéro n'existe pas car les pirates trouvent toujours de nouveaux moyens d'atteindre leur but. En plus des mesures de protection déjà mises en place, il vaut donc mieux assurer vos arrières. C'est pourquoi nous préconisons à minima de réaliser régulièrement des sauvegardes de vos données d'entreprise. Ainsi que des logiciels et tout autres éléments

indispensables à la réalisation de vos tâches quotidiennes. Par exemple, en cas d'attaque par ransomware ces sauvegardes constitueront votre Graal pour remettre sur pied votre activité rapidement

Rôles et responsabilités

Les rôles et les responsabilités de l'utilisateur sont cruciaux pour assurer la sécurité et la fiabilité des systèmes informatiques.

1. Sécurité des données : L'utilisateur doit veiller à la sécurité de ses données en mettant en place des mesures de protection telles que l'utilisation de mots de passe forts, le chiffrement des données sensibles et la sauvegarde régulière des fichiers importants. Il doit également éviter de partager des informations confidentielles avec des sources non fiables.

2. Mises à jour et maintenance : L'utilisateur a la responsabilité de maintenir son système d'exploitation, ses logiciels et ses applications à jour en installant les dernières mises à jour et correctifs de sécurité. Cela permet de prévenir les vulnérabilités et les failles de sécurité qui pourraient être exploitées par des cybercriminels.

3. Sensibilisation à la sécurité : L'utilisateur doit être conscient des menaces potentielles en ligne telles que les logiciels malveillants, les attaques par hameçonnage et les rançongiciels. Il doit adopter des pratiques sécurisées telles que l'utilisation de logiciels antivirus, l'éducation sur les techniques d'ingénierie sociale et la prudence lors de l'ouverture de pièces jointes ou de clics sur des liens suspects.

4. Utilisation responsable des ressources : L'utilisateur doit faire un usage responsable des ressources informatiques en évitant le gaspillage de bande passante, en éteignant les appareils inutilisés et en respectant les politiques de l'entreprise en matière d'utilisation des ressources informatiques.

5. Respect de la vie privée : L'utilisateur doit respecter la vie privée des autres en ne partageant pas d'informations confidentielles sans autorisation, en respectant les politiques de confidentialité des sites web et des applications, et en protégeant ses propres informations personnelles.

Outils et technologies de sécurité

L'objectif principal des outils de sécurité informatique est de contrôler l'accès au réseau, de protéger le flux d'informations sensibles et de prévenir les attaques malveillantes visant les systèmes de télécommunications, le transport d'informations et le contenu des communications.

Voici une présentation des outils et technologies de sécurité utilisés pour renforcer la posture de sécurité :

- **Outils de détection et de prévention des menaces :**

Logiciel antivirus Windows Defender: Il s'agit d'un outil intégré dans les systèmes d'exploitation Windows qui aide à détecter et à bloquer les logiciels malveillants, les virus et autres menaces potentielles pour la sécurité de l'ordinateur.

Voici quelques éléments clés sur le fonctionnement de Windows Defender :

- ➔ **Analyse en temps réel** : Windows Defender surveille constamment les fichiers et les activités sur votre ordinateur pour détecter et bloquer les menaces potentielles dès qu'elles sont identifiées.
- ➔ **Mises à jour régulières** : Les définitions de virus de Windows Defender sont constamment mises à jour pour garantir une protection contre les dernières menaces en ligne.
- ➔ **Analyse planifiée** : Vous pouvez également planifier des analyses régulières de votre système pour rechercher des logiciels malveillants et des virus.
- ➔ **Protection contre les programmes potentiellement indésirables (PUP)** : Windows Defender peut également détecter et bloquer les programmes potentiellement indésirables qui pourraient compromettre la sécurité de votre ordinateur.

- **Solutions de chiffrement des données sensibles :**

Mkcert : Mkcert est un outil open source qui permet de générer facilement des certificats locaux pour sécuriser les connexions HTTPS lors du développement ou du test d'applications web sans avoir à passer par des autorités de certification externes.. Il simplifie le processus de création et d'installation de certificats SSL/TLS.

La solution de chiffrement des données sensibles mkcert fonctionne en créant des certificats auto-signés localement pour sécuriser les connexions HTTPS lors du développement ou du test d'applications web.

Voici comment cela fonctionne :

- ➔ **Génération de certificats auto-signés** : Lorsque vous utilisez mkcert, vous spécifiez les **domaines** pour lesquels vous souhaitez générer des certificats SSL/TLS auto-signés.
Mkcert génère ensuite localement des **paires de clés privées et publiques** pour chaque domaine spécifié.
Ces clés sont utilisées pour créer un **certificat auto-signé** qui sera reconnu comme valide pour le domaine spécifié.
- ➔ **Installation des certificats** : Une fois les certificats générés, mkcert les installe dans votre système d'exploitation.
Les certificats sont ajoutés au **magasin de certificats de confiance** de votre système, ce qui permet aux navigateurs et aux applications de les reconnaître comme des certificats valides.
- ➔ **Utilisation dans le développement** : Vous pouvez ensuite utiliser ces certificats pour sécuriser les connexions HTTPS entre votre navigateur et votre application web locale pendant le développement.
Les certificats auto-signés créés par mkcert permettent d'établir des connexions chiffrées sans afficher **d'alertes de sécurité** liées à des certificats non valides.

OpenSSL : OpenSSL est une bibliothèque open source qui fournit des implémentations de protocoles de sécurité tels que SSL (Secure Sockets Layer) et TLS (Transport Layer Security). Il est largement utilisé pour le chiffrement des données sensibles et la sécurisation des communications sur Internet.

Voici une explication des étapes pratiques de chiffrement des données sensibles avec OpenSSL :

→ Génération de clés privées et publiques :

- La première étape consiste à générer une paire de clés : une clé privée et une clé publique.

La clé privée est conservée secrète et utilisée pour chiffrer et déchiffrer les données, tandis que la clé publique est partagée pour chiffrer les données.

Création d'un certificat auto-signé :

- À l'aide de la clé privée, un certificat auto-signé est généré en incluant des informations telles que le nom du propriétaire, la période de validité et d'autres détails.

Ce certificat est ensuite utilisé pour établir l'identité du serveur lors de connexions SSL/TLS.

→ Configuration du serveur avec OpenSSL :

Le serveur web est configuré pour utiliser le certificat généré par OpenSSL, permettant ainsi d'établir des connexions sécurisées via HTTPS.

Les paramètres de chiffrement, les protocoles pris en charge et d'autres options de sécurité peuvent être configurés pour renforcer la sécurité des communications.

→ Établissement de connexions sécurisées :

Lorsqu'un client se connecte au serveur via HTTPS, OpenSSL gère la négociation des paramètres de sécurité, y compris le chiffrement à utiliser, en s'appuyant sur le certificat pour valider l'identité du serveur.

Les données échangées entre le client et le serveur sont chiffrées à l'aide des clés générées, assurant la confidentialité et l'intégrité des informations.

Panorama des menaces

Le panorama des menaces dans le domaine de la cybersécurité est vaste et en constante évolution. Comprendre les principales sources de menaces est essentiel pour renforcer la résilience des systèmes d'information. Explorer ce panorama permet d'anticiper les risques et de mettre en place des mesures adaptées. Voici un aperçu des menaces les plus courantes :

1. Hameçonnage & Ingénierie Sociale

Les attaques d'hameçonnage impliquent l'utilisation de techniques de manipulation psychologique pour tromper les utilisateurs et les inciter à divulguer des informations sensibles telles que des mots de passe ou des informations financières. Les attaques de phishing demeurent l'une des principales menaces. Les attaquants utilisent des techniques sophistiquées pour tromper les utilisateurs et les inciter à divulguer des informations sensibles. Les différents types d'hameçonnage :

- ❖ **La manipulation de liens** est un procédé par lequel un acteur malveillant incite un utilisateur à cliquer sur un lien vers un site web contrefait.

- ❖ **L'hameçonnage par sms** est une forme d'hameçonnage par laquelle on essaie de tromper une victime en lui envoyant des informations privées par le biais d'un message texte. La forme la plus courante d'hameçonnage par sms est un texte contenant un lien qui télécharge automatiquement un logiciel malveillant. Un logiciel malveillant installé peut voler des données personnelles telles que des identifiants bancaires, des données de géolocalisation ou des numéros de téléphone provenant de listes de contacts, dans le but de voir le virus se multiplier de manière exponentielle.

- ❖ **L'hameçonnage vocal (vishing)** est une escroquerie vocale, ou un type d'hameçonnage partant d'un appel téléphonique ou d'une interaction humaine afin d'inciter les victimes à partager des informations telles que des informations personnelles ou privées, des mots de passe ou d'autres données personnelles.

- ❖ **La contrefaçon de sites Internet** consiste à faire passer un site Internet malveillant pour un site authentique, afin d'inciter les visiteurs à divulguer leurs

informations sensibles, telles que leurs coordonnées bancaires, leurs mots de passe et leurs numéros de carte de crédit.

2. Fraude Interne

La fraude interne se produit lorsque des personnes au sein d'une organisation abusent de leur accès et de leurs privilèges pour commettre des actes malveillants, tels que le vol d'informations confidentielles ou la manipulation de données.

3. Intrusion Informatique

Les intrusions consistent en l'accès non autorisé à un système ou à un réseau. Les attaquants exploitent souvent des vulnérabilités pour pénétrer dans un environnement informatique.

4. Intrusion Informatique

Les intrusions consistent en l'accès non autorisé à un système ou à un réseau. Les attaquants exploitent souvent des vulnérabilités pour pénétrer dans un environnement informatique.

5. Virus Informatique

Les virus informatiques sont des logiciels malveillants capables de se propager et d'infecter d'autres programmes. Ils peuvent causer des dommages en détruisant des fichiers ou en altérant le fonctionnement d'un système.

6. Déni de Service

Les attaques par déni de service (DDoS) visent à submerger un service, un site web ou un réseau en générant un trafic excessif, rendant ainsi les ressources indisponibles pour les utilisateurs légitimes.

7. Ransomware

Les attaques par ransomware ciblent souvent les entreprises en chiffrant leurs données et en demandant une rançon. Ces attaques peuvent causer des perturbations importantes et des pertes financières.

8. Ver (Worm)

Un ver est un type de logiciel malveillant capable de se propager de manière autonome à travers les réseaux informatiques. Il exploite souvent les vulnérabilités

des systèmes pour se propager rapidement. La segmentation réseau et les mises à jour de sécurité sont des mesures préventives importantes.

9. Cheval-de-Troie (Trojan)

Les chevaux de Troie sont des programmes malveillants qui se font passer pour des logiciels légitimes mais qui ouvrent des portes dérobées dans un système. Ils permettent à un attaquant d'accéder et de contrôler le système à distance. Éviter les téléchargements suspects et utiliser des solutions de sécurité sont des moyens de protection.

10. Bombe Logique

Une bombe logique est une partie de code malveillant qui est activée lorsqu'une condition spécifique est remplie. Cela peut inclure des actions destructrices, telles que la suppression de fichiers critiques. La vigilance lors de l'exécution de scripts et l'utilisation de pare-feu sont des précautions importantes.

Conclusion

La cybercriminalité est le fruit d'une longue évolution économique conduite par le développement accru des N.T.I.C. Cette nouvelle forme de criminalité connaît une ampleur exponentielle difficile à évaluer. La difficulté d'appréhender des cyberattaques sur le réseau Internet tient en partie au fait que ce réseau est un moyen de communication mondial permettant de véhiculer tous types de données. Ainsi, les pratiques d'hygiène informatique sont cruciales pour assurer la fiabilité, la sécurité et la confidentialité des systèmes informatiques dans un monde de plus en plus connecté et dépendant de la technologie..

Partie 2: Applications Pratiques

Intégrité, confidentialité et gestionnaire de mots de passe

1. Objectif

Le but de cette partie pratique est de mettre en œuvre des mesures de sécurité pour garantir l'intégrité et la confidentialité des données, et de savoir utiliser un gestionnaire de mots de passe pour renforcer la sécurité des informations personnelles.

2. Intégrité des données

De manière générale, l'intégrité des données désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

Et pour garantir l'intégrité des données on calcule le hash en utilisant les outils de calcul de hash comme openssl, certutil et Get-FileHash.

La "hash" d'un fichier, également connue sous le nom de "hachage de fichier", est une valeur unique générée à partir du contenu du fichier en utilisant un algorithme de hachage. Ce hachage est généralement utilisé pour vérifier l'intégrité des données du fichier, car toute modification apportée au fichier entraînera un changement dans la valeur du hachage. Cela permet de détecter toute altération ou corruption du fichier. Certains des algorithmes de hachage couramment utilisés sont MD5, SHA-1, SHA-256, etc.

Dans cet exemple, nous allons télécharger une image ubuntu server 20.04 et vérifier son intégrité en comparant les empreintes.

[Empreinte du fichier disponible sur le site de Ubuntu](#)

Nom du fichier	ubuntu-20.04.6-live-server-amd64.iso
Format	ISO
Taille	1,39 Go
Version	20.04.6
Date de sortie	14 mars 2023
Éditeur	Canonical
Hash (SHA-256)	b8f31413336b9393ad5d8ef0282717b2ab19f007df2e9ed5196c13d8f9153c8b
Architecture	x64 (64 bits)
Langue	Multilingual
Avis	★★★★★ (0 avis)

- Calcul du hash en utilisant openssl et la fonction de hachage sha256

sous linux:

```
root@zahra-VirtualBox:/home/zahra/Téléchargements# openssl dgst -sha256 /home/zahra/Téléchargements/ubuntu-20.04.6-live-server-amd64.iso
SHA256(/home/zahra/Téléchargements/ubuntu-20.04.6-live-server-amd64.iso)= b8f31413336b9393ad5d8ef0282717b2ab19f007df2e9ed5196c13d8f9153c8b
root@zahra-VirtualBox:/home/zahra/Téléchargements#
```

Sous windows:

```
PS C:\Users\PC1\Documents> Get-FileHash .\ubuntu-20.04.6-live-server-amd64.iso -Algorithm SHA256 | Format-List

Algorithm : SHA256
Hash      : B8F31413336B9393AD5D8EF0282717B2AB19F007DF2E9ED5196C13D8F9153C8B
Path      : C:\Users\PC1\Documents\ubuntu-20.04.6-live-server-amd64.iso
```

- Calcul du hash en utilisant certutil:

syntaxe sous windows:

`certutil -hashfile <chemin_du_fichier> <type_de_hachage>`

```
PS C:\Users\PC1> certutil -hashfile C:\Users\PC1\Documents\ubuntu-20.04.6-live-server-amd64.iso sha256
Hachage SHA256 de C:\Users\PC1\Documents\ubuntu-20.04.6-live-server-amd64.iso :
b8f31413336b9393ad5d8ef0282717b2ab19f007df2e9ed5196c13d8f9153c8b
CertUtil: -hashfile La commande s'est terminée correctement.
PS C:\Users\PC1>
```

Le calcul de la fonction de hachage avec l'algorithme SHA256 donne le même résultat que le hash publié sur le site de ubuntu. On en déduit que le fichier est intègre.

3. Chiffrement des données sensibles

Le chiffrement est une forme de **cryptographie** consistant à brouiller des données afin de les rendre incompréhensibles à première vue. Une information textuelle écrite en langage clair, c'est-à-dire lisible par un être humain, est ainsi convertie en un langage codé avec pour résultat un texte illisible ou « chiffré ».

Il existe plusieurs méthodes de chiffrement. En effet, des besoins différents en matière de sécurité aboutissent au développement de solutions variées. Cependant, on distingue aujourd'hui deux principaux modèles de chiffrement des informations : le chiffrement symétrique et le chiffrement asymétrique.

★ Le chiffrement symétrique

Le chiffrement symétrique consiste en l'utilisation d'une clé secrète unique, à la fois pour chiffrer le message original et pour décoder le texte. Expéditeur et destinataire des données chiffrées se servent tous deux de la même clé secrète pour réaliser le chiffrement puis le déchiffrement. Il y a donc symétrie dans la technique utilisée pour chacune des opérations.

Un exemple d'algorithme de chiffrement symétrique largement utilisé est l'algorithme AES (Advanced Encryption Standard).

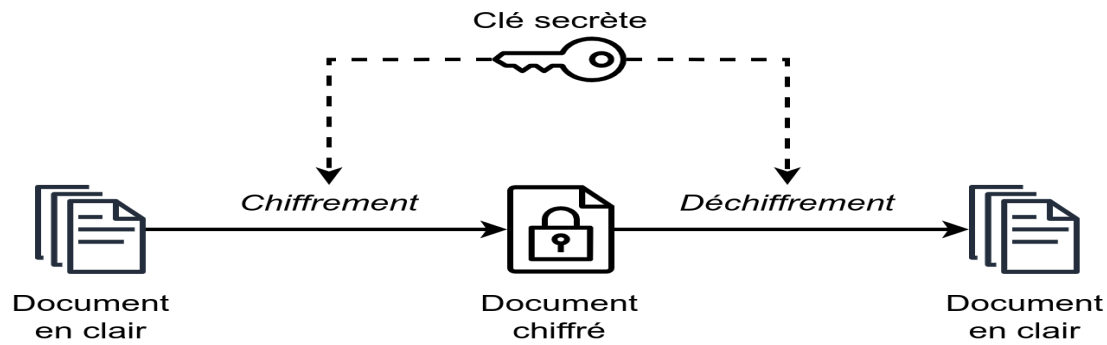
On a aussi:

DES (Data Encryption Standard)

3DES (Triple Data Encryption Standard)

Blowfish

Twofish,...



★ Le chiffrement asymétrique

Le chiffrement asymétrique, ou cryptographie à clé publique, utilise deux clés cryptographiques différentes : l'une pour chiffrer les données et l'autre pour les déchiffrer. La première se nomme « clé publique », tout simplement parce que cette dernière est accessible à tout le monde. La seconde, la clé de déchiffrement ou « clé privée », est quant à elle conservée par le destinataire uniquement. Seul ce dernier a donc la capacité de déchiffrer le message.

Voici quelques exemples d'algorithmes de chiffrement asymétrique couramment utilisés :

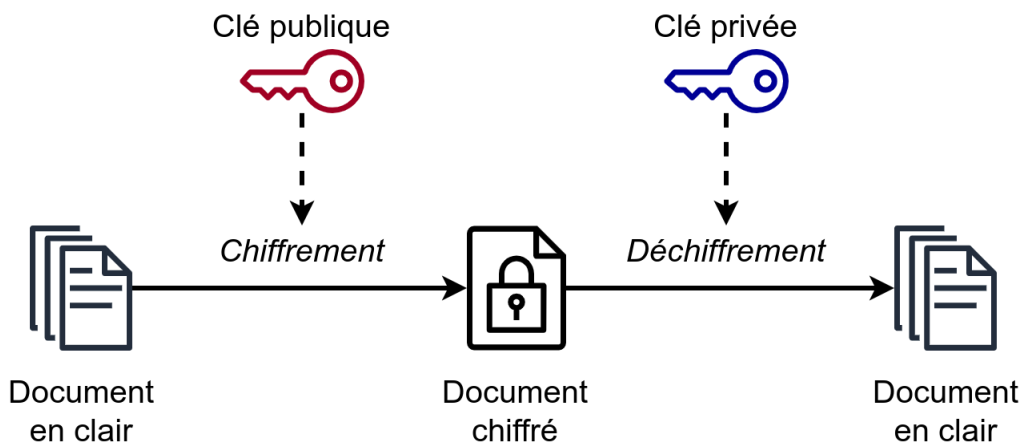
RSA (Rivest-Shamir-Adleman) : L'algorithme de chiffrement asymétrique le plus largement utilisé pour le cryptage des données et la sécurisation des communications.

DSA (Digital Signature Algorithm) : Utilisé principalement pour les signatures numériques et la vérification de l'authenticité des données.

Diffie-Hellman : Un protocole de chiffrement à clé publique utilisé pour l'échange sécurisé de clés cryptographiques sur un canal non sécurisé.

ECC (Elliptic Curve Cryptography) : Un algorithme de chiffrement asymétrique basé sur les courbes elliptiques, offrant un niveau élevé de sécurité avec des clés plus courtes.

ElGamal : Un algorithme de chiffrement asymétrique utilisé pour le cryptage des données et les échanges de clés sécurisées.



- **Générez une paire de clés de chiffrement RSA.**

Pour générer une paire de clés de chiffrement RSA, vous pouvez utiliser des outils comme OpenSSL en ligne de commande. Voici comment vous pouvez le faire :

Utilisez la commande suivante pour générer une clés privée RSA :

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

Cette commande générera une clé privée RSA de 2048 bits et l'enregistrera dans un fichier nommé `private_key.pem`.

```

root@zahra-VirtualBox:/# openssl genpkey -algorithm RSA -out cle_privee.pem
.....+++++
.....+++++
root@zahra-VirtualBox:/# ls
bin          doc1         lib          lost+found  messagetst.txt  oui
boot        Documents  lib32       media      mnt            point
cdrom       etc         lib64       mercia_chiff.bin  montage        prive_cle_zahra.pem
cle_privee.pem  exo.py     libx32     message_chiffre.bin  opt          proc
dev         home       lo         messagetst_chiffre.txt  oubli        public_cle_zahra.pem
root@zahra-VirtualBox:/#
  
```

Ensuite, vous pouvez extraire la clé publique à partir de la clé privée en utilisant la commande suivante :

```
openssl rsa -pubout -in cle_privee.pem -out cle_public.pem
```

Cette commande extrait la clé publique correspondante à partir de la clé privée et l'enregistre dans un fichier nommé `cle_public.pem`.


```

root@zahra-VirtualBox:/# openssl rsa -pubout -in cle_privee.pem -out cle_public.pem
writing RSA key
root@zahra-VirtualBox:/# ls
bin          doc1         lib32        mercia_chiff.bin    opt           public_cle_zahra.pem  swapfile
boot         Documents   lib64        message_chiffre.bin  oubli         root                sys
cdrom        etc         libx32       messagest_chiffre.txt oui           run                tmp
cle_privee.pem  exo.py      lo          messagest.txt       point         sbin               tpmaths
cle_public.pem  home       lost+found  mnt                 prive_cle_zahra.pem snap              usr
dev          lib         media       montage             proc          srv                var

```

● Chiffrer et déchiffrer les données sensibles.

Pour chiffrer et déchiffrer des données sensibles avec RSA en utilisant OpenSSL, on suit les étapes suivantes :

→ Chiffrement de données sensibles :

Avec la clé publique, Chiffrer les données:

Supposons que vous ayez un fichier contenant les données sensibles nommé message.txt.

Utilisez la commande suivante pour chiffrer les données avec la clé publique cle_public.pem :

openssl rsautl -encrypt -inkey cle_public.pem -pubin -in data.txt -out message_chiffre000.bin

Cette commande chiffre les données du fichier message.txt en utilisant la clé publique et enregistre le résultat chiffré dans un fichier message_chiffre000.bin.

```

root@nemesis: /home/cloud
GNU nano 4.8 message.txt
Dieu a dit de partager mais pas le contraire

root@nemesis:/home/cloud# openssl rsautl -encrypt -inkey cle_public.pem -pubin -in message.txt -out message_chiffre000.bin
root@nemesis:/home/cloud# ls
Rhythmbox  Documents  message_chiffre000.bin  Modèles  Public  Téléchargements
cle_public.pem  Images  message.txt            Musique  snap  Vidéos
root@nemesis:/home/cloud#

```

```

root@zahra-VirtualBox:/# ls
bin          doc1         lib32        mercia_chiff.bin    montage        proc           srv
boot         Documents   lib64        message_chiffre000.bin  opt           public_cle_zahra.pem  swapfile
cdrom        etc         libx32       message_chiffre.bin  oubli         root           sys
cle_privee.pem  exo.py      lo          messagest_chiffre.txt oui           run            tmp
cle_public.pem  home       lost+found  messagest.txt       point         sbin           tpmaths
dev          lib         media       montage             prive_cle_zahra.pem snap           usr
root@zahra-VirtualBox:/# cat message_chiffre000.bin
-qNp(=[  ]b0Q[  ]z+_+;+/_+T
0?h_+9h+!+TU+|+q+yR++W++++y++++u+Z'i+6mG5+*+3+Y3+Û+V+e+kC}Û%!+
AF+*+x+`+++++p+`++X+lv +);f++[+H5+†(T+M+root@zahra-VirtualBox:/#
root@zahra-VirtualBox:/#

```

→ Déchiffrement de données chiffrées :

Déchiffrer les données avec la clé privée :

En Utilisant la commande suivante pour déchiffrer les données chiffrées dans message_chiffre000.bin en utilisant la clé privée cle_privee.pem :

```
openssl rsautl -decrypt -inkey cle_privee.pem -in message_chiffre000.bin
```

Cette commande déchiffre les données chiffrées dans message_chiffre000.bin en utilisant la clé privée.

```
root@zahra-VirtualBox:/#  
root@zahra-VirtualBox:/# openssl rsautl -decrypt -inkey cle_privee.pem -in message_chiffre000.bin  
Dieu a dit de partager mais pas le contraire  
root@zahra-VirtualBox:/#
```

● Signez numériquement des données et vérifiez la signature

Pour chiffrer et signer un message sous Linux avec OpenSSL afin que le destinataire puisse le lire en clair et vérifier la signature, vous pouvez suivre ces étapes :

Chiffrer le message avec la clé publique du destinataire :

```
openssl rsautl -encrypt -inkey cle_public_ch.pem -pubin -in test.txt -out test.enc
```

Assurez-vous d'avoir la clé publique du destinataire au format PEM dans un fichier (dans cet exemple, cle_public_ch.pem) et que le message à chiffrer est dans un fichier texte (dans cet exemple, test.txt).

```
root@zahra-VirtualBox:/# nano test.txt  
root@zahra-VirtualBox:/# openssl rsautl -encrypt -inkey cle_public_ch.pem -pubin -in test.txt -out test.enc  
root@zahra-VirtualBox:/# cat test.enc  
}g0WY0A3000_N,0Q0;+#:0T0+00dQ0000qi0.t000)}00 00=Z00W  
  A0*Z00003t00b00*z^0Q0  
          N(00zi<0S00%00  
          r0004]&w0@70;+0Q-000l0Cd+P0>'0n00m[r00  
000>00Z03$QIX.0eI000`N00i05)*jLE000Nup00^l0'c0N  
]000}00ysL0zE00t Zt00\0root@zahra-VirtualBox:/#
```

Signer le message avec votre clé privée :

Vous pouvez signer le message en utilisant la commande OpenSSL suivante :

```
openssl dgst -sha256 -sign cle_privee.pem -out test.bin test.enc
```

Assurez-vous d'avoir votre clé privée au format PEM dans un fichier (dans cet exemple, cle_privee.pem) et que le message chiffré est dans un fichier (dans cet exemple, test.enc).

Envoyer le message chiffré seulement et le message chiffré et signé et au destinataire.

```

root@zahra-VirtualBox:/#
root@zahra-VirtualBox:/# openssl dgst -sha256 -sign cle_privee.pem -out test.bin test.enc
root@zahra-VirtualBox:/# scp test.bin chaarani@192.168.100.189:/home/chaarani
chaarani@192.168.100.189's password:
test.bin
100% 256 47.7KB/s 00:00
root@zahra-VirtualBox:/#

```

```

root@zahra-VirtualBox:/# scp test.bin chaarani@192.168.100.189:/home/chaarani
chaarani@192.168.100.189's password:
test.bin
100% 256 45.5KB/s 00:00
root@zahra-VirtualBox:/#

```

Vérifier la signature du message :

Le destinataire peut vérifier la signature en utilisant la commande OpenSSL suivante :

```
openssl dgst -sha256 -verify cle_public.pem -signature test.bin test.enc
```

Assurez-vous que le destinataire possède votre clé publique au format PEM dans un fichier (dans cet exemple, cle_public.pem).

et déchiffrer le message!

```

root@frede:/home/chaarani# openssl dgst -sha256 -verify cle_public.pem -signature test.bin test.enc
Verified OK
root@frede:/home/chaarani# openssl rsautl -decrypt -inkey cle_privee.pem -in test.enc
message confidentiel signé!
root@frede:/home/chaarani#

```

● Générez une clé de chiffrement AES et chiffrer/déchiffrer les données sensibles

L'AES (Advanced Encryption Standard) est un algorithme de chiffrement symétrique largement utilisé pour sécuriser des données. Voici un exemple d'utilisation d'AES avec OpenSSL en ligne de commande. Assurez-vous d'avoir OpenSSL installé sur votre système.

Voici les étapes à suivre pour générer une clé de chiffrement AES et chiffrer/déchiffrer des données sensibles en utilisant OpenSSL :

→ Génération d'une clé de chiffrement AES :

Générer une clé AES :

On utilise la commande suivante pour générer une clé AES de 256 bits et l'enregistrer dans un fichier cle_aes.txt:

```
openssl rand -hex 32 > cle_aes.txt
```

Cette commande génère une clé AES aléatoire de 256 bits et l'enregistre dans un fichier cle_aes.txt.

```
root@zahra-VirtualBox:/# openssl rand -hex 32 > cle_aes.txt
root@zahra-VirtualBox:/#
```

→ Chiffrer les données sensibles avec AES :

Chiffrer les données avec la clé AES :

Supposons que vous ayez un fichier contenant les données sensibles nommé test.txt.

On utilise la commande suivante pour chiffrer les données avec la clé AES à partir du fichier cle_aes.txt :

```
openssl enc -aes-256-cbc -in test.txt -out fichier_chiffre.enc -kfile cle_aes.txt -pbkdf2
```

Cette commande chiffre les données du fichier test.txt en utilisant la clé AES contenue dans cle_aes.txt et enregistre le résultat chiffré dans un fichier fichier_chiffre.enc.

```
root@zahra-VirtualBox:/# openssl enc -aes-256-cbc -in test.txt -out fichier_chiffre.enc -kfile cle_aes.txt -pbkdf2
root@zahra-VirtualBox:/# cat fichier_chiffre.enc
Salted__Pt
EdN000090000root@zahra-VirtualBox:/#
root@zahra-VirtualBox:/#
```

→ Déchiffrer les données chiffrées avec AES :

Déchiffrer les données avec la clé AES :

Utilisez la commande suivante pour déchiffrer les données chiffrées dans fichier_chiffre.enc en utilisant la clé AES à partir du fichier cle_aes.txt :

```
openssl enc -d -aes-256-cbc -in fichier_chiffre.enc -out fichier_dechiffre.txt -kfile cle_aes.txt -pbkdf2
```

Cette commande déchiffre les données chiffrées dans fichier_chiffre.enc en utilisant la clé AES contenue dans cle_aes.txt et enregistre le résultat déchiffré dans un fichier_dechiffre.txt.

```
root@zahra-VirtualBox:/# openssl enc -d -aes-256-cbc -in fichier_chiffre.enc -out fichier_dechiffre.txt -kfile cle_aes.txt -pbkdf2
root@zahra-VirtualBox:/#
root@zahra-VirtualBox:/#
```

```
root@zahra-VirtualBox:/# cat fichier_dechiffre.txt
message confidentiel signé!
root@zahra-VirtualBox:/#
```

4. Utilisation d'un gestionnaire de mots de passe

Un gestionnaire de mots de passe est un outil logiciel conçu pour stocker de manière sécurisée et gérer les identifiants de connexion, tels que les noms d'utilisateur et les mots de passe, pour différents comptes en ligne.

Le logiciel libre KeePass est un gestionnaire de mots de passe qui ne dépend d'aucun service tiers, d'aucune société tierce. À la différence de ses concurrents comme le tristement célèbre Lastpass, le logiciel libre KeePass ne stocke pas les mots de passe sur un service Cloud en ligne, mais sur le disque dur de l'utilisateur. KeePass fait partie du kit de sensibilisation du grand public à la sécurité informatique, qui a été mis en place par l'État français à partir du 14 juin 2018. KeePass permet de générer des mots de passe aléatoires, longs et complexes que l'utilisateur n'a pas besoin de mémoriser.

En plus de ses performances, KeePass est recommandé parce que sa qualité de logiciel libre est une garantie de sécurité et de confidentialité que les logiciels commerciaux (privateurs de liberté) ne peuvent pas offrir.

- **Installez le gestionnaire de mots de passe fiable et sécurisé comme KeePass 2**

La version officielle de KeePass est un logiciel Windows disponible sur keepass.info. Il est fortement conseillé de prendre la version 2.x, qui dispose de beaucoup plus de fonctionnalités. Elle est disponible en deux variantes : *Installer* pour une installation sur PC, et *Portable* pour un lancement depuis une clé USB

← → ↻ keepass.info/download.html



KeepPass
mot de passe sécurisé

Maison

- Actualités locales
- Forums
- Liste des fonctionnalités
- Captures d'écran

Obtenir KeePass

- Téléchargements
- Traductions
- Plugins/Ext.

Informations / WWW


- Aide

Obtenir KeePass - Téléchargements

Ici vous pouvez télécharger KeePass :

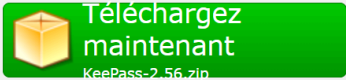
KeepPass 2.56

Programme d'installation pour Windows (2.56) :


KeePass-2.56-Setup.exe

Téléchargez le fichier EXE ci-dessus, exécutez-le et suivez les étapes du programme d'installation. Vous avez besoin de droits d'installation locaux (utilisez la version portable à droite, si vous n'avez pas de droits d'installation locaux).

Portable (2,56) :

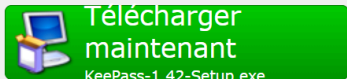

KeePass-2.56.zip

Téléchargez le package ZIP ci-dessus et décompressez-le dans votre emplacement préféré (clé USB, ...). KeePass fonctionne sans aucune installation supplémentaire et ne stockera aucun paramètre en dehors du répertoire de l'application.

Systèmes d'exploitation pris en charge : Windows 7/8/10/11 (chacun 32 bits et 64 bits), **Mono** (Linux, MacOS, BSD, ...).

KeepPass 1.42

Programme d'installation pour Windows (1.42) :













































KeePass-1.42-Setup.exe

Portables (1.42) :

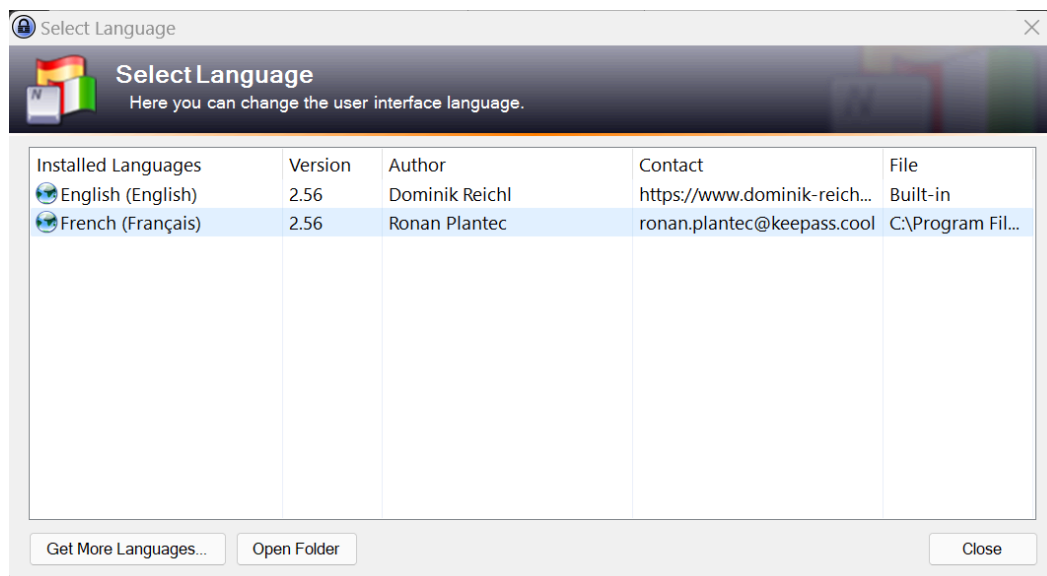

KeePass-1.42.zip

Par défaut, le logiciel est en anglais. Il faut télécharger le pack linguistique français avec la même version que le keepass installé (ici **2.56**), le dézipper et copier le fichier « French.lgnx » dans le dossier «*C:\Program Files\KeePass Password Safe 2\Languages* ».

keepass.info/translations.html

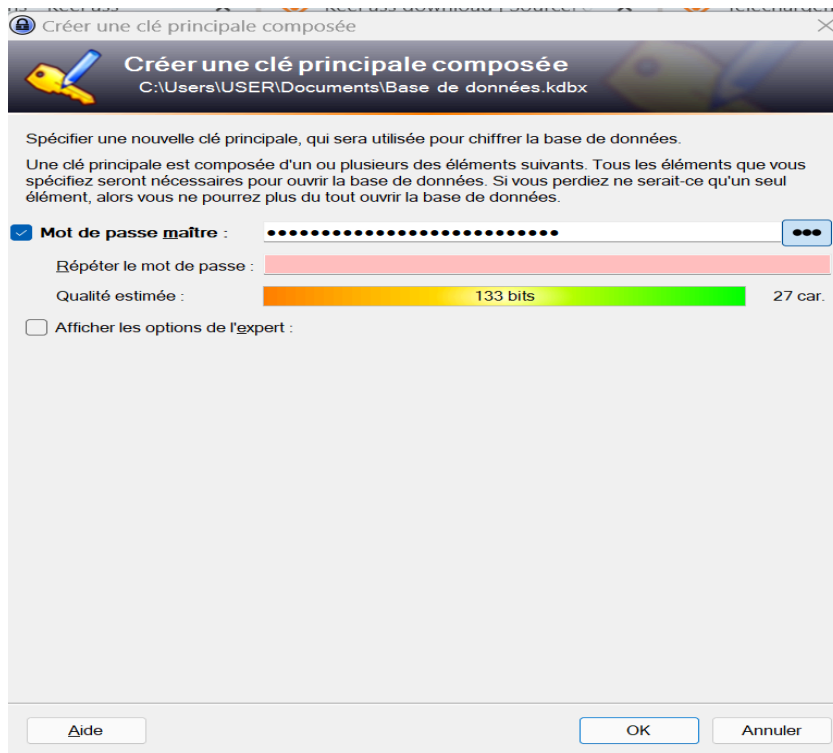
	danois	Christian Staal	 [1,41+]	 [2,53+]
	Néerlandais	Hilbrand Edskes	 [1,42+]	 [2,56+]
	Anglais	Dominique Reichl	Intégré, pas de téléchargement	
	estonien	A. Kuhlberg (2.x), A. Viiland (1.x)	 [1,14+]	 [2,38+]
	finlandais	Kari Eveli	 [1,42+]	 [2,56+]
	Français	Ronan Plantec	 [1,42+]	 [2,56+]
	Galicien	Jésus Amieiro	 [1,10+]	[2.x] N/A
	Allemand	Dominique Reichl	 [1,42+]	 [2,56+]
	grec	M. Ntovas-Tzimas (2.x), S. Vradelis (1.x)	 [1,25+]	 [2,56+]
	hébreu	Oded Eli (2.x), Tomer Shalev (1.x)	 [1,04+]	 [2,35+]
	hongrois	Pc et Pc Szerviz (2.x), Zotius et Herka (1.x)	 [1,42+]	 [2,56+]
	islandais	Stefan Örvar Sigmundsson	[1.x] N/A	 [2,45+]
	indonésien	Vaksin.com	[1.x] N/A	 [2,23+]
	italien	Luca 'Hexaae' Longone	 [1,39+]	 [2,56+]
	Japonais	Hiroki Matsumoto	 [1,42+]	 [2,56+]
	coréen	Incrisis (2.x), PD Beom (1.x)	 [1,04+]	 [2,56+]

Ensuite, il suffit de sélectionner la langue française dans le menu « *View -> Change language* ».

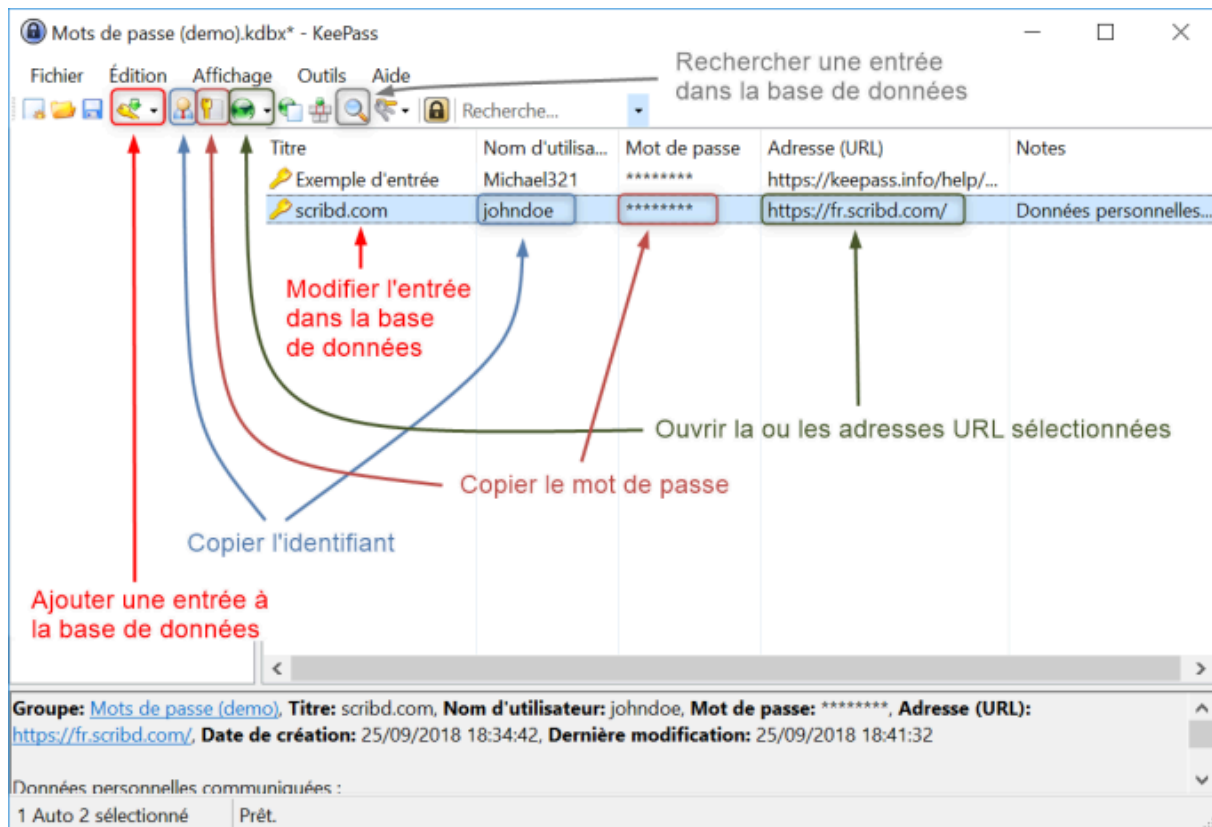


- **Protéger l'accès au gestionnaire avec un mot de passe principal fort**

Il faut d'abord aller dans « *Fichier-> Nouvelle...* » et définir un nom pour le nouveau fichier KDBX qui va contenir votre base de mots de passe. Ensuite, le plus important est de définir la clé principale. Plutôt que d'utiliser un mot de passe aléatoire, il est conseillé de créer une **longue phrase** constituée de quatre ou cinq mots choisis au hasard. Ce sera plus facile à mémoriser pour un niveau de sécurité équivalent. C'est important car vous allez utiliser cette phrase en permanence pour accéder aux mots de passe. L'usage de chiffres et de caractères spéciaux peut vite, dans ce contexte, devenir pesant.



Fenêtre principale de Keepass 2



● Configuration d'une nouvelle base de données

- Ouvrez KeePass.
- Cliquez sur "Fichier" dans la barre de menu.
- Sélectionnez "Nouveaux" .
- Choisissez l'emplacement et le nom de votre nouvelle base de données.
- Définissez un mot de passe fort pour protéger votre base de données.
- Configurez les paramètres de sécurité selon vos besoins.
- Enregistrez la nouvelle base de données.

Configurer une nouvelle base de données

Paramètres de la base de données

C:\Users\USER\Documents\Base de données.kdbx

Général Sécurité Compression Corbeille Avancé

Nom de la base de données :

Description de la base de données :
Saisir une courte description de la base de données ou laisser ce champ vide

Nom d'utilisateur par défaut pour les nouvelles entrées :

☐ Personnaliser la couleur de la base de données :

Aide OK Annuler

Base de données.kdbx* - KeePass

Fichier Groupe Entrée Rechercher Affichage Outils Aide

Recherche...

Base de données	Titre	Nom d'utilisat...	Mot de passe	Adresse (URL)	Remarques
Général	Exemple d'e...	Nom d'utilisat...	*****	https://keepas...	Remarques
Windows	Exemple d'e...	Michael321	*****	https://keepas...	
Réseau					
Internet					
Courriel					
Banque à domicile					

Groupe: [Base de données](#). Titre: Exemple d'entrée. Nom d'utilisateur: Nom d'utilisateur. Mot de passe: *****. Adresse (URL): <https://keepass.info/>. Date de création: 15/03/2024 19:08:39. Dernière modification: 15/03/2024 19:08:39.

Remarques

- **Créez des mots de passe forts et uniques pour chaque compte et service**


Ajout d'une entrée dans la base de données :

- Clic sur l'outil montrant la clé avec une flèche 


Modification d'une entrée dans la base de données :

- Double-clic sur le titre de l'entrée (ci-dessus : scribd.com)


Copie dans le presse-papier de l'identifiant de l'entrée sélectionnée :

- Double-clic sur l'identifiant (ci-dessus : johndoe)
- Clic sur l'outil montrant un buste avec une cravate 
- Raccourcis clavier : CTRL b


Copie dans le presse-papier du mot de passe de l'entrée sélectionnée :


- Double-clic sur le mot de passe (ci-dessus : *****)
- Clic sur l'outil montrant une clé verticale devant une page vide 
- Raccourcis clavier : CTRL c

Ouvrir l'URL de l'entrée sélectionnée dans le navigateur par défaut :

- Double-clic sur l'URL (ci-dessus : https://fr.scribd.com/)
- Clic sur l'outil montrant le globe terrestre 
- Raccourcis clavier : CTRL u


Rechercher dans la base de données :

- Clic sur l'outil montrant une loupe 
- Raccourcis clavier : CTRL f


 Ajouter une entrée


Ajouter une entrée
Cr  er une nouvelle entr  e de mot de passe.

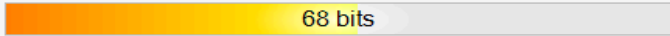

G  n  ral | Avanc   | Propri  t  s | Saisie automatique | Historique

Titre : facebook Ic  ne : 

Nom d'utilisateur : mouhadieng209@gmail.com



Mot de passe : RAYMONDREDDINGTON2098 


Confirmation : 

Qualit   :  68 bits 21 car. 

Adresse (URL) : https://m.facebook.com/login/?locale=fr_FR

Remarques :

☐ Expire le : 07/03/2024 00:00:00  

 Outils OK Annuler

The screenshot shows the KeePass application window titled "Base de donn  es.kdbx - KeePass". The menu bar includes "Fichier", "Groupe", "Entr  e", "Rechercher", "Affichage", "Outils", and "Aide". The toolbar contains icons for file operations, search, and security. The "Database.kdbx" and "Base de donn  es.kdbx" tabs are visible. On the left, a tree view shows the "Base de donn  es" folder expanded, with sub-items: "G  n  ral", "Windows", "R  seau", "Internet", "Courriel", "Banque    domicile", and "Corbeille". The main table displays a single entry for "facebook" with the following details: "Nom d'utilis..." is "mouhadien...", "Mot de passe" is masked with "*****", and "Adresse (URL)" is "https://m.fa...". The "Remarques" column is empty.

- **Copie et ouverture de la base de données dans une autre machine ou smartphone.**

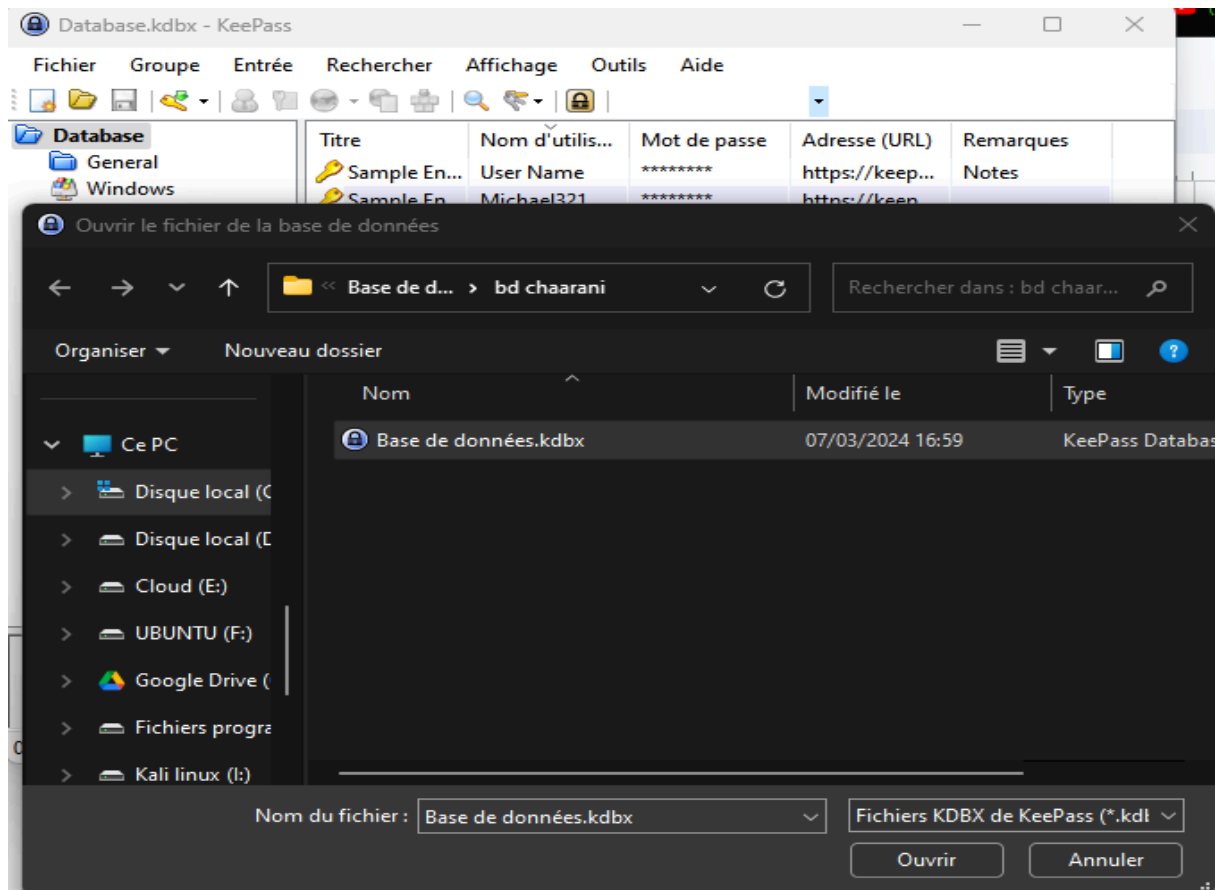
Pour copier et ouvrir la base de données KeePass sur une autre machine ou smartphone, voici les étapes à suivre:

Sur la machine d'origine :

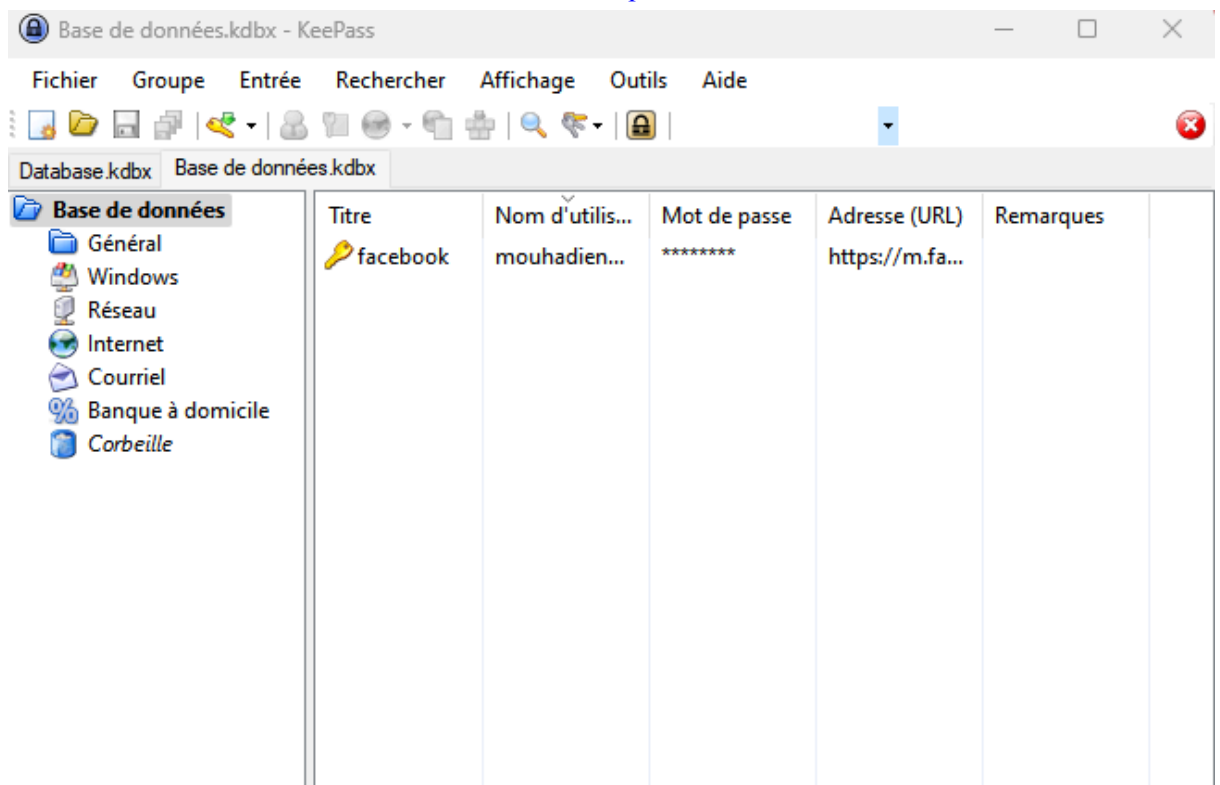
Copiez le fichier de la base de données KeePass (extension .kdbx) sur un support de stockage comme une clé USB ou un service de cloud.

Sur la nouvelle machine ou smartphone :

- Transférez le fichier de la base de données KeePass depuis le support de stockage vers l'appareil.
- Assurez-vous d'avoir KeePass installé sur l'appareil.
- Ouvrir KeePass
- Cliquer sur "Fichier" dans la barre de menu.
- Sélectionnez "Ouvrir base de données" ou "Open database".
- Chercher et sélectionner le fichier de la base de données KeePass que vous avez transféré.
- Entrez le mot de passe que vous avez défini lors de la création de la base de données.



Après avoir cliquer sur ouvrir, nous aurons sa base de donée dans notre machine et on pourra accéder aux contenus seulement si nous détenons son [mot de passe de sécurité](#).



CONCLUSION

En conclusion, notre rapport met en lumière l'importance cruciale des bonnes pratiques d'hygiène informatique pour contrer les menaces croissantes dans le paysage numérique actuel. Ainsi, nous avons souligné l'essence des notions d'hygiène informatique et mis en évidence les diverses menaces qui pèsent sur les systèmes informatiques, tout en mettant l'accent sur l'adoption de bonnes pratiques pour renforcer la sécurité.

La **sensibilisation à la cybersécurité** est une démarche essentielle pour tous. Elle permet de développer une meilleure compréhension des risques et d'adopter les bonnes pratiques pour se prémunir contre les cyberattaques. L'enjeu est de taille pour sécuriser notre avenir numérique et celui des générations à venir.

En combinant une compréhension approfondie des risques potentiels avec des solutions concrètes comme KeePass 2, il est possible de renforcer la sécurité de manière proactive et de préserver la confidentialité des données dans un environnement numérique en constante évolution.