Pour lutter contre les intrusions malveillantes, il faut sécuriser son espace de travail. Ainsi, il faut éviter les comportements à risques et avoir un logiciel de protection installé sur sa machine.

Pourquoi faut-il sécuriser son espace de travail ?

- Pour pouvoir accéder à nos ressources **quand on en éprouve le besoin** et **pour le temps nécessaire**.
- Pour pouvoir accéder à nos ressources **sans que celles-ci aient été modifiées**.
- Pour que mes données restent **confidentielles** (mot de passe, n° de carte, fichier, …).

Quels sont les risques ?

- La récupération de mes données personnelles,
- La prise de contrôle de mon ordinateur, ainsi que son exploitation pour lancer des attaques,
- Le détournement de mon IP personnelle (l'adresse internet permet d'identifier de manière unique mon ordinateur sur le réseau), l'usurpation d'identité,
- La perte de mes données, …

Qu'est-ce l'adresse IP ?

L'adresse IP est une « adresse » (un code) internet qui permet d'identifier de manière unique mon ordinateur sur le réseau ou sur internet. Elle géolocalise mon ordinateur et sert d'identifiant personnel pour toute autorité. Elle peut être statique (elle ne change pas) ou dynamique (elle change en fonction de certaines conditions).

Qu'est-ce qu'un logiciel ?

Un logiciel est un ensemble de fichiers permettant d'exécuter un programme informatique.
Parmi les logiciels, on distingue :

- les applications : logiciels destinés aux utilisateurs comme le traitement de texte, le navigateur, etc. ;
- les logiciels systèmes : logiciels proches de la machine qui permettent aux applications de communiquer avec le matériel.

Le système d'exploitation (Windows, MAC OS, Linux, Unix) est un logiciel système de base.
Chaque application est développée pour fonctionner avec un système d'exploitation spécifique.

Pour vérifier l'intégrité d'un fichier téléchargé et être certain qu'il est identique à l'original, il faut calculer la somme SHA-256 et vérifier qu'elle est identique au fichier original.

Trouver la somme SHA-256

1. Télécharger le fichier
2. Aller dans les téléchargements
3. Faire un clic droit dans une zone non vide tout en restant appuyé sur la touche Maj (⇧)
4. Cliquer sur : « Ouvrir la fenetre PowerShell ici »
5. Entrez ensuite la commande Get-FileHash .\NomDuFichier.iso –Algorithme SHA256
(Pensez à l'auto-complétion avec la touche TAB (⇄)).

I / Qui peut attaquer mon ordinateur ?

Un « hacker » informatique désigne un virtuose en informatique qui utilise ses compétences dans le but de résoudre un problème lié à la programmation, l'architecture matérielle d'un ordinateur, l'administration système, l'administration réseau, la sécurité informatique ou tout autre domaine de l'informatique.
Les médias associent souvent les hackers aux pirates, personne qui utilise ses compétences de façon nuisible, illégale.

En général, on distingue plusieurs types de hackers :

- Les « **White hat hackers** » sont des professionnels de la sécurité informatique.
- Les « **Black hat hackers** » ou **pirates** informatiques sont des cybers escrocs (ou cyber criminel). leurs buts est de gagner de l'argent en :
  - créant des virus (en détruisant ou contournant les protections des logiciels),
  - vendant des informations piratées,
  - extorquant de l'argent.
- Les **chapeaux gris ou Grey hat** n'ont pas de mauvaises intentions et sont souvent motivés par l'exploit informatique.
- Les **hacktivistes** agissent afin de défendre une cause, ils peuvent transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations

II / Quels sont les principaux types d'attaque informatique ?

Une **cyberattaque** est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

- **Le "spam"** ou pourriels est un simple courrier publicitaire non sollicité.

- Le **"spam" téléphonique** existe aussi. Il est généralement adressé à des fins de prospection commerciale mais peut également revêtir un caractère malveillant (incitation à appeler un numéro surtaxé, …).

- **L'arnaque au faux support technique** consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

- **L'arnaque aux faux ordres de virement** consiste pour le fraudeur à se faire passer pour un directeur en **usurpant son identité** et à vous demander de réaliser un virement à l'international.

- Le «**typosquatting**» : quand les pirates informatiques exploitent les fautes de frappe

- Le **"phishing" ou hameçonnage** consiste pour le fraudeur à se faire passer pour un organisme qui vous est familier (banque, administration fiscale, caisse de sécurité sociale…), en utilisant son logo et son nom. Vous recevez un courriel dans lequel il vous est demandé de "mettre à jour" ou de "confirmer suite à un incident technique" vos données.
  Leur but est de soutirer des informations confidentielles comme :

- Des données personnelles : nom, prénom, adresse postale ou de messagerie, numéro de téléphone…
- Des identifiants de connexion : nom d'utilisateur, mot de passe…
- Des informations bancaires : RIB, numéro de carte bancaire…

Autrefois facilement identifiables, ces arnaques par message électronique apparaissent de mieux en mieux réalisées et même les internautes les plus avertis peuvent parfois s'y méprendre.
Voici quelques éléments que vous devez observer avec attention :

- **Le corps du texte.** Attention aux éventuelles fautes d'orthographe, de grammaire…
- **L'adresse de messagerie de l'expéditeur.**
- **Le lien.**

- Le **"smishing"** (mot composé de SMS et phishing) consiste à transmettre des messages type SMS pour tromper des victimes en les incitants à agir immédiatement. En effet, nous avons plus confiance en nos SMS qu'en nos mails.

- **Chantage à l'ordinateur ou à la webcam piratés** (dit « **cryptoporno** ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés afin de vous soutirer de l'argent.
  Il prend généralement la forme d'un message reçu (souvent par courriel). Le cybercriminel annonce avoir des vidéos compromettantes qu'il menace de publier si la victime ne lui verse pas une rançon.

- Un **défacement** exploite la faille de sécurité d'un système d'exploitation d'un serveur web de manière à modifier la présentation d'un site internet. Les défaceurs attaquent les sites web principalement pour exprimer leur revendication. Ainsi les principales cibles sont des organisations gouvernementales ou des sites religieux.
  Lorsqu'un site web est défiguré, il doit se mettre hors ligne. Sa maintenance entraîne une grande perte de temps et d'énergie. L'image de l'organisation est endommagée puisqu'il ne paraît pas sécurisé.

- Une **attaque par l'homme du milieu** représente un pirate qui s'insère dans les communications entre un client et un serveur réseau :
  1. Le client se connecte à un serveur.
  2. Le pirate s'insère entre le client et le serveur. Il déconnecte le client et prend sa place. Il usurpe ainsi l'identité du client et continue le dialogue avec le serveur.

- Une **injection SQL** est devenue un problème courant qui affecte les sites Web exploitant des bases de données. Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur. Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies. Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et, dans certains cas, envoyer des commandes au système d'exploitation.

- **Une attaque par force brute :** Il s'agit de tester une à une, toutes les combinaisons possibles des mots de passe.

- **Une attaque par DNS** : L'objectif de cette attaque est de rediriger, à leur insu, des internautes vers des sites pirates.

III / Quels sont les différents types de logiciels malveillants ?

Un **logiciel malveillant** ou **malware** est un ensemble de programmes conçu par un pirate pour être implanté dans un système afin d'y déclencher une opération non autorisée ou d'en perturber le fonctionnement. Les logiciels malveillants peuvent être transmis via l'Internet, un réseau local ou par des supports tels que les clés USB, les disques durs externes, ...
Parmi les logiciels malveillants, on distingue :

- le virus : logiciel, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, **s'implante au sein des programmes en les parasitant**, **se duplique** à l'insu des utilisateurs et **produit ses effets dommageables** quand le programme infecté est exécuté ou quand survient un événement donné.
- le ver : **logiciel indépendant** (il ne s'implante pas au sein d'un autre programme) qui se transmet d'ordinateur à ordinateur par l'Internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. **Les vers sont souvent conçus pour saturer les ressources disponibles ou allonger la durée des traitements**. Ils peuvent aussi **détruire les données d'un ordinateur, perturber le fonctionnement du réseau ou transférer frauduleusement des informations**. Une bombe programmée est un **logiciel malveillant** qui se déclenche lorsque certaines conditions sont réunies.
- Un cheval de Troie (ou Troyen) est un logiciel au sein duquel a été dissimulé un programme malveillant qui peut par exemple **permettre la collecte frauduleuse, la falsification ou la destruction de données.** Le cheval de Troie ne se reproduit pas.
- Un logiciel publicitaire (ou adware) est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur.
- *Les rançongiciels* sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des victimes et réclament le paiement d'une rançon.

IV / Les sites sécurisés

Lors d'un achat, vérifier que le site est sécurisé (http**s**)
En effet, il existe 2 types de sites internet.

- ✓ Ceux dont l'adresse commence par « http:// ». (Site non sécurisé)
  Les données transmises en http transitent en clair.
  Évitez de faire vos achats sur les sites en « http:// » et ne créez par un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires, etc.) peuvent être interceptées par des tiers (cette condition est nécessaire, mais pas suffisante).

- ✓ Ceux dont l'adresse commence par « https:// ». (Site sécurisé)
  Le protocole https est une variante du protocole http incluant l'utilisation de canal de communication sécurisé. En effet, les informations seront cryptées (chiffrées).
  En général, au moment du paiement, un petit cadenas est visible dans l'adresse de votre navigateur.

V / Le chiffrement de bout en bout, c'est quoi ?

Le récepteur du message (Alice) génère une clé privée (A) et une clé publique (B).
Le récepteur du message (Alice) envoie sa clé publique (B) à un émetteur (Bob).
L'émetteur (Bob) chiffre son message avec la clé publique (B) du récepteur (Alice).
Le récepteur (Alice) déchiffre le message de l'émetteur (Bob) grâce à sa clé privée (A).
Seul le récepteur (Alice) pourra prendre connaissance des messages de l'émetteur (Bob).
Il suffit que l'émetteur (Bob) applique le même procédé que le récepteur (Alice) et cet échange de clés publiques leur permet une communication bidirectionnelle sécurisée.
La clé privée (A) est générée aléatoirement et la clé publique (B) est générée à partir de la clé privée.
On appelle cette méthode le chiffrement asymétrique.

Le chiffrement permet d'assurer la confidentialité des données, de certifier les échanges numériques et d'apporter une preuve numérique qu'un document n'a pas été modifié.

VI / Comment éviter les comportements à risque : les bonnes pratiques

Une bonne pratique est l'ensemble de nos actions qui contribue à sécuriser l'ordinateur :

- Installer des logiciels de protection :
  - Antivirus : logiciel possédant une base de données de signatures virales qui scanne les fichiers à la recherche de ces signatures dans leur code. Il les répare les fichiers infectés quand c'est possible ou les met en quarantaine pour empêcher la propagation du virus. (Kaspersky, bit defender). Il est nécessaire quand la connexion passe par un réseau WIFI public.
  - Pare-feu (firewall) est un système permettant de protéger l'ordinateur des intrusions extérieures par le réseau. Il agit comme un filtre entre le réseau et l'ordinateur.
  - Logiciel anti-espion (antispyware) pour éradiquer les logiciels espions (spywares).

- Sécuriser ses mots de passe
  - ✓ Avoir des mots de passe de 8 à 12 caractères minimum.
  - ✓ Caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).
  - ✓ Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance…).
  - ✓ Le même mot de passe ne doit pas être utilisé pour des accès différents.
  - ✓ Changer de mot de passe régulièrement (72 jours recommandé !)
  - ✓ Ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.
  - ✓ Ne pas utiliser des mots de passe avec des mots trouvés dans les dictionnaires.
  - ✓ Ne pas noter le mot de passe dans un post-it ou un document à côté.
  - ✓ Éviter de stocker ses mots de passe dans un fichier en local.
  - ✓ Utiliser des logiciels comme keepass pour les gérer

- Mettre à jour son navigateur et les logiciels présents sur votre ordinateur.
- Lors d'un achat, vérifier que le site est sécurisé (http**s**)
- Se méfier des sites douteux, des pop-up ou des redirections étranges.
- Ne pas sauvegarder ses données bancaires
- Eviter de payer sur les réseaux Wi-Fi publics.
- Ne jamais donner ses coordonnées bancaires
- Ne pas ouvrir les pièces jointes douteuses.