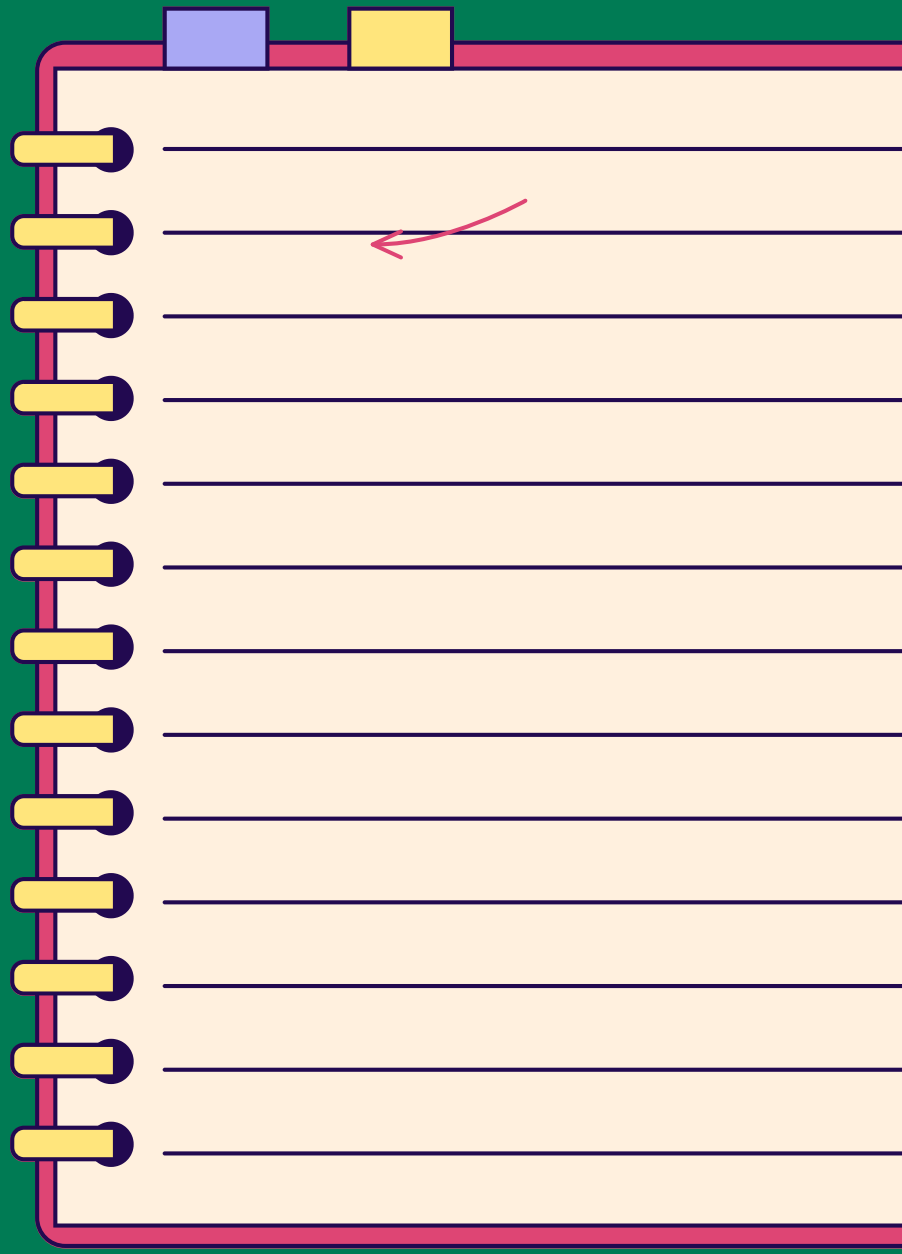
MODULE 12 - ARNAQUES EN LIGNE

# CHAPITRE 2

## COMMENT SE PROTÉGER FACE AUX ARNAQUES

Skills to Connect



# INTRODUCTION

Dans ce chapitre, nous allons explorer les meilleures pratiques pour vous protéger contre les arnaques en ligne. Vous découvrirez des outils de sécurité essentiels comme les antivirus et les pare-feu, ainsi que des habitudes simples à adopter pour sécuriser vos appareils. Vous apprendrez aussi à utiliser des méthodes de protection supplémentaires, telles que l'authentification à deux facteurs, pour garantir la sécurité de vos comptes en ligne. À la fin de ce chapitre, vous saurez comment renforcer vos défenses face aux cybercriminels.

# 1 QUELQUES TERMES À CLARIFIER

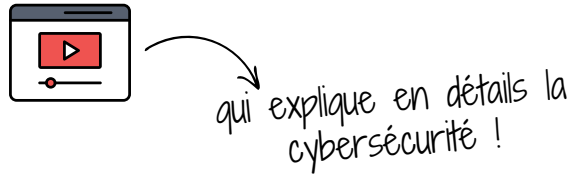
## C’EST QUOI LA CYBERSÉCURITÉ ?

La cybersécurité désigne l'ensemble des stratégies et des technologies mises en place pour protéger les systèmes informatiques, les réseaux et les données contre toute forme de menace, qu'elle soit malveillante ou accidentelle.

- Son objectif principal est de prévenir l'accès non autorisé, le vol, la corruption ou l'endommagement des informations et des infrastructures informatiques. Cela comprend la protection des données personnelles, la sécurisation des transactions en ligne, ainsi que la gestion des risques liés aux logiciels malveillants, aux attaques par hameçonnage (phishing) et aux violations de sécurité.

- En pratique, la cybersécurité repose sur des mesures techniques comme les pare-feu, les antivirus, et l'authentification à plusieurs facteurs, mais elle inclut également des aspects organisationnels, tels que la formation des utilisateurs et la mise en place de politiques de sécurité robustes pour garantir une gestion appropriée des risques.

Regardez la vidéo



# 1 QUELQUES TERMES À CLARIFIER

## C’EST QUOI LA DIFFÉRENCE ENTRE UN PIRATE ET UN HACKEUR ?

La différence entre "pirate informatique" et "hacker" dépend généralement du contexte et de l'interprétation, car les définitions peuvent varier.

- **Hacker**: À l'origine, un hacker était quelqu'un qui avait une connaissance approfondie des systèmes informatiques et des logiciels. Ils étaient des passionnés de technologie qui aimaient explorer et comprendre les systèmes complexes. Les hackers développent souvent des compétences de programmation avancées et sont capables de trouver des solutions créatives aux problèmes techniques. Au sein de cette communauté, "hacker" a généralement une connotation positive et est associé à la curiosité et à la compétence technique.

- **Pirate** : Ce terme est souvent utilisé pour décrire quelqu'un qui utilise des compétences techniques pour accéder à des systèmes informatiques sans permission et avec des intentions malveillantes. Les pirates informatiques peuvent être impliqués dans des activités telles que le vol d'informations, la compromission de systèmes, la diffusion de logiciels malveillants, entre autres. Contrairement aux hackers, les pirates informatiques sont généralement perçus de manière négative et sont associés à des activités illégales et nuisibles.

Cependant, il est important de noter que ces définitions peuvent se chevaucher ou être interprétées de différentes manières, surtout dans le contexte en constante évolution de la cybersécurité et de la culture technologique. De plus, le terme "hacker" peut être utilisé de manière plus large pour décrire une variété de personnes talentueuses en technologie, tandis que "pirate informatique" est plus spécifique aux activités criminelles.

# 2 SE PROTÉGER CONTRE LES ARNAQUES

## COMMENT FAIRE ?

### ETAPE 1 : PROTÉGER SES APPAREILS

Tout d'abord, il est essentiel de protéger nos ordinateurs et appareils mobiles contre les attaques cybernétiques. Cela inclut l'installation de programmes antivirus et de pare-feu fiables, ainsi que le maintien de tous les logiciels à jour. De nombreuses attaques cybernétiques exploitent les vulnérabilités des logiciels non mis à jour, il est donc essentiel de maintenir le système à jour pour prévenir les intrusions.

- **Pare-feu :** Un pare-feu est un système de sécurité qui agit comme une barrière pour protéger un réseau informatique. Il surveille les connexions internet et décide quelles données peuvent entrer ou sortir, afin de bloquer les menaces ou les attaques. En gros, il empêche les mauvaises connexions de passer et protège votre ordinateur ou réseau contre les dangers.

- **Antivirus :** Un antivirus est un programme conçu pour détecter et supprimer les virus et autres logiciels malveillants sur votre ordinateur. Il protège votre appareil en analysant les fichiers et en empêchant les menaces d'infecter votre système. Il joue aussi un rôle de prévention en arrêtant les virus avant qu'ils ne causent des dégâts.

ALERTE MODULE

Découvrez en plus sur la protection de vos appareils dans le module 1 !

# 2 SE PROTÉGER CONTRE LES ARNAQUES

COMMENT FAIRE ?

## ETAPE 2 : PROTÉGER SES COMPTES

Protéger nos comptes en ligne est très important. Beaucoup de personnes utilisent des mots de passe simples ou les mêmes mots de passe pour plusieurs comptes, ce qui rend plus facile pour les pirates informatiques de les voler.

- Il est essentiel d'avoir **des mots de passe forts et différents pour chaque compte.**

ALERTE MODULE

Découvrez comment choisir un mot de passe dans le module 5 sur la gestion des données !

- Il est également conseillé d'utiliser **l'authentification à deux facteurs** quand c'est possible :
  - L'authentification à deux facteurs est une méthode de sécurité supplémentaire pour protéger vos comptes en ligne. Au lieu de vous contenter de votre mot de passe pour vous connecter, cette méthode vous demande deux informations pour vérifier votre identité.
  - La première étape consiste à entrer votre mot de passe, comme d'habitude. La deuxième étape, c'est là que l'authentification à deux facteurs entre en jeu : un code supplémentaire vous est envoyé. Ce code peut être envoyé par SMS sur votre téléphone, par email, ou il peut être généré par une application comme Google Authenticator.
  - Ce code est généralement valable pendant un court moment et il est unique à chaque connexion. Même si quelqu'un parvient à voler votre mot de passe, il lui sera impossible de se connecter sans le deuxième code. Ce double contrôle garantit que vous seul pouvez accéder à votre compte, même si quelqu'un d'autre connaît votre mot de passe.

De plus en plus d'application et de sites internet imposent l'authentification à deux facteurs, comme Facebook, Google + Microsoft

# 2 SE PROTÉGER CONTRE LES ARNAQUES

COMMENT FAIRE ?

## ETAPE 3 : PROTÉGER SES DONNÉES

Il est crucial d'être conscient de la manière dont nous partageons nos données personnelles en ligne et de prendre des mesures pour les protéger. Cela signifie limiter les informations que nous diffusons sur les réseaux sociaux et autres sites, ainsi qu'être particulièrement vigilant lorsque nous remplissons des formulaires en ligne. Les pirates informatiques ciblent souvent des données sensibles telles que les numéros de carte de crédit, les numéros de sécurité sociale et les dates de naissance, qui peuvent être utilisées pour des vols d'identité ou d'autres formes de fraude.

La protection de nos données personnelles est donc une étape essentielle dans la prévention des arnaques en ligne. En réduisant les informations que nous partageons et en étant attentifs à la sécurité des sites que nous utilisons, nous pouvons minimiser le risque d'être victimes d'escroqueries.


ALERTE MODULE

Découvrez comment protéger vos données en suivant le module 1 sur la protection des appareils !

# A RETENIR !

Les habitudes à prendre pour vous protéger des arnaques en ligne :

- Apprenez à reconnaitre les différents types d'arnaques et les signes à repérer pour ne pas tomber dans le panneau
- Protégez vos appareils en faisant les mises à jours de vos appareils et en installant des pare-feu et anti-virus
- Protégez vos données et vos comptes en utilisant des mots de passes robustes et utilisez l'authentification à deux facteurs.