# CYBERATTAQUE : QU'EST-CE QUE C'EST CONCRÈTEMENT ?

LÉA NOÉ

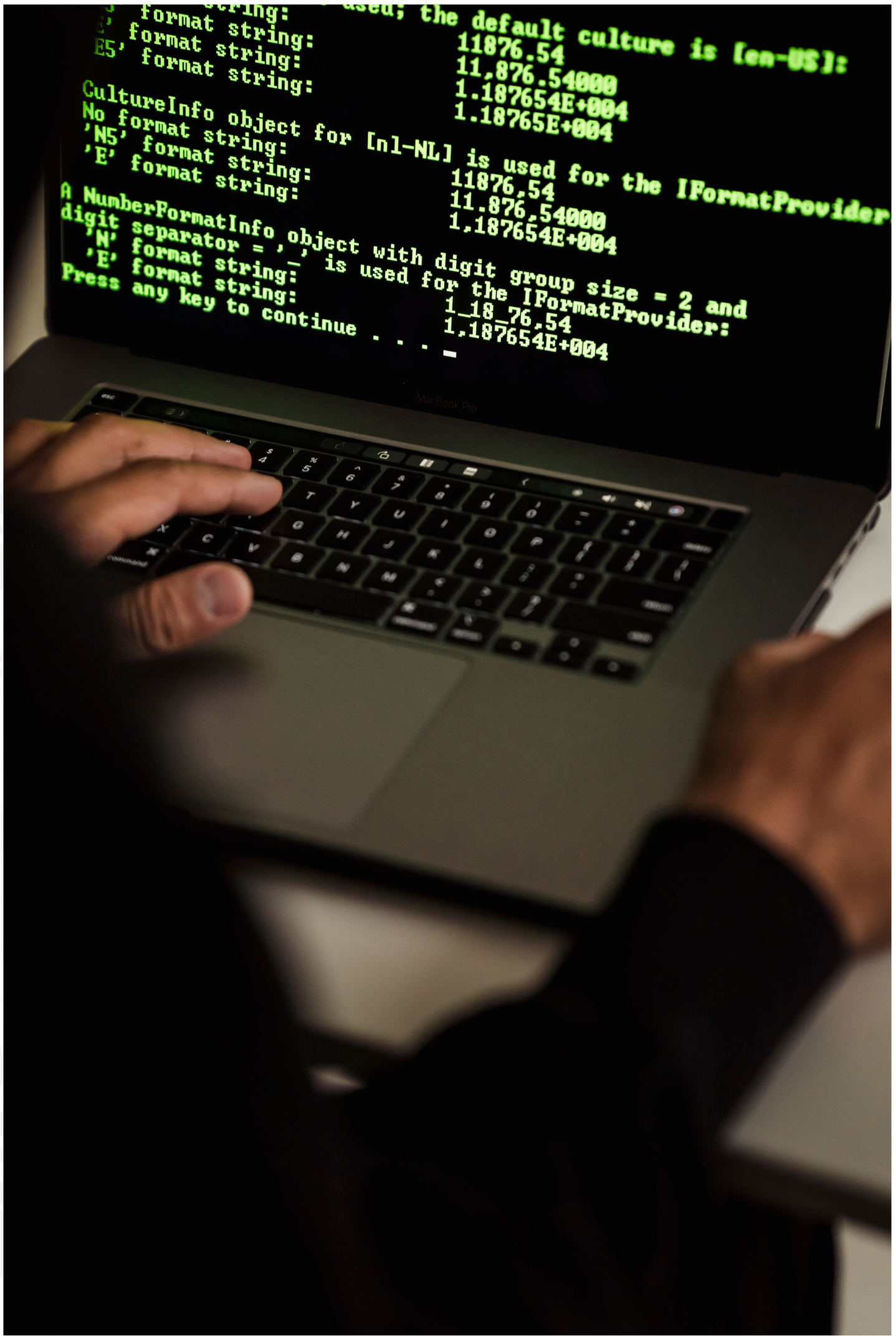
AVRIL 2022


Credits: CANVA

DEF'INSEEC DEFINSEEC@GMAIL.COM 0 6 6 6 7 3 7 1 6 5

# DÉFINIR UNE CYBERATTAQUE

Depuis le début de la crise sanitaire, le terme de « cyberattaque » s'est démocratisé et fait maintenant partie du vocabulaire commun. Cependant, êtes-vous réellement en mesure de définir une cyberattaque et d'expliquer les différents types et les différentes étapes de ce phénomène ? Nous allons décrypter les bases de ce phénomène.




## Définition

Avant toute chose, il est important de définir précisément ce qu'est une cyberattaque.

Les cyberattaques ou attaques informatiques sont le fait de pirates informatiques et se caractérisent par une action malveillante menée grâce à un réseau informatique. Les données informatiques sont considérées comme la cible principale des pirates. Le vol de ces données permet plusieurs modes d'action aux hackers :

- Les revendre sur les darknets (« réseaux permettant de partager de manière anonyme des données cryptées inaccessibles aux moteurs de recherche traditionnels » - Larousse) ;
- Espionner et/ou saboter (avantage concurrentiel ou destruction)
- Être un moyen (préparer une cyberattaque, porter atteinte à la réputation)

Depuis 2020, les cyberattaques sont en augmentation et cela est particulièrement dû au fait qu'elles ont pu remplacer ou en tout cas, compenser les autres types de vols. Les autres types de vols se sont vu particulièrement réduits par les confinements.

Credits : CANVA

# LES DIFFÉRENTES FORMES ET LES DIFFÉRENTES PHASES D'UNE CYBERATTAQUE

Cybersécurité

## Quelles sont les formes les plus communes de cyberattaque ?

L'objectif étant de connaître les bases en matière de cyberattaque, nous détaillerons seulement les principales menaces répertoriées pour l'année 2021, soit six menaces différentes :

- Un **rançongiciel** (ou ransomware) se caractérise par le blocage à distance (cryptage) de fichiers ou plus généralement d'un appareil et qui découle sur une demande de rançon pour débloquer (décrypter) les fichiers.

- Le **hameçonnage** (ou phishing) se caractérise par l'usurpation d'identité d'une entité connue telle que l'Assurance Maladie ou la CAF. Cette usurpation d'identité se fait généralement par mail, par sms, voire par appel téléphonique et elle vise à obtenir les informations personnelles ou professionnelles (données bancaires, identifiants et mots de passe...). Cette technique d'attaque se décline en deux types, les attaques opportunistes (campagne de mails envoyés à une multitude d'adresse mail) et les attaques ciblées visant à installer un programme malveillant.

- Le **zoombombing** est l'infiltration de visioconférence privée par un internaute afin d'en perturber le bon déroulement.

- Le **cheval de Troie** se retrouve principalement dans les mails spam et une fois que votre appareil est infecté, en fonction du type de cheval de Troie, il peut envoyer des mails à vos contacts, voler vos informations bancaires ainsi que toutes les données qui se trouvent sur l'appareil touché.

- L'**enregistreur de frappe** (ou keylogger) est un dispositif permettant d'enregistrer les frappes sur votre clavier. Cela permet aux pirates de récupérer les identifiants et mots de passe et notamment les données bancaires.

- La **fuite de données** peut apparaître de deux manières différentes, soit via une faille technologique, soit par une intervention humaine (volontaire ou par inadvertance).

## Les différentes phases d'une cyberattaque

Du point de vue du hacker, un cyberattaque se déroule en cinq phases :

1. **Reconnaissance** : cette phase a lieu plusieurs mois, voire années avant la détection de la cyberattaque ; elle permet au pirate de connaître sa cible et d'identifier l'angle d'attaque le plus adapté.
2. **Intrusion initiale** : cette phase permet au pirate de s'introduire et de s'implanter au sein de l'environnement informatique de l'entreprise. Il n'est généralement pas détecté à ce stade.
3. **Propagation** : l'objectif du pirate est d'avoir accès à davantage d'informations, de comptes utilisateurs etc, tout en restant indétecté.
4. **Persistance** : au bout de plusieurs mois de travail, le pirate a accès aux données recherchées.
5. **Action** : en fonction du mode opératoire, le pirate peut dès à présent se manifester pour obtenir une rançon, utiliser les informations comme avantage concurrentiel ou même revendre ces informations.

# QUE FAUT-IL FAIRE ?

## Que faire en cas de cyberattaque ?

En fonction de la cible et du type de cyberattaque, les réactions préconisées ne sont pas les mêmes. De façon générale, il est recommandé de :

- Ne pas éteindre l'appareil infecté
- Éteindre les appareils non contaminés
- Ne pas appeler les numéros affichés
- Ne pas cliquer sur les liens ou sur les fenêtres apparaissant sur votre écran

Pour les professionnels, il est fondamental de contacter le service informatique ou l'agence en charge de la sécurité des données ; ils seront alors en mesure de lancer un traceur et de localiser toutes les failles, ils seront aussi en mesure de connaître l'adresse IP du hacker et de comprendre son mode opératoire. Une fois cela fait, il sera impératif de mettre à jour votre antivirus et de changer tous les mots de passe.

En cas de cyberattaque, il est possible et conseillé de déposer plainte. Il est primordial d'en tirer les enseignements et de s'organiser à tous les niveaux pour que cela ne se reproduise plus.

Pour se préparer, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a publié son Guide d'hygiène informatique - Renforcer la sécurité de son système d'information en 42 mesures.

## Que faire pour prévenir une cyberattaque ?

En ce qui concerne les entreprises, il faut déterminer quelles sont les données sensibles et adapter le système de sécurité informatique en conséquence, et s'il n'existe pas déjà le mettre en place.

## La sauvegarde comme méthode de prévention

Au niveau professionnel, il est possible de se protéger de tout cryptage et ransomware grâce à une sauvegarde régulière dans un ou plusieurs datacenters.

Crédit photo : CANVA

Du côté des particuliers, une sauvegarde sur disques durs externes pourrait prévenir toute tentative de ransomware.

# SOURCES


- Anonyme (2021). Cyberattaque : qu'est-ce que c'est ? Consulté le 19/04/2022. [En ligne].
- Anonyme (2021). Cyberattaque. Consulté le 19/04/2022. [En ligne].
- Anonyme (2021). Cyberattaque - Définition et Explications. Consulté le 19/04/2022. [En ligne].
- Anonyme (2021). RANÇONGICIEL. Consulté le 19/04/2022. [En ligne].
- Anonyme (2021). ATTAQUE PAR HAMEÇONNAGE (PHISHING). Consulté le 19/04/2022. [En ligne].
- Anonyme (2021). SÉCURITÉ INFORMATIQUE : QUE FAIRE EN CAS DE CYBER-ATTAQUE ? Consulté le 19/04/2022. [En ligne].

H.E.I.P

AEROSPACE
CYBERSECURITY

DEF'INSEEC

# SUIVEZ DEF'INSEEC SUR

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65