ASSURER SA SÉCURITÉ EN LIGNE

Introduction à la cybersécurité et aux bonnes pratiques numériques

info@hub01.org
hub01.org

HUB NUMÉRIQUE

SOMMAIRE

info@hub01.org
hub01.org

HUB NUMÉRIQUE

À PROPOS

0/1, c’est le numérique
par la culture,
pour la culture.

Nous préférons
les gens aux machines
et le café - ou le thé - à
l’eau.

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

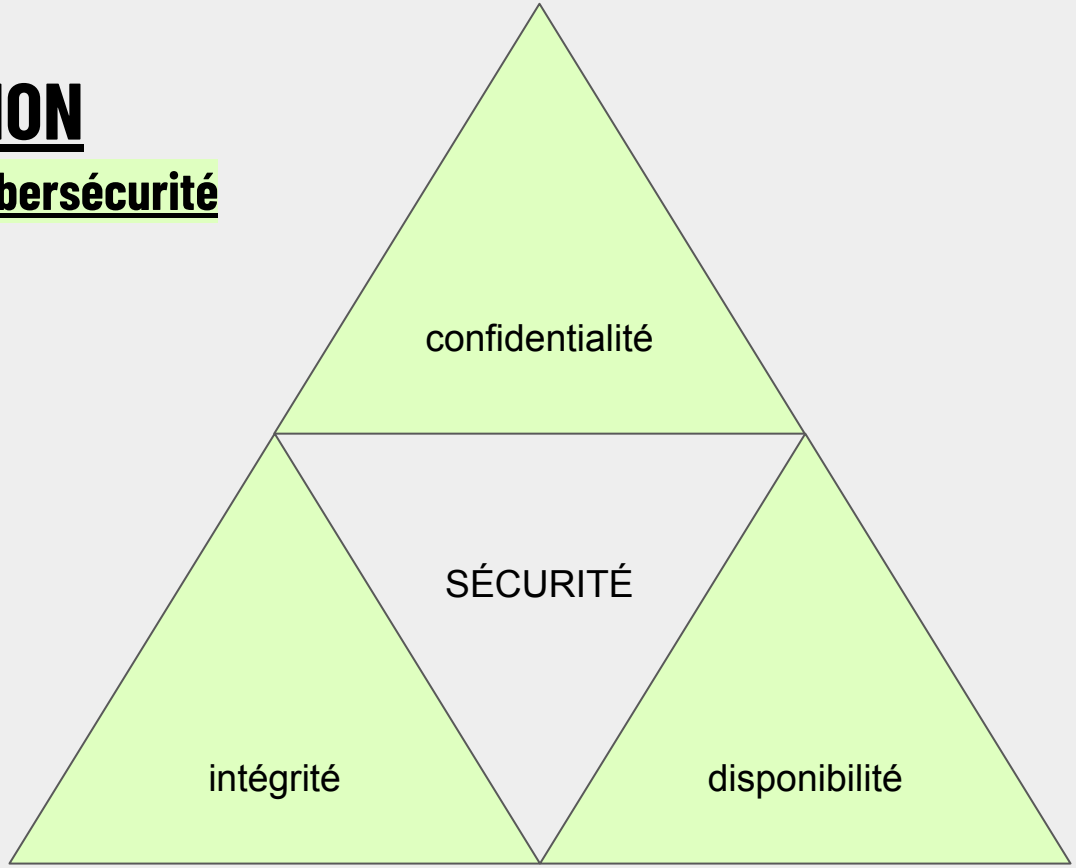
INTRODUCTION

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

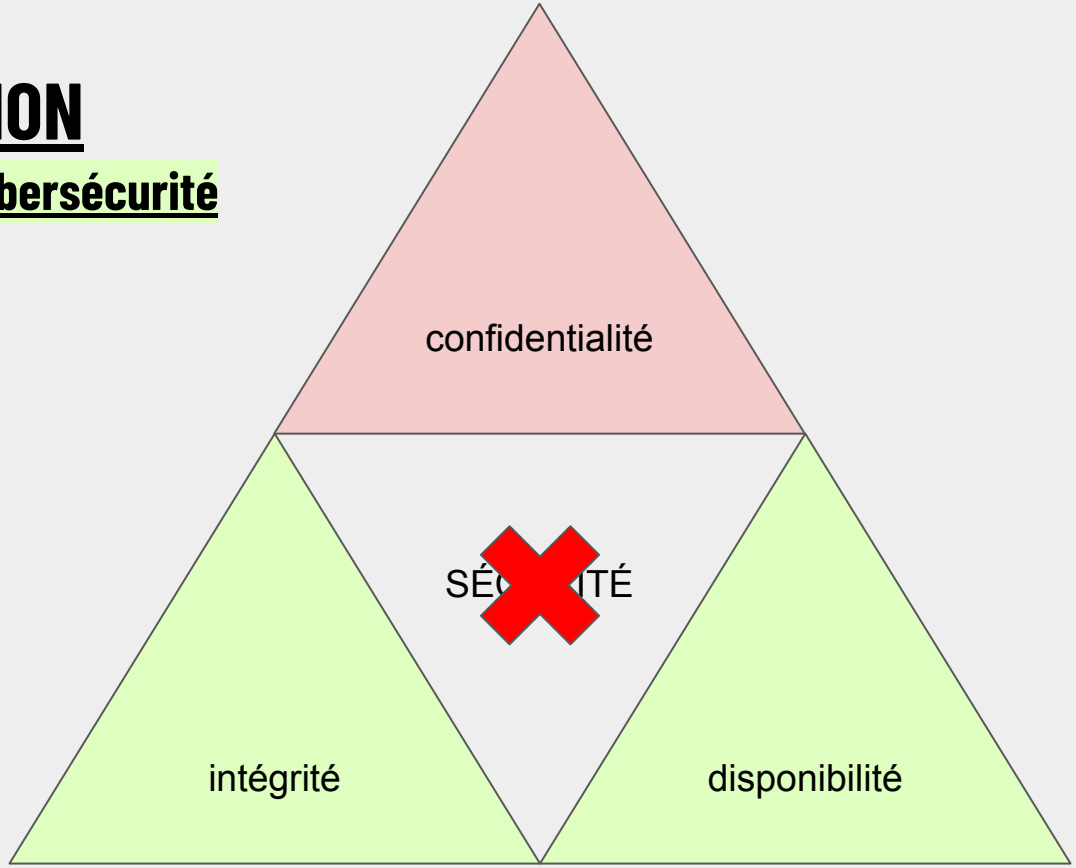
INTRODUCTION

La triade de la cybersécurité



INTRODUCTION

La triade de la cybersécurité



LES TYPES DE CYBERATTAQUES

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

LES MENACES PHYSIQUES

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

LES TYPES DE CYBERATTAQUES

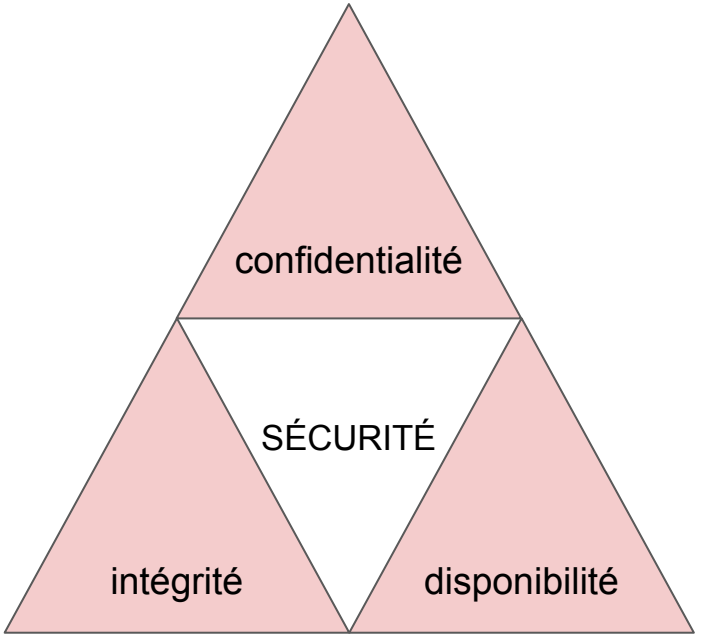
Les menaces physiques

1 de 3 | ***Vol et/ou destruction***

Les attaquants peuvent voler ou détruire du matériel informatique, tels que des disques durs, des ordinateurs portables, des clés USB, des serveurs, des routeurs, etc.

CONSÉQUENCES

- **L'intégrité des données est compromise**
- **La confidentialité des données est compromise**
- **La disponibilité des données est compromise**



LES TYPES DE CYBERATTAQUES

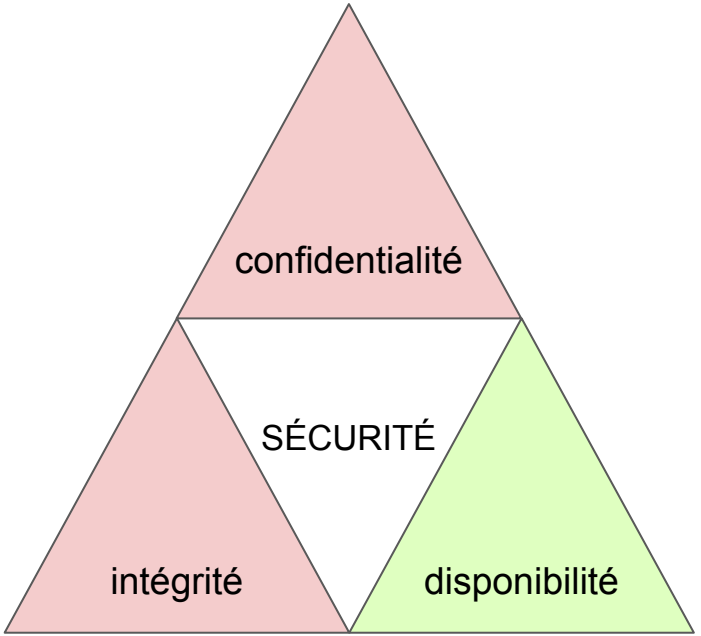
Les menaces physiques

2 de 3 | ***Attaques "man-in-the-middle"***

Les attaquants peuvent intercepter les transmissions de données entre les équipements de réseau en les reliant à un équipement malveillant intermédiaire, leur permettant ainsi d'espionner ou de modifier les données en transit.

CONSÉQUENCES

- **L'intégrité des données est compromise**
- **La confidentialité des données est compromise**



LES TYPES DE CYBERATTAQUES

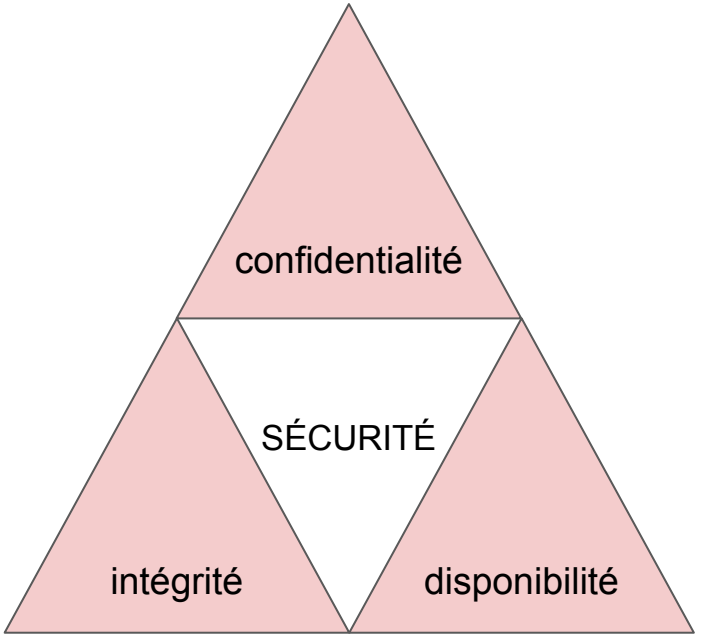
Les menaces physiques

3 de 3 | ***Accès physique non autorisé***

Les attaquants peuvent accéder physiquement aux équipements de réseau sans autorisation pour installer des logiciels malveillants ou pour voler des données.

CONSÉQUENCES

- **L'intégrité des données est compromise**
- **La confidentialité des données est compromise**
- **L'accessibilité des données est compromise**



LES MENACES À DISTANCE

info@hub01.org
hub01.org

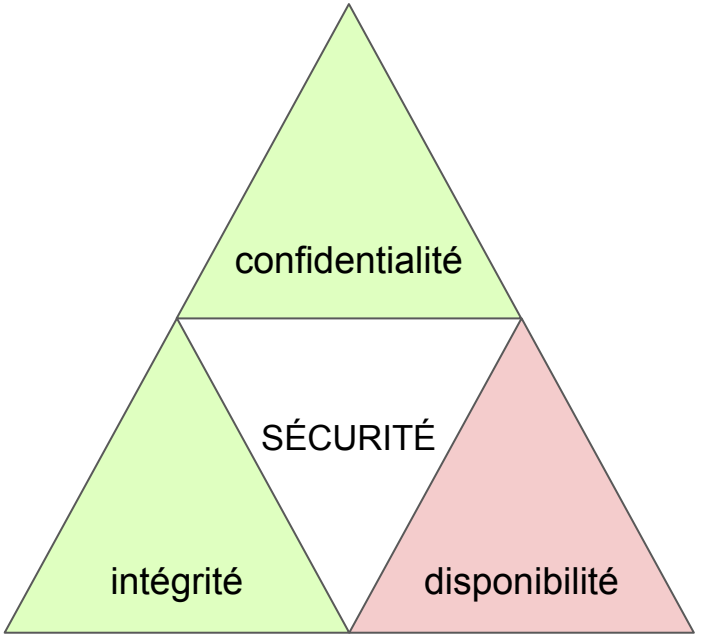
HUB
NUMÉRIQUE

LES TYPES DE CYBERATTAQUES

Les menaces à distance

1 de 5 | ***Attaque par déni de service***

Attaque qui vise à rendre un service en ligne indisponible en surchargeant les serveurs.



CONSÉQUENCES

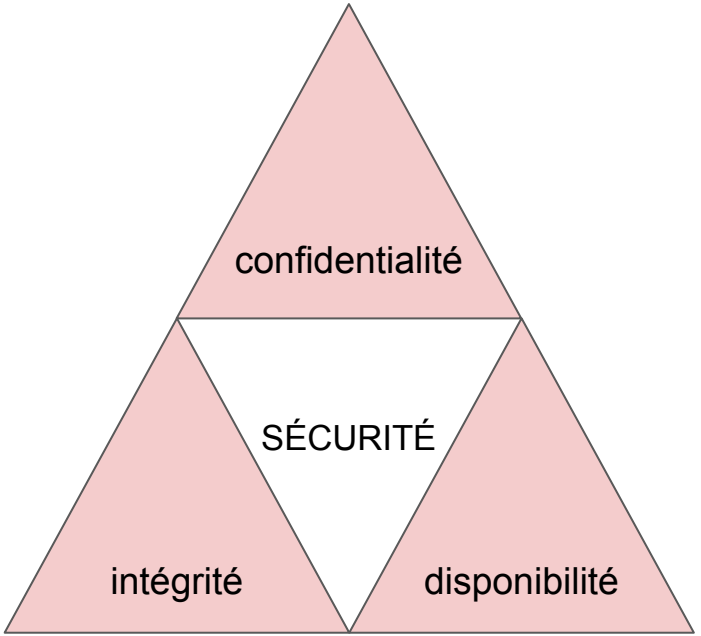
- **Pertes de revenus**
- **Détérioration de la réputation**
- **La disponibilité des données est compromise**

LES TYPES DE CYBERATTAQUES

Les menaces à distance

2 de 5 | ***Attaque au mots de passe***

Attaque automatisée - ou humaine - consistant à essayer de deviner un mot de passe jusqu'à ce qu'il soit trouvé.



CONSÉQUENCES

- **Vol d'informations**
- **Perte d'accès aux comptes**
- **Transactions frauduleuses**

LES TYPES DE CYBERATTAQUES

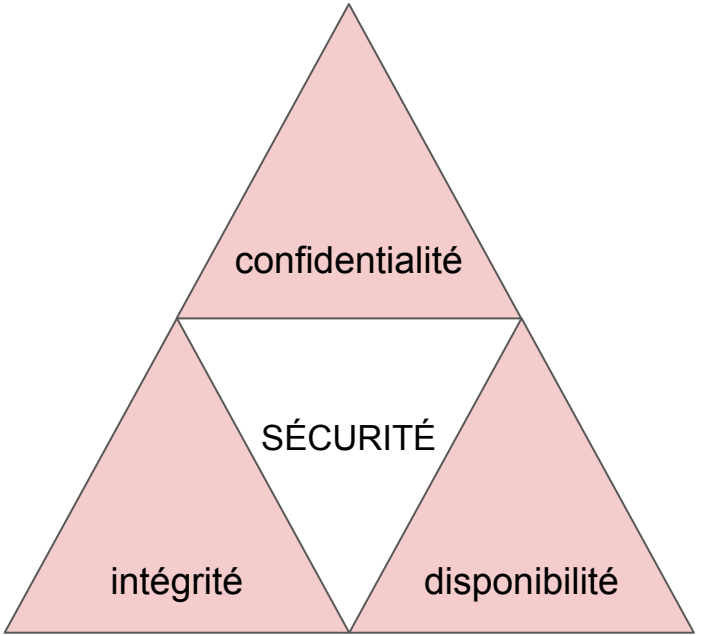
Les menaces à distance

3 de 5 | ***Exploitation des vulnérabilités***

Les attaquants exploitent les vulnérabilités connues dans les logiciels ou les systèmes d'exploitation pour accéder à distance aux systèmes, les compromettre et voler des données.

CONSÉQUENCES

- **L'intégrité des données est compromise**
- **La disponibilité des données est compromise**
- **La confidentialité des données est compromise**



PETITE PARENTHÈSE (LES MALICIELS)

info@hub01.org
hub01.org

HUB NUMÉRIQUE

LES TYPES DE CYBERATTAQUES

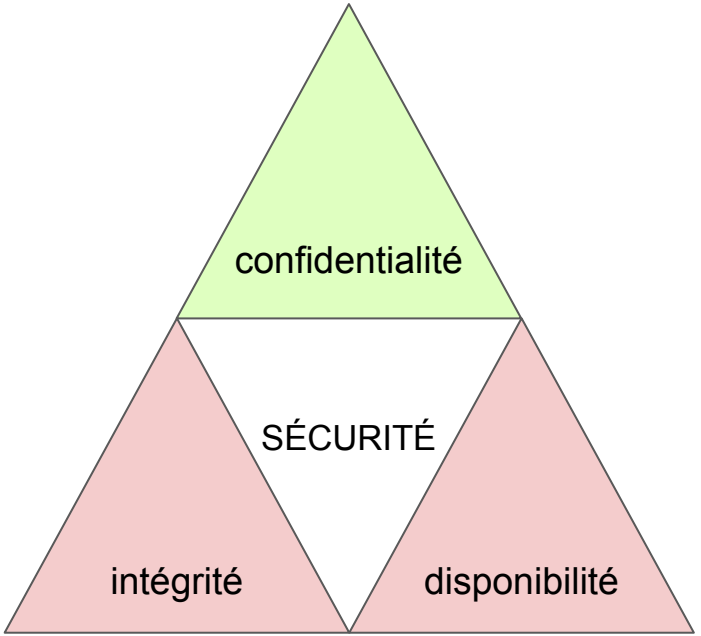
Petite parenthèse (les maliciels)

1 de 3 | ***Les virus***

Un virus informatique est un type spécifique de maliciel qui s'auto-réplique en infectant des fichiers et des programmes sur un ordinateur.

CONSÉQUENCES

- **Perturbation des performances du système**
- **Intégrité des données compromise**
- **Disponibilité des données compromise**



LES TYPES DE CYBERATTAQUES

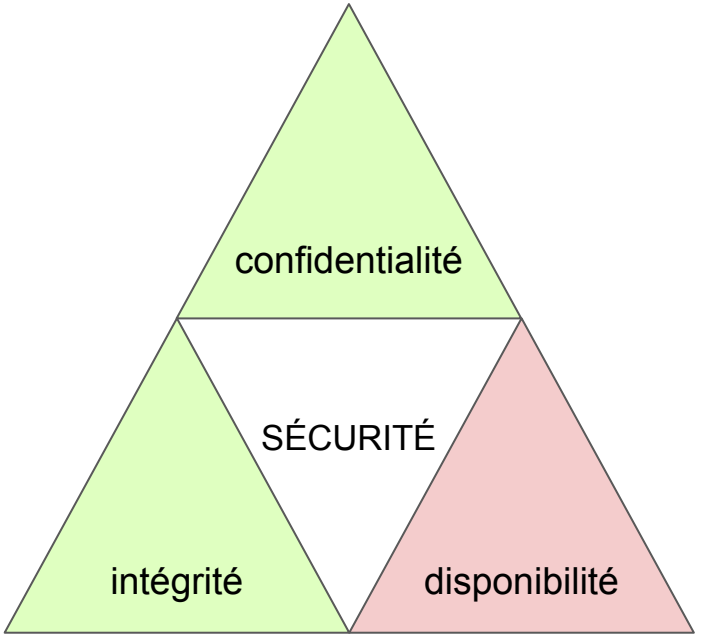
Petite parenthèse (les maliciels)

2 de 3 | ***Les rançongiciels***

Type de logiciel malveillant qui chiffre les fichiers d'un utilisateur - ou d'un réseau - et demande ensuite une rançon pour restaurer l'accès à ces fichiers.

CONSÉQUENCES

- **Disponibilité des données compromise**
- **Perte financière**



LES TYPES DE CYBERATTAQUES

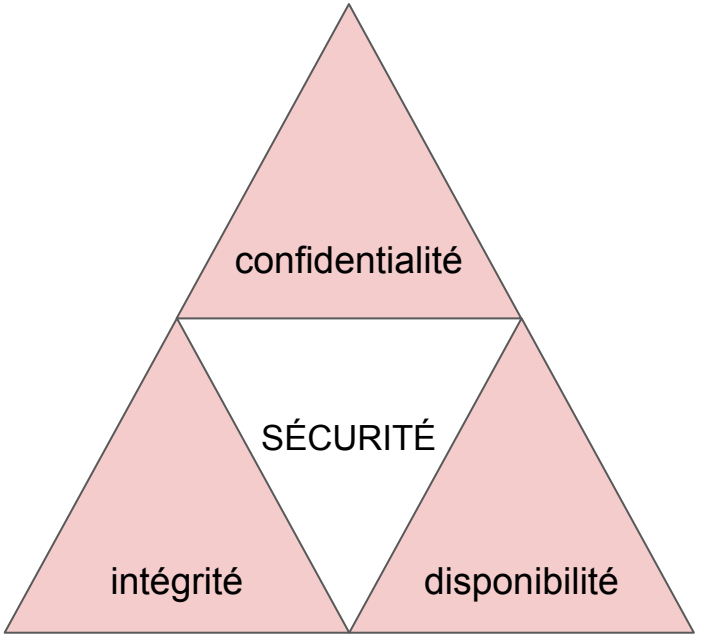
Petite parenthèse (les maliciels)

3 de 3 | ***Les vers***

Type de logiciel malveillant qui se propage automatiquement d'un ordinateur à un autre via des réseaux informatiques, sans intervention humaine.

CONSÉQUENCES

- **Perturbation des performances du système**



FIN DE LA PARENTHÈSE

info@hub01.org
hub01.org

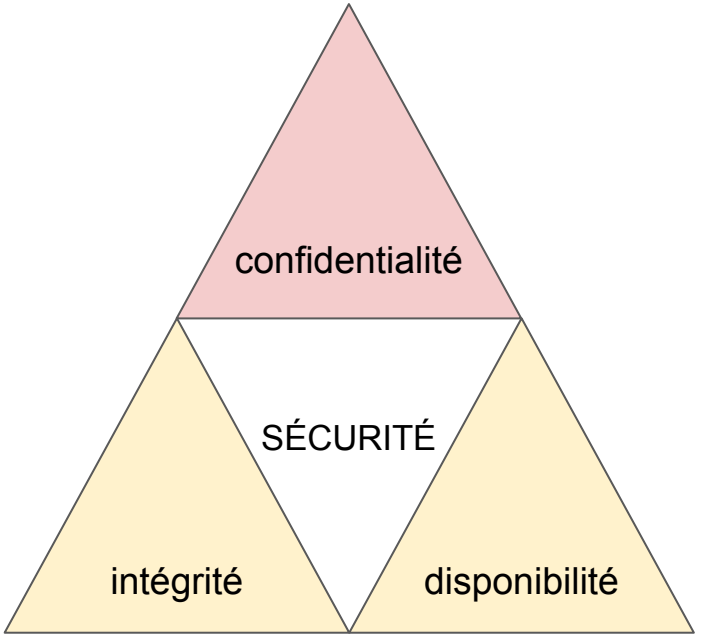
HUB
NUMÉRIQUE

LES TYPES DE CYBERATTAQUES

Les menaces à distance

4 de 5 | ***Publicité malveillante***

Pop-ups, bannières ou liens sponsorisés diffusés sur n'importe quel type de site web, même les sites web de confiance.



CONSÉQUENCES

- **Téléchargement de logiciels malveillant**
- **Vol d'informations personnelles et financières**
- **Perturbation des performances du système**

LES TYPES DE CYBERATTAQUES

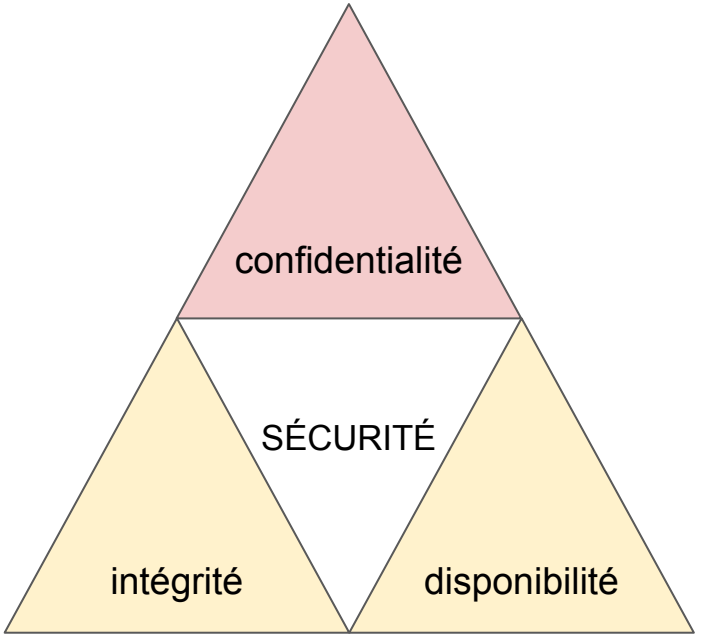
Les menaces à distance

5 de 5 | ***Hameçonnage***

E-mails ou messages frauduleux pour tromper les utilisateurs et les inciter à télécharger un maliciel ou fournir des informations sensibles, telles que des mots de passe, des numéros de carte de crédit, etc.

CONSÉQUENCES

- **Vol d'informations personnelles**
- **Vol d'identifiants et de mots de passe**
- **Perte financière**



LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

info@hub01.org
hub01.org

01 HUB NUMÉRIQUE

LA BASE

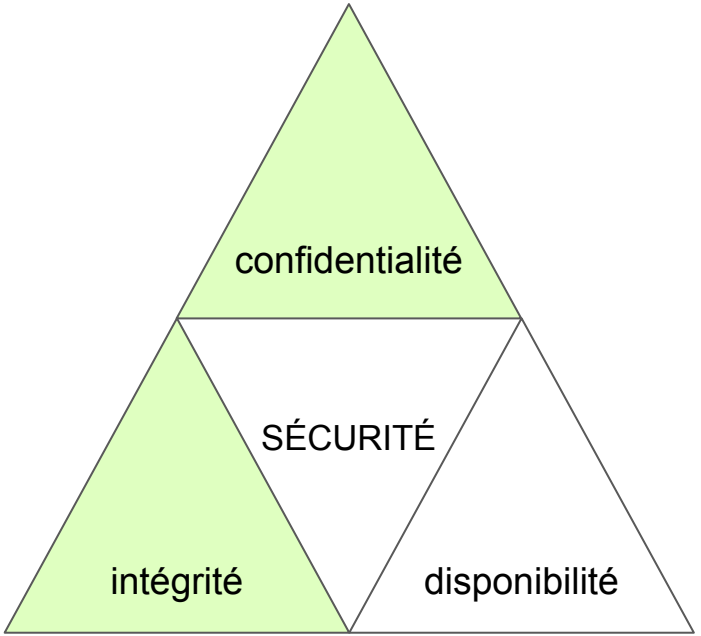
LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

La base

1 de 2 | ***Pare-feu (Firewall)***

Dispositif de sécurité qui contrôle le trafic réseau entrant et sortant d'un système informatique ou d'un réseau.

- Filtre chaque paquet de données et vérifie s'il correspond aux règles de sécurité définies
- Protège le réseau ou le système informatique



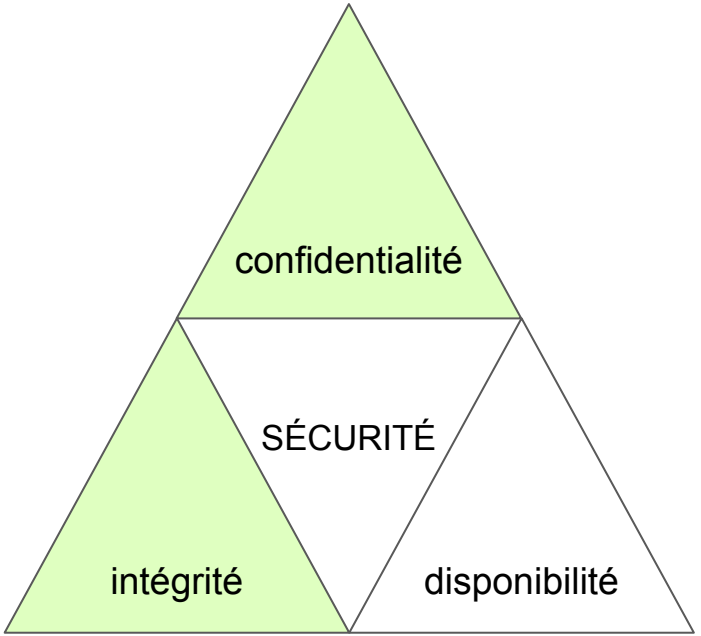
LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

La base

1 de 2 | ***Antivirus***

Un antivirus est un logiciel de sécurité informatique qui est conçu pour détecter, prévenir et éliminer les logiciels malveillants.

- Analyse les fichiers et les programmes en cours d'exécution sur le système à la recherche de signatures de logiciels malveillants connus pour ensuite les éliminer



QUELQUES SUPPLÉMENTS

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

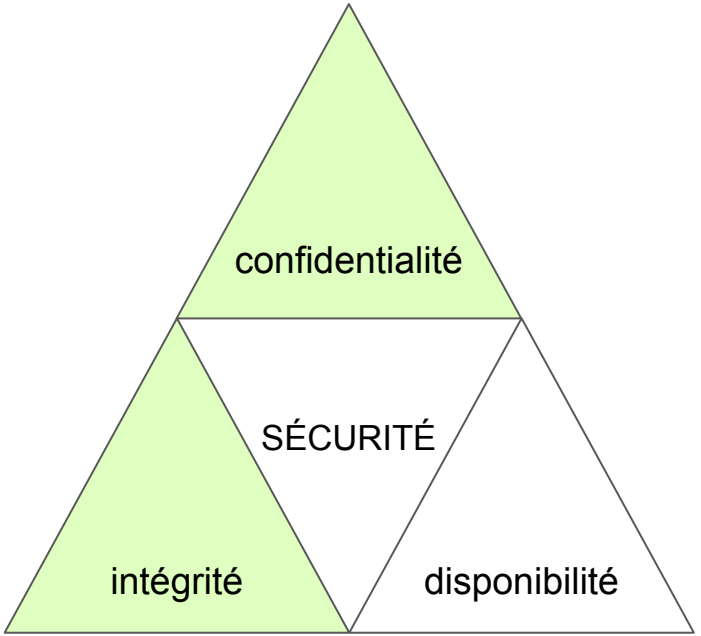
LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

Quelques suppléments

1 de 3 | ***VPN***

Sécurise une connexion en créant un tunnel de communication chiffré entre l'utilisateur et le serveur VPN.

- Créer un tunnel de communication chiffré pour toutes les communications de l'utilisateur
- Masque l'adresse IP de l'utilisateur en remplaçant son adresse IP réelle par l'adresse IP du serveur VPN



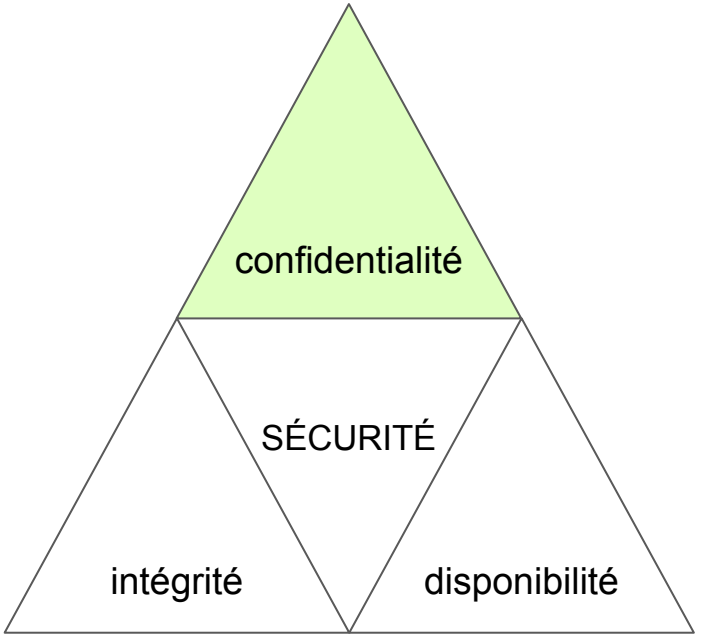
LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

Quelques suppléments

2 de 3 | ***Gestionnaire de mots de passe***

Outil qui permet de stocker en toute sécurité les noms d'utilisateur et les mots de passe pour les comptes en ligne.

- Stockage sécurisé des mots de passe
- Génération de mots de passe forts
- Protection contre certaines attaques de phishing
- Facilite la gestion des comptes en ligne
- Permet de partager des mots de passe de manière sécuritaire



LE SYSTÈME IMMUNITAIRE NUMÉRIQUE

Quelques suppléments

2 de 3 | ***Sauvegarde et restauration des données***

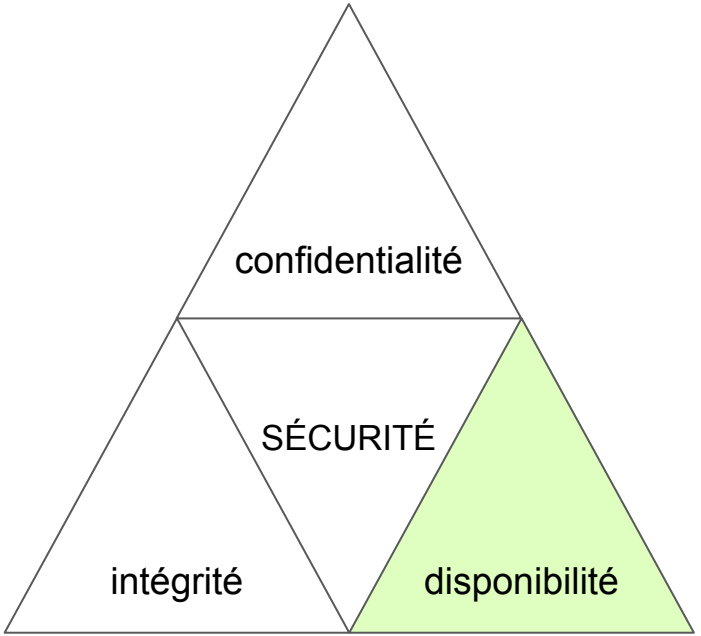
Mesures essentielles pour garantir que les données sont toujours disponibles, même en cas de perte ou de dommages.

Sauvegarde sur site

- disques durs, des
- serveurs de sauvegarde

Sauvegarde en ligne

- serveurs distants



BONNES PRATIQUES

info@hub01.org
hub01.org

HUB
NUMÉRIQUE

BONNES PRATIQUES

Toujours faire les mises à jour

1 de 2 | ***Système d'exploitation***

La plupart des mises à jour système corrigent des failles de sécurité connues ou potentielles pour protéger l'utilisateur contre les cyberattaques et les vulnérabilités.

BONNES PRATIQUES

Toujours faire les mises à jour

2 de 2 | ***Logicielles (incluant le navigateur)***

Tout comme les mises à jour du système d'exploitation, les mises à jour logicielles corrigent souvent des failles de sécurité pour protéger les utilisateurs contre les vulnérabilités connues ou potentielles dans le logiciel.

Les applications web sont mises à jour automatiquement.

BONNES PRATIQUES

Être sensible aux tentatives d'hameçonnage

1 de 3 | ***ALARME! ALARME! ALARME!***

Trois drapeaux rouges :

- L'urgence ou la nécessité d'une action immédiate de la part du destinataire,
- L'intrigue ou la curiosité pour inciter l'ouverture du courriel,
- La personnification ou l'utilisation d'une source de confiance pour faire croire que le courriel est légitime.

BONNES PRATIQUES

Être sensible aux tentatives d'hameçonnage

2 de 3 | ***Être attentif aux détails***

Plus souvent qu'autrement, le nom de domaine de l'envoyeur ne correspond pas exactement au nom de domaine personnifié.

- microsft
- facedook
- dejardins

BONNES PRATIQUES

Être sensible aux tentatives d'hameçonnage

3 de 3 | ***Êtes-vous nommé?***

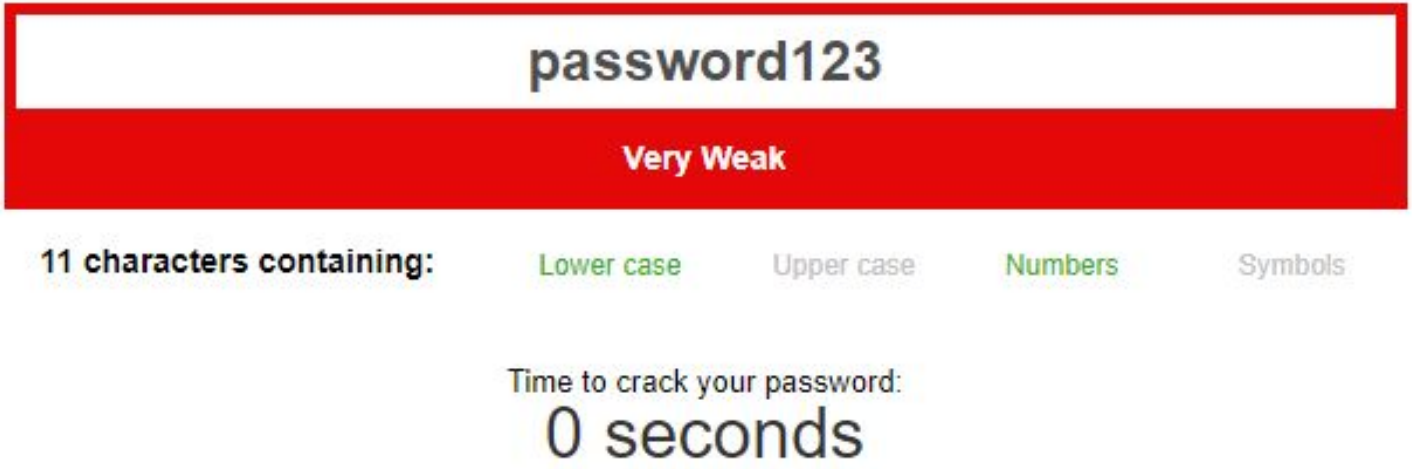
Les courriels d'hameçonnage sont généralement envoyés en masse. Pour cette raison, les messages sont dépersonnalisés.

Si un service de confiance veut vous contacter, il saura assurément s'adresser à vous en utilisant votre nom, prénom ou toute autres informations personnelles à votre compte.

BONNES PRATIQUES

Toujours utiliser des mots de passe forts

1 de 3 | ***password123***

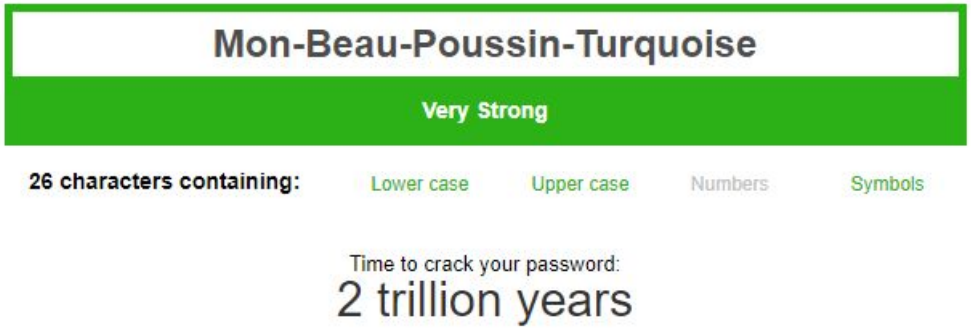


BONNES PRATIQUES

Toujours utiliser des mots de passe forts

2 de 3 | ***Phrase de passe***

Les phrases de passe sont beaucoup plus facile à mémoriser pour un humain et sont autant difficile à décrypter que les mots de passe illisible



BONNES PRATIQUES

Toujours utiliser des mots de passe forts

3 de 3 | ***Gestionnaire de mots de passe***

Mots de passe générés par un humain :

g00gl3GTd2 = 7 mois

3495U8289T34Ce = 59 000 ans

Mots de passe Générés par un gestionnaire de mots de passe :

meWJn3QkQeCCFg = 193 milliards d'années

G4kGZGhXESB2Wq = 200 trillions d'années

MERCI!

Vous souhaitez en savoir plus?
Si vous avez des questions,
qui que vous soyez, n'hésitez pas!

info@hub01.org
hub01.org

Suivez-nous sur Facebook!
Restez à l'affût!