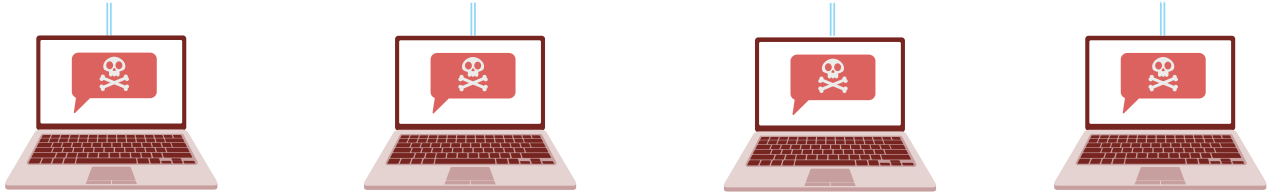
Qu'est-ce qu'une cyberattaque ?
Les menaces tapies dans l'ombre

Les cyberattaques sont nombreuses et peuvent être massives ou plus ciblées. Elles frappent de façon directe (par force brute, en utilisant des dictionnaires et / ou des permutations de lettres pour obtenir votre mot de passe) ou indirecte (en vous incitant à cliquer sur un lien ou un fichier contaminé).



Cybercriminalité

Phishing ou utilisation de ransomwares (chiffrant vos données pour vous soustraire de l'argent).

Atteinte à l'image

Défiguration d'un site hacké ou typosquatting (ex : Goigle).

Espionnage

Usage de spywares ou de keyloggers pour enregistrer vos frappes clavier.

Sabotage

Recours à un Trojan ou à un réseau de botnets pour infecter et causer un déni de service.

Conséquences

Pertes financières

Vol, divulgation et revente d'informations

Usurpation d'identité

Perte de confiance et de crédibilité

Perte de disponibilité ou dysfonctionnement d'un service

Que faire pour se protéger?
Les bons réflexes

1. Privilégiez une authentification forte

- Quand c'est possible : préférez une authentification multifacteur (mot de passe + code envoyé par sms, par exemple).
- Utilisez des mots de passes différents pour chaque site. Ne laissez pas le navigateur les mémoriser pour vous, il existe des coffres-forts comme Keepass pour les garder en sécurité.
- Créez des mots de passe complexes composés de 10 caractères minimum, comprenant majuscules, minuscules, chiffres et caractères spéciaux.

2. Restez vigilant

- Ne cliquez pas sur des liens ou pièces jointes en cas de doute sur l'expéditeur.
- Utilisez les sites chiffrant vos données de bout en bout, notamment en cas de paiement (https).

3. Anticipez les accidents

- Faites des sauvegardes régulières sur différents supports.
- Protégez vos enfants en utilisant un moteur de recherche adapté à leur âge (comme Qwant Junior).

Plus d'informations
& liens utiles

Il est important de protéger la disponibilité, l'intégrité et la confidentialité des données. En effet, vérifier leur traçabilité et leur imputabilité est l'affaire de tous.

- L'ANSSI est l'un des organismes responsables de la cybersécurité, et leur MOOC, disponible sur notre plateforme Moodle, enseigne comment naviguer en toute quiétude : **https://moodle.univ-tln.fr/course/index.php?categoryid=876**
- Le site **https://haveibeenpwned.com** permet de vérifier que votre messagerie n'a pas été compromise.
- Si vous cliquez sur un mauvais lien avec votre compte de l'université, changez de mot de passe aussitôt et contacter la DSIUN.

CONTACT

Direction du Système d'Information et des Usages Numériques (DSIUN)
Bâtiment T - Campus de La Garde
usagesnum@univ-tln.fr - 04.94.14.26.45
https://dsiun.univ-tln.fr

© DSIUN Pôle Usages Numériques UTLN 2022 - Ne pas jeter sur la voie publique

Formations
& sensibilisation

Consciente des enjeux liés à la sécurité du numérique, l'UTLN souhaite vous soumettre deux parcours de positionnement Pix à réaliser.

- Sécuriser l'environnement informatique : **https://app.pix.fr/campagnes/SLFSFJ527**
- Protéger les données personnelles et la vie privée : **https://app.pix.fr/campagnes/NXYBBL498**

Retrouvez ces parcours sur Moodle : Autres Enseignements / Sécurité / Parcours Pix / Sécurité du numérique

Ces parcours sont **obligatoires**. Ils permettront de vous positionner par rapport aux compétences attendues et de vous proposer des formations adaptées à vos résultats personnels.

La méconnaissance des risques en matière de cybersécurité peut compromettre notre système d'information mais également vos données personnelles : vos propres informations peuvent être revendues et valoir leur pesant d'or pour les pirates !

La sécurité est l'affaire de tous, vous en êtes le maillon essentiel !

SÉCURITÉ
DU SYSTÈME D'INFORMATION

UNIVERSITÉ DE TOULON