

Risques cyber et votre résilience numérique

MARC PARENTHOËN^{1,2}



Université inter ages. 9 octobre 2025. NIORT

Rappel des ancêtres concernant l'informatique

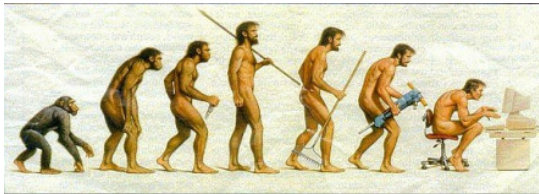
Loi n°78-17 du 6 janvier 1978 dite « informatique et libertés »

Article 1. *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*

Rappel des ancêtres concernant l'informatique

Loi n°78-17 du 6 janvier 1978 dite « informatique et libertés »

Article 1. *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*



Quelque part, quelque chose a terriblement mal tourné

Sécurité des données numériques : DIC

Intègres

FAKE

Disponibles

1

Accès momentanément indisponible

En raison d'un très grand nombre de connexions, l'accès à l'ENT est temporairement restreint.

Confidentielles



Toute donnée numérique (texte, multimédia, programme...) n'est qu'un ensemble d'octets transférables entre objets connectés

Criminalité



Des sous, de l'oseille, de la moula...

Intelligence (économique)



De l'espionnage, des renseignements, de la surveillance...

Sabotage



De la dégradation, de la pollution, de la belligérance...

Déstabilisation



De la guerre cognitive, de la réputation, de l'influence...

Déstabilisation



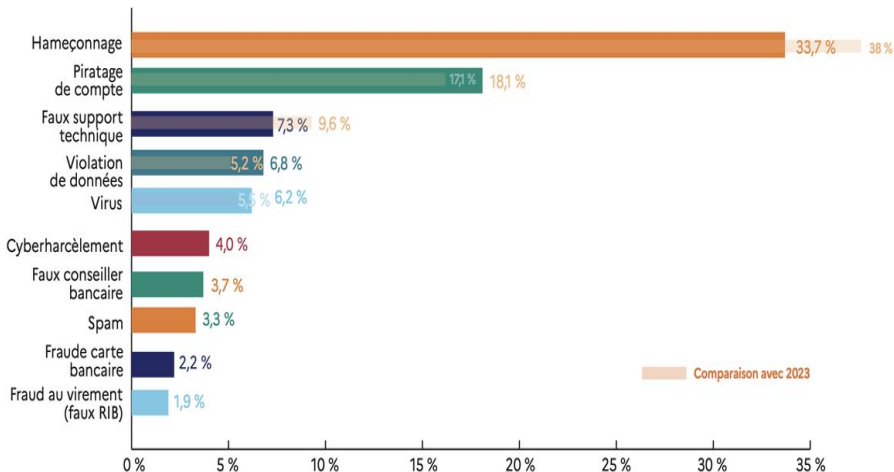
De la guerre cognitive, de la réputation, de l'influence...

Vocabulaire : cybercrimes (cybermalveillance)

- | | | |
|--|--|--|
| ● Arnaque au chantage à l'ordinateur/webcam prétendus piratés. | ● Fausses offres d'emploi créées par des fraudeurs. | ● Piratage de la téléphonie fixe. |
| ● Arnaque au chantage au site Internet prétendu piraté. | ● Fraude à la carte bancaire. | ● Proposition d'emploi non sollicitée. |
| ● Arnaque au Compte Personnel de Formation (CPF). | ● Fraude au prélèvement SEPA non autorisé. | ● Rançongiciel. |
| ● Arnaque au faux support technique. | ● FOVI. | ● Recel. |
| ● Arnaque au proche en situation d'urgence. | ● Hameçonnage (phishing en anglais). | ● Sextorsion (chantage à la webcam ciblé). |
| ● Arnaque à la fausse commande. | ● Litige commercial. | ● Spam électronique. |
| ● Arnaque commerciale. | ● Logiciel publicitaire. | ● Spam téléphonique. |
| ● Arnaque nigériane. | ● Machine zombie. | ● Usurpation d'identité. |
| ● Arnaque téléphonique (pingcall en anglais). | ● Piratage d'un objet connecté. | ● Usurpation de numéro de téléphone (phone spoofing en anglais). |
| ● Contenu illicite. | ● Piratage d'un système informatique – Professionnels. | ● Violation de données – Professionnels. |
| ● Contrefaçon. | ● Piratage d'un système informatique – Particuliers. | ● Violation de données personnelles – Particuliers. |
| ● Cyberharcèlement. | ● Piratage de compte en ligne. | ● Violation de données personnelles – Professionnels. |
| ● Défiguration. | ● Piratage de compte bancaire. | ● Virus. |
| ● Dénî de service. | ● Piratage de l'espace personnel d'un recruteur (site d'emploi). | ● Vol d'identité. |
| ● Escroquerie sentimentale. | | ● Vol de carte bancaire. |

Cybermalveillances les plus fréquentes (2024)

• Particuliers



Principales recherches d'assistance pour les particuliers



makeameme.org

95% des attaques commencent par un phishing



C. pén. Des atteintes aux STAD. Articles 323-1 à 323-8.

95% des attaques commencent par un phishing

Quels sont les signes qui doivent vous alerter du risque d'arnaque :

a

Demande de mise à jour ou de confirmation de données personnelles

c

Appel à l'aide

b

Défaut de paiement ou problème de facturation

d

Demande d'informations inattendue



UNIQUE PASSWORD



EVERY SITE

Risque

Usurpation
d'identité

Dark web

`https://
haveibeenpwned.
com/`

Prévention

Politique de
mots de passe

Code pénal

Articles 226-16
à 226-24

GIP ACyMa cybermalveillance.gouv.fr

Actions contre la cybermalveillance (ACyMa)



- 1 sensibilisation au risque numérique
- 2 assistance aux victimes d'actes de cybermalveillance
- 3 observation et anticipation de la menace

Plateforme <https://www.cybermalveillance.gouv.fr>

- particuliers, entreprises, associations, collectivités territoriales
- guichet central d'assistance des victimes de cybermalveillances
- diagnostic, conseils et mise en relation avec des spécialistes

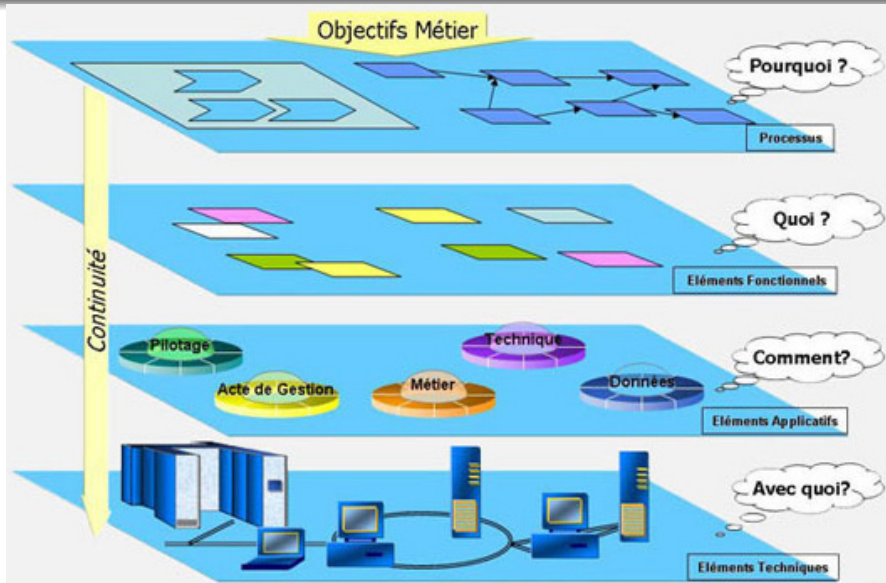
Dispositifs similaires : cert.govt.nz et lhc.lu

Identifier ses criticités

**Quelles sont les adhérences
de mes activités essentielles
à mon système d'information ?**

Autrement dit, comment je réalise mes activités essentielles si mon système d'information est HS ?

Vue fonctionnelle d'un SI : quoi ?



Mon adhérence numérique

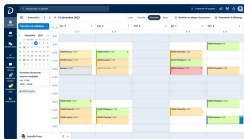
Être vivant

respirer, boire, manger, se soigner, se déplacer, habiter...

Être social

prouver vos droits, s'informer, se cultiver, débattre, voter...

Être à la retraite, actif et connecté



Sauvegarde des données critiques : 321



3 sauvegardes,

2 endroits,

1 déconnectée

Que faire en cas de cyberattaque ?

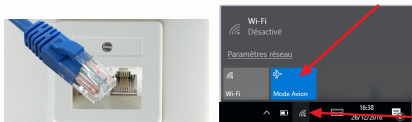


Connecté à votre box ou point d'accès cellulaire

- ❶ **Déconnecter immédiatement du réseau (eth et wifi)**
- ❷ Ne pas éteindre/redémarrer la machine infectée
- ❸ Ne pas reconnecter la machine sur un autre système d'information
- ❹ **Alerter** vos proches, votre banque, votre assurance...
- ❺ Avec une autre machine, changer les mots de passe de vos services essentiels
- ❻ **Porter plainte**
- ❼ Lâcher un billet à un prestataire informatique pour nettoyer et durcir votre machine
- ❽ Pourquoi ne pas en profiter pour **passer au libre** : (Zorin-OS Lite, Mint-XFCE, Linux-Lite...)
- ❾ Réinstaller vos données sauvegardées après avoir fait vérifier par le prestataire qu'elles ne sont pas corrompues

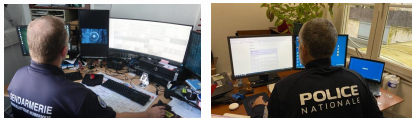
Réagir en images :

Couper l'accès internet

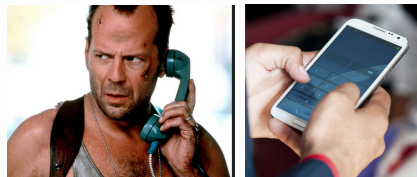


Garder la machine allumée

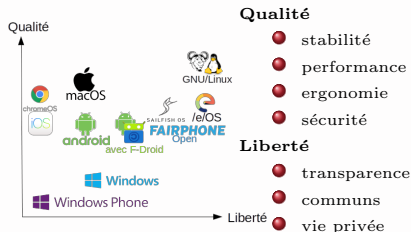
Porter plainte



Alerter ses proches, sa banque



Durcir son système



Quelques liens qui peuvent vous aider...

- Signaler un contenu illicite :
<https://internet-signalement.gouv.fr/>
- Police et Gendarmerie Nationale :
<https://17cyber.gouv.fr/>
- Assistance et prévention en cybersécurité :
<https://www.cybermalveillance.gouv.fr/>
- Trousse de premiers soins numériques :
<https://digitalfirstaid.org/fr/>
- Installer Linux à la place de Windows10 :
Ateliers du Bocage, 15 rue de la gare, Niort

Notions de cyberrésilience pour les particuliers...

- 1 Les cyberrisques
 - Sécurité sur les données
 - Menaces : motivation des attaquants [ETL 2024]
 - Tactiques courantes
- 2 Prévenir les risques cyber
 - Maintenir son esprit critique
 - Préserver son identité numérique
 - Se former aux cyberrisques
- 3 Mon adhérence numérique
 - Anticiper la crise
 - Dépendance numérique
 - Sauvegardes
- 4 Réagir
 - À la maison
 - Pour aller plus loin
- 5 Conclusion

Risques cyber et votre résilience numérique

MARC PARENTHOËN^{1,2}



Université inter ages. 9 octobre 2025. NIORT

Merci !