Sensibilisation à la cybersécurité

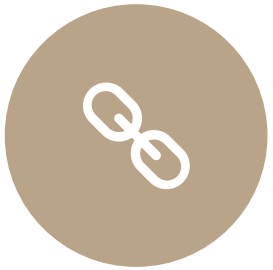
La gestion et la protection des données

Laurent Linard

Les objectifs de la sensibilisation

APPRENDRE À APPLIQUER LES BONNES PRATIQUES ;

SAVOIR COMMENT RECONNAITRE LES MENACES LES PLUS COURANTES ;



LE LIEN AVEC VOTRE TRAVAIL AU QUOTIDIEN ;

LEVER LES INTERROGATIONS PAR RAPPORT À LA SÉCURITÉ DE L'INFORMATION ET LA CYBER SÉCURITÉ.

Cadre légal
Le RGPD

Le RGPD impose à toutes les entreprises et organisations étatiques européennes une série d'exigences pour protéger les données des citoyens. Il impose notamment des besoins de sécurité comme le modèle CIA et une traçabilité dès que des données personnelles permettent d'identifier directement et/ou par recoupement une personne physique.

Cadre légal : le RGPD

Le RGPD en moins de 2 min

Cadre légal
Le RGPD

Actuellement quel process est en place:

Tout porteur de projet :

1. Remplit une fiche projet ;
2. Complète des informations relatives au « RPGD » ;
3. Il est ensuite recontacté par la cellule sécurité de l'information pour fournir davantage d'éléments, via un questionnaire.
    1. Il est accompagné par la cellule
    2. Cela débouche :
        1. sur une analyse de la sécurité de l'information
        2. sur un avis de conformité RGPD

Introduction: La sécurité de l'information?

Que signifie pour vous la « sécurité de l'information »?

- **Définition:** La sécurité de l'information est un ensemble de pratiques, de moyens (techniques, organisationnels, humains, juridiques) visant à protéger des informations.
- Il s'agit de l'information sous toutes ses formes et indépendamment des supports: logiciel, matériel, papier, savoir-faire…
- Exemple: logiciels RH, données des employés, …

- La sécurité de l'information est la protection de la *confidentialité*, de l'*intégrité* et de la *disponibilité* de l'information (source: ISO 27000).

1. Les bases de la sécurité de l'information

- Les besoins de sécurité (critères) fondamentaux
- Le triangle de la sécurité
- Définition de la donnée
- Définition d'un traitement de données

1. Les bases de la sécurité de l'information

Les critères fondamentaux

- CONFIDENTIALITÉ :
- QUI PEUT AVOIR ACCÈS ET POURQUOI ?

- INTÉGRITÉ :
- L'INFORMATION EST CORRECTE.

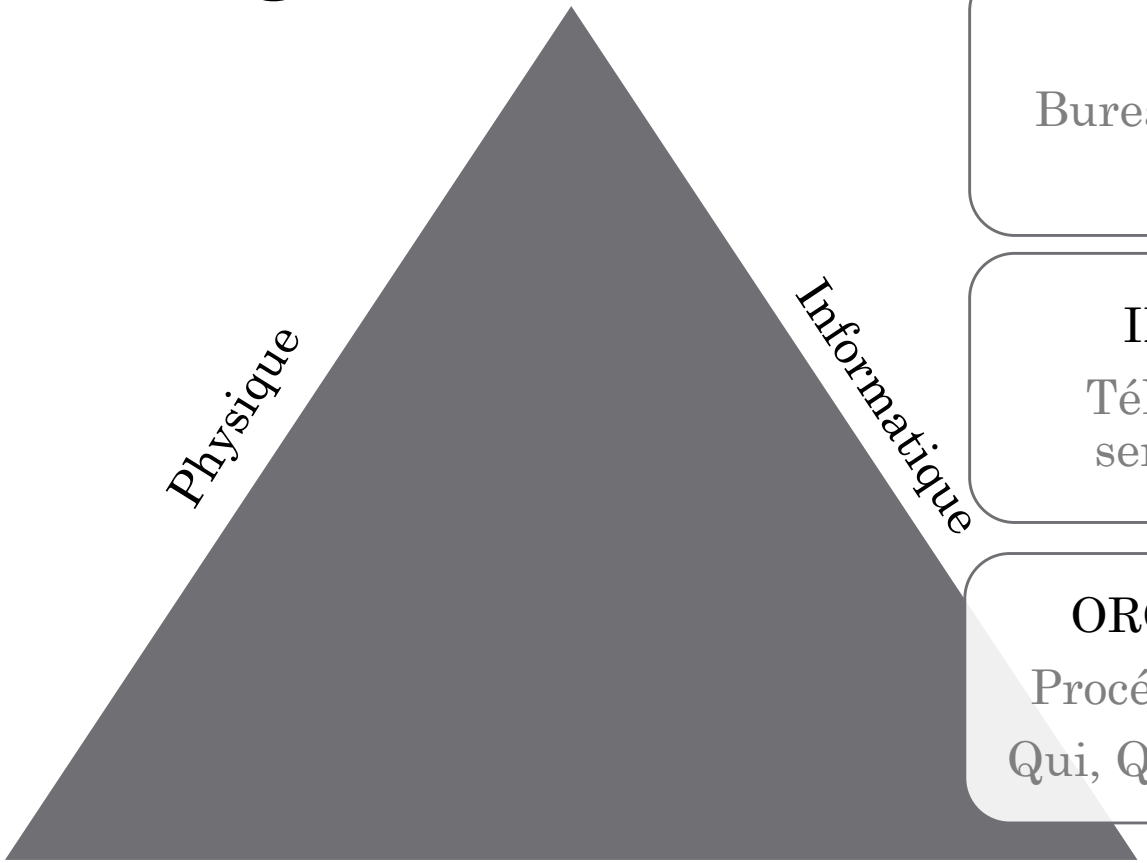
- DISPONIBILITÉ (Avaibility) :
- ACCESSIBLE ET UTILISABLE. Plus Internet? Nous avons la 4G!

- (TRACABILITÉ)
- CONSERVATION DES TRACES ET MOUVEMENTS

- (AUTHENTICITE)
- PROUVER SON IDENTITE ou l'AUTHENTICITE de l'action

MODELE
CIA
+T
+A

1. Les bases de la sécurité de l'information
Le triangle de la sécurité



PHYSIQUE:

Bureau, immeuble, voiture, armoires,…

INFORMATIQUE :

Téléphone, ordinateur, serveurs, accès wifi,…

ORGANISATIONNEL :

Procédures et Management

Qui, Quoi, Comment, Quand?

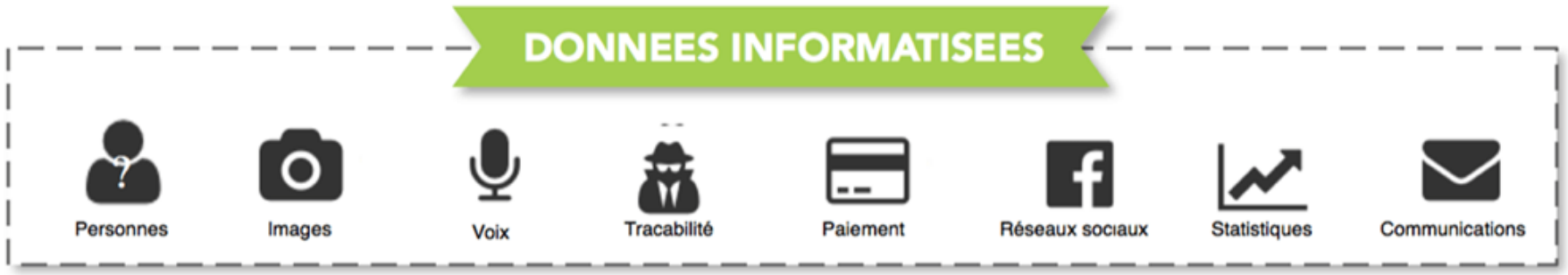
1. Les bases de la sécurité de l'information

Qu'est-ce qu'une donnée à caractère personnel (DACP)?

1. Une **donnée personnelle (DACP)** est toute information se rapportant à une personne physique identifiée ou identifiable

2. Une **donnée sensible (DACPS)** : information qui révèle
   - la prétendue origine raciale ou ethnique,
   - les opinions politiques,
   - les convictions religieuses ou philosophiques ou l'appartenance syndicale,
   - ainsi que le traitement des données génétiques,
   - des données biométriques
   - des données concernant la santé
   - des données sur l'orientation sexuelle

PAPIER aussi !



Est-ce une DACP/DACPS ou pas ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Le jeux des données DACP / DACPS /

ou pas ?

Copie de Carte d'identité	N° TVA BE 0567 789 654	Claude.delamarne@gmail.com
Bidibule.1980@skynet.be	Compte Bancaire Laura Miretti de BPOST	Compte bancaire ING de d'une organisation
0476 78 90 45	contact@spw.be	Fiche de paie d'André
Empreinte du pouce	Adresse postale d'une entreprise	Registre National
Information syndicale d'un employé	Adresse postale de l'apprenant	Liste des délégués syndicaux

Selon vous, que veut-on dire par "traitement de données" ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Les bases de la sécurité de l'information

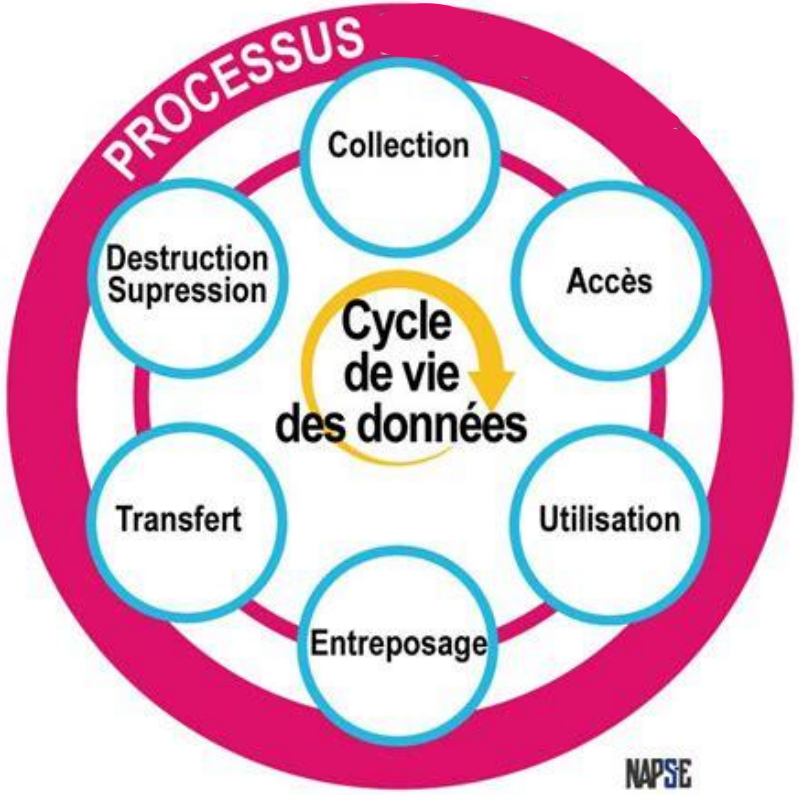
Un traitement

- **C'est quoi un traitement de données ?**

- Toute opération ou tout ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé.

- Il n'est pas nécessairement informatisé (il y a aussi les fichiers papiers),

- *Collecte, enregistrement, conservation, modification, utilisation, transmission, diffusion…*



Sécurisation à chaque stade !

Les bases de la sécurité de l'information

Un traitement - suite

- Un traitement de données doit avoir un objectif et une finalité déterminés préalablement au moment du recueil de celles-ci ainsi qu'au moment de leur exploitation.
- Exemples de traitements :
- Tenue du registre des sous-traitants,
- Gestion des ressources humaines,
- Gestion des salaires,
- Gestion des inscriptions,
- Accès-consultation d'une base de données,
- … le simple fait de se constituer une liste de noms et prénoms sur papier etc…

Vous avez dit données ? Oui mais lesquelles ?

- Le personnel ?
- Les partenaires ?
- Les clients ?
- Et où sont-elles ?
- Matériel informatique et appareils mobiles :
  - ± des centaines (pc, tablettes, GSM,…)
  - Chiffres en croissance constante

INTERNATIONAL • BELGIQUE

Partage

Une attaque informatique massive a paralysé les services publics belges

Des pirates s'en sont pris par vagues successives à Belnet, mardi 4 mai, un acteur majeur de l'accès à Internet du pays. Les auteurs n'ont pas encore été identifiés.

Par Jean-Pierre Stroobants (Bruxelles, Correspondant)

Publié le 05 mai 2021 à 11h54 - Mis à jour le 05 mai 2021 à 12h53 · Lecture 3 min.

Article réservé aux abonnés

Cybersécurité: la longue convalescence d'un hôpital hack

Du Trends-Tendances du 01/07/2021 05/07/21 à 09:00 Mise à jour à 10:40

Source : Trends-Tendances

Gilles Quoistiaux
Journaliste Trends-Tendances

Six mois après la cyberattaque, le Centre Hospitalier de Wallonie picarde n'a pas encore pu relancer l'ensemble de ses systèmes informatiques. Récit d'une longue bataille contre un ennemi invisible.

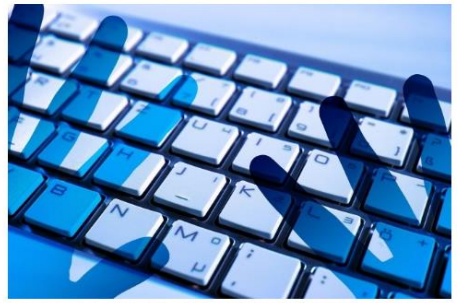
TOUTE L'ACTUALITÉ / SÉCURITÉ / **INTRUSION, HACKING ET PARE-FEU**

La faille dans Log4j piège le ministère belge de la Défense

Jacques Cheminat, publié le 21 Décembre 2021

12-0-24

Le ministère belge de la Défense joue la transparence en admettant avoir été victime d'un piratage reposant sur la faille Log4Shell. L'exploitation de cette dernière bat son plein en intégrant des malwares comme Dridex.



Le ministère belge de la Défense a précisé que la cyberattaque avait eu lieu la semaine dernière et a paralysé plusieurs services. (Crédit Photo: Geralt/Pixabay)

SUIVRE TOUTE L'ACTUALITÉ

Newsletter

Recevez notre newsletter comme plus de 50 000 professionnels de l'IT!

JE M'ABONNE

ACCUEIL • SOCIÉTÉ

Une cyberattaque touche l'administration à Liège: le personne peut pas allumer son ordinateur

La Ville de Liège analyse l'ampleur de l'attaque informatique dont elle fait l'objet depuis lundi.

Accueil » Actualité » La Barbie connectée va-t-elle espionner vos enfants ?

La Barbie connectée va-t-elle espionner vos enfants ?

par **EDOUARD LE RICQUE**, le 18 mars 2015 09:00

L'inconnu parlait au bébé : l'angoissante histoire d'un babyphone hacké

Accueil / Cyber sécurité / Loi internet / Technologies et politique

La Belgique frappée par une cyberattaque de grande ampleur

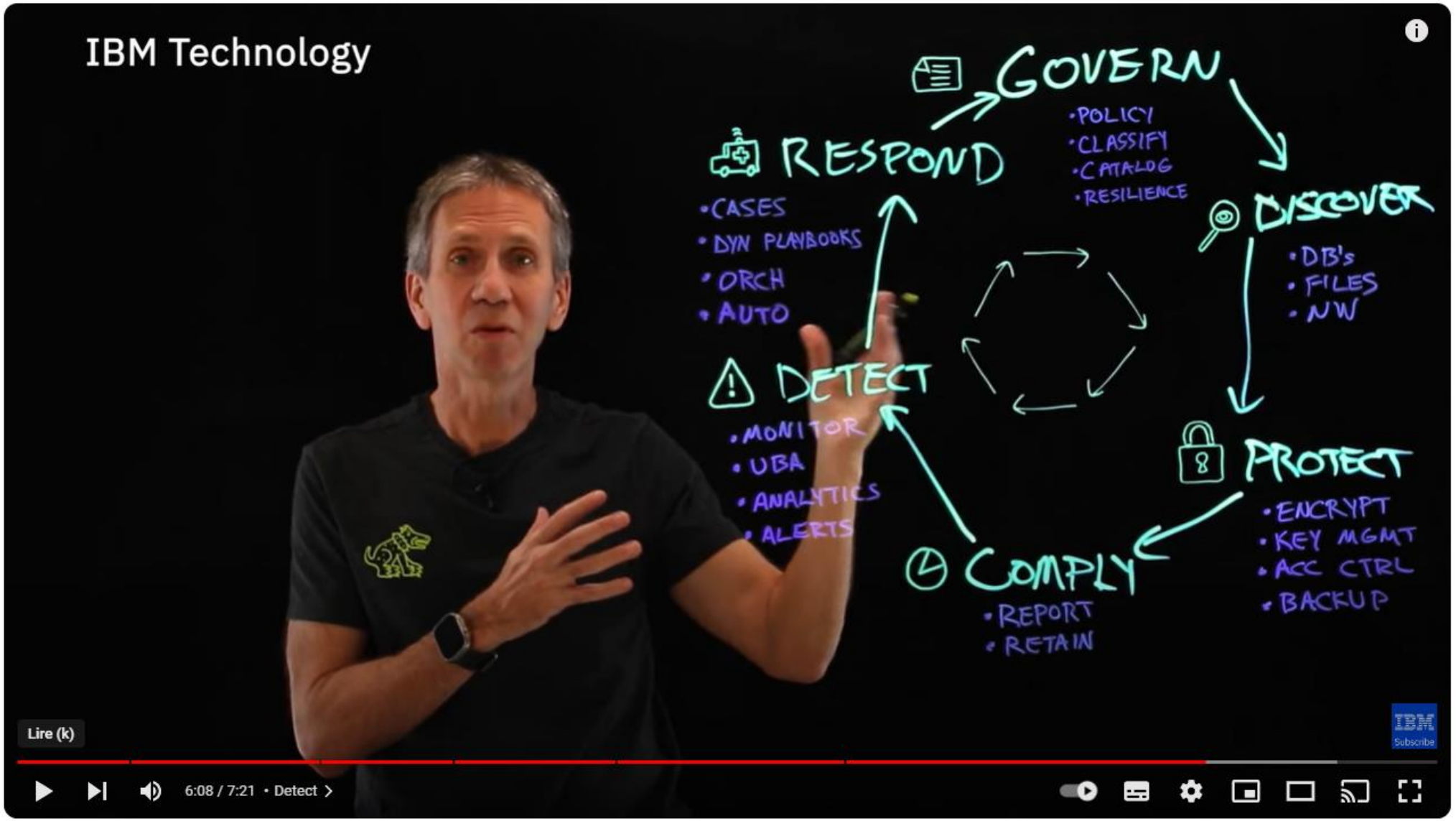
L'ULB relance ses serveurs après avoir été ciblée par une cyberattaque

RTBF

Publié le lundi 02 mars 2020 - Mis à jour le lundi 02 mars 2020 à 15h08

La gestion et la protection des données

Une approche Pro



https://www.youtube.com/watch?v=N8xEgSe5RwE

La cybersécurité et les types de menaces facteur d'insécurité

- Pourquoi ces attaques peuvent réussir?

1. Mauvaise Organisation ;
2. Mauvaise Protection Physique ;
3. Mauvaise Protection Informatique ;

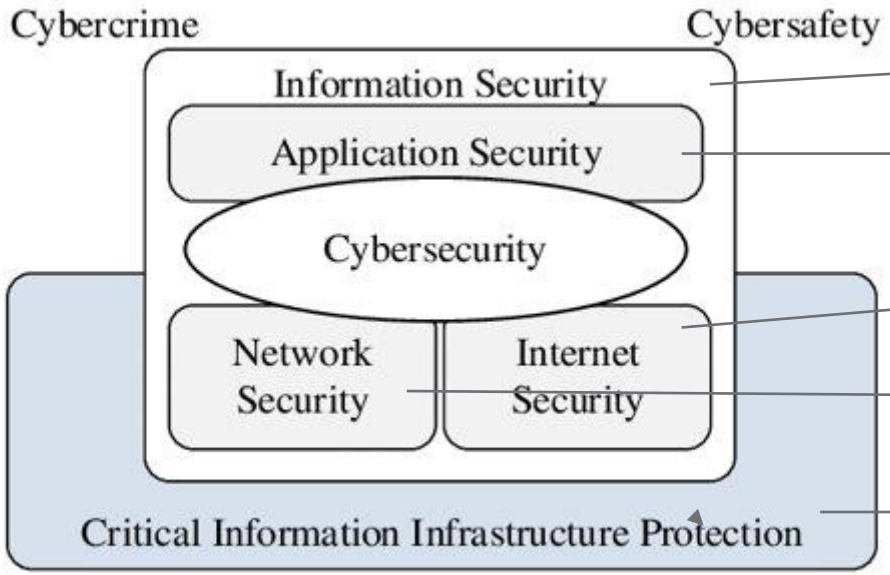
- Malgré toutes les précautions possibles, la sécurité 100% n'existe pas et n'existera jamais.

La cybersécurité et les types de menaces
Les facteurs d'insécurité

1. Mots de passe faibles, devinables ou codés en dur (dans la page du site ou de l'appli) ;
2. Services de réseaux non sécurisés ;
3. Interfaces utilisateurs non sécurisés ;
4. Absence de mécanisme de mise à jour sécurisée ;
5. Utilisation d'éléments insécurisés ou obsolètes ;
6. Protection insuffisante de la vie privée ;
7. Transfert et stockage de données non sécurisées ;
8. Manque de gestion des dispositifs ;
9. Paramètres par défaut non sécurisés ;

La cybersécurité et les types de menaces

La cybersécurité :



Sécurité des informations

Sécurité des applications

Sécurité de l'internet

Sécurité du réseau

Sécurité de l'infrastructure

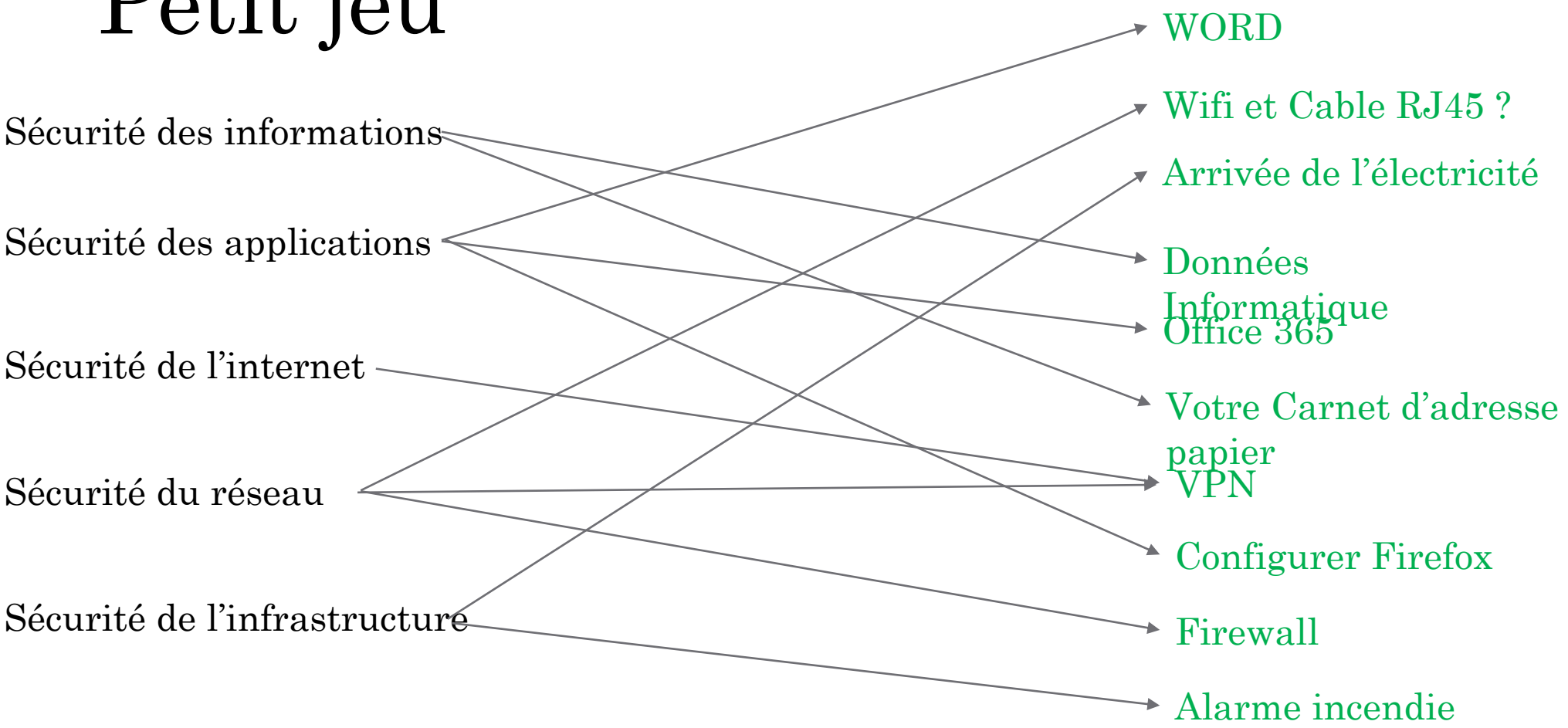
Reliez le type de sécurité à ce qu'il représente

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

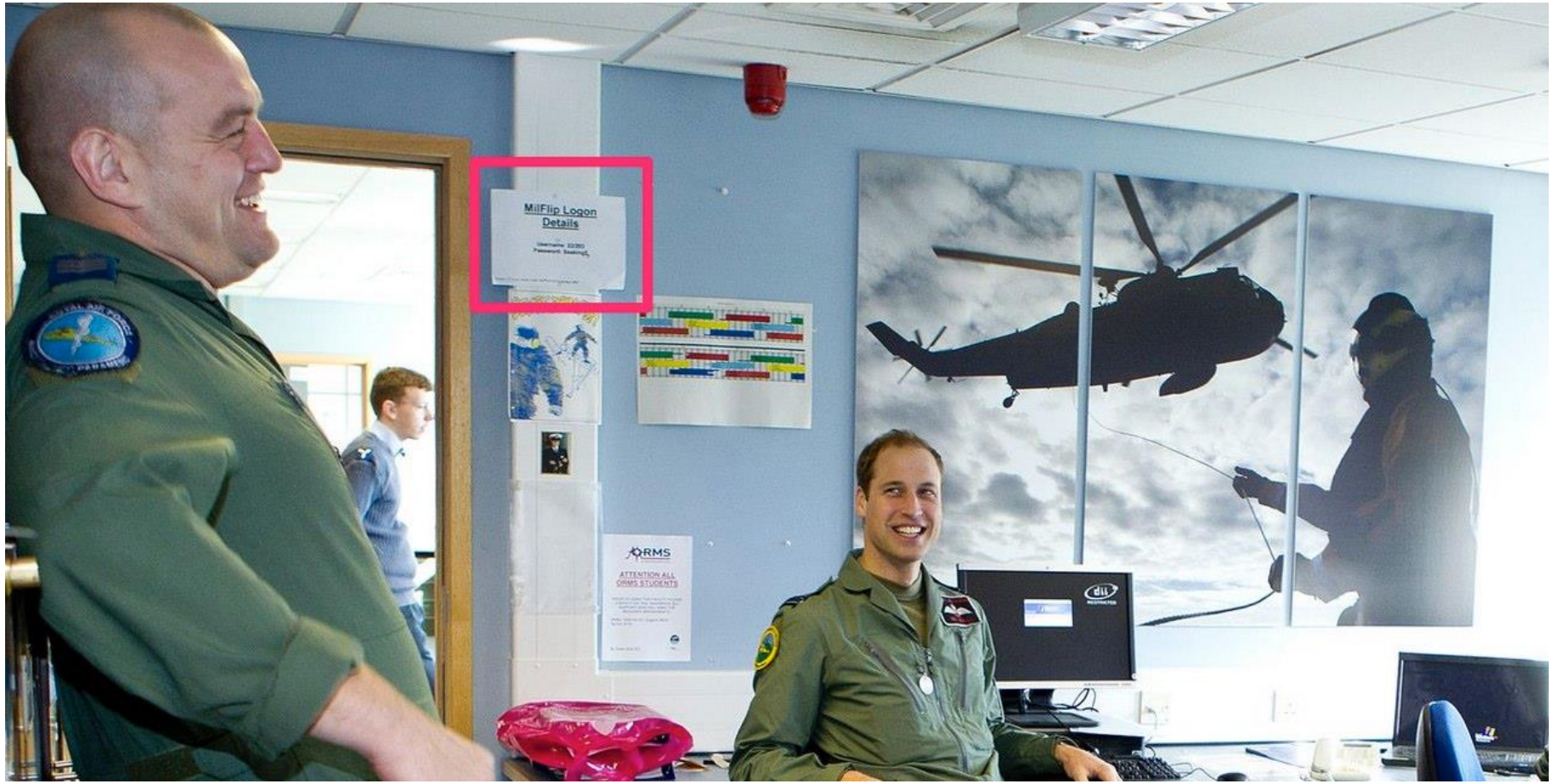
Code d'événement
CRF23

Petit jeu


Sécurité des informations
Sécurité des applications
Sécurité de l'internet
Sécurité du réseau
Sécurité de l'infrastructure
WORD
Wifi et Cable RJ45 ?
Arrivée de l'électricité
Données Informatique
Office 365
Votre Carnet d'adresse papier
VPN
Configurer Firefox
Firewall
Alarme incendie

L'erreur est humaine et ça passe à la télé ;)

Même chez les pros



Les bons réflexes à adopter
L'usage mixte personnel/professionnel

- Télétravail – Conseils
- VPN
- L'environnement de travail: La sécurité du bâtiment
- L'environnement de travail : Votre espace de travail
- L'environnement de travail: vos déplacements
- La destruction et l'effacement
- Vos appareils mobiles
- Les réseaux sociaux
- Mises à jour et installation

Les bons réflexes à adopter Télétravail les 12 recos utilisateurs

1. Séparez le privé du professionnel ;
2. Suivez les consignes de l'administration (cette formation) ;
3. Votre comportement doit rester dans l'optique professionnelle ! (comme au bureau) ;
4. Ne reportez pas les mises à jour !
5. Antimalware doit être professionnel :
   - WINDEFENDER ou autre
   - …un petit scan de temps en temps ;
6. Phrase passe et multi facteur le plus souvent possible !

Les bons réflexes à adopter Télétravail les **12** recos utilisateurs

7. Votre connexion WIFI et pas celle du voisin !

8. Plan de sauvegarde de votre travail et pas de sauvegarde sur des clés USB privées …

9. Attention au PHISHING/SMISHING (Mail ; SMS ; Messageries ; Pièce(s) jointe(s) ; Lien …) ;

10. Ordinateur professionnel > ne rien installer de privé !

11. Conservez vos ordinateurs hors de portée des enfants (+Verrouillage de l'écran) ;

12. Prenez conseils auprès du service IT si vous n'avez pas de solutions sécurisées ;

Les bons réflexes à adopter Télétravail : Conseils

- pour transférer des données ou des fichiers :

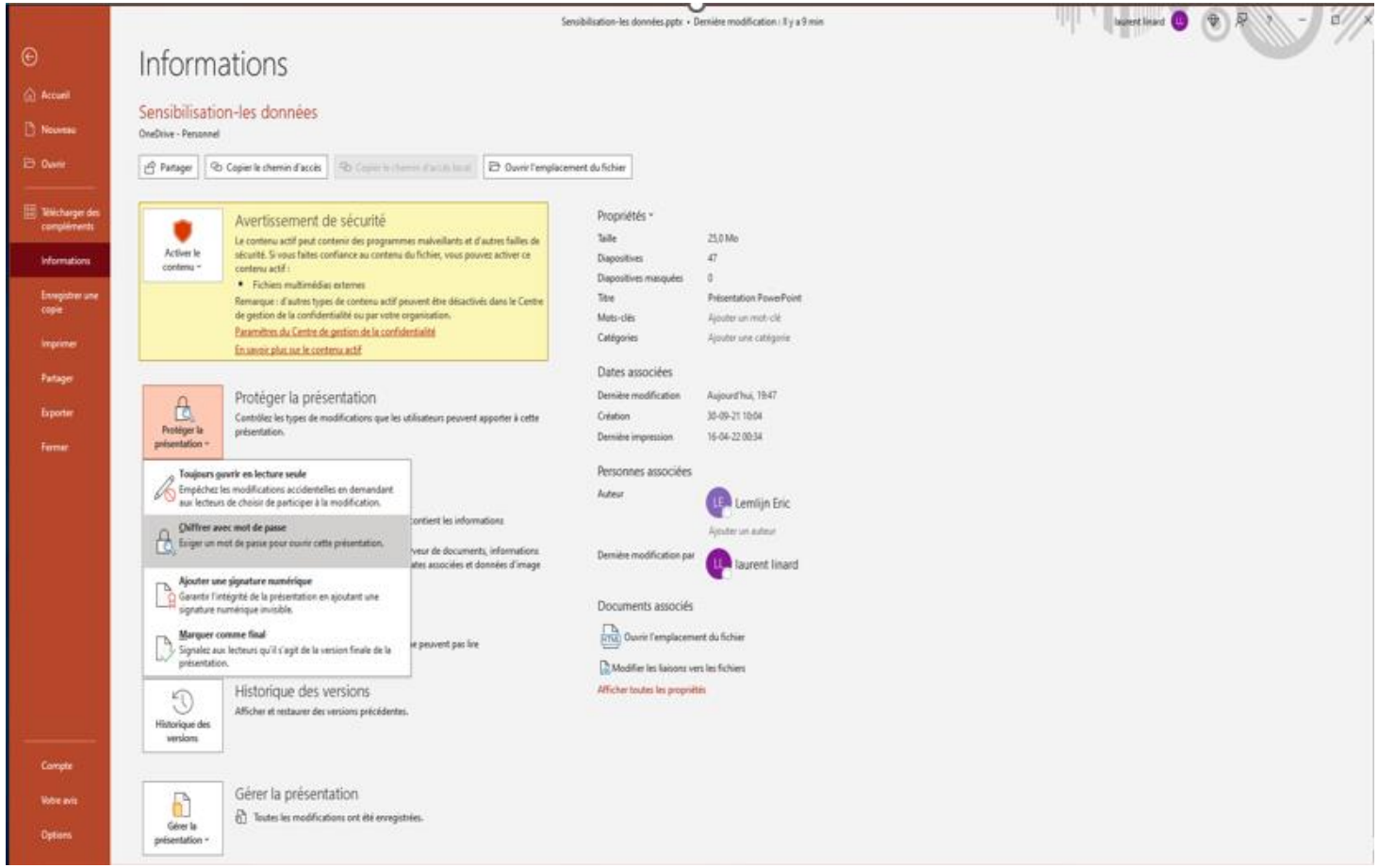
Ne pas utiliser les outils :

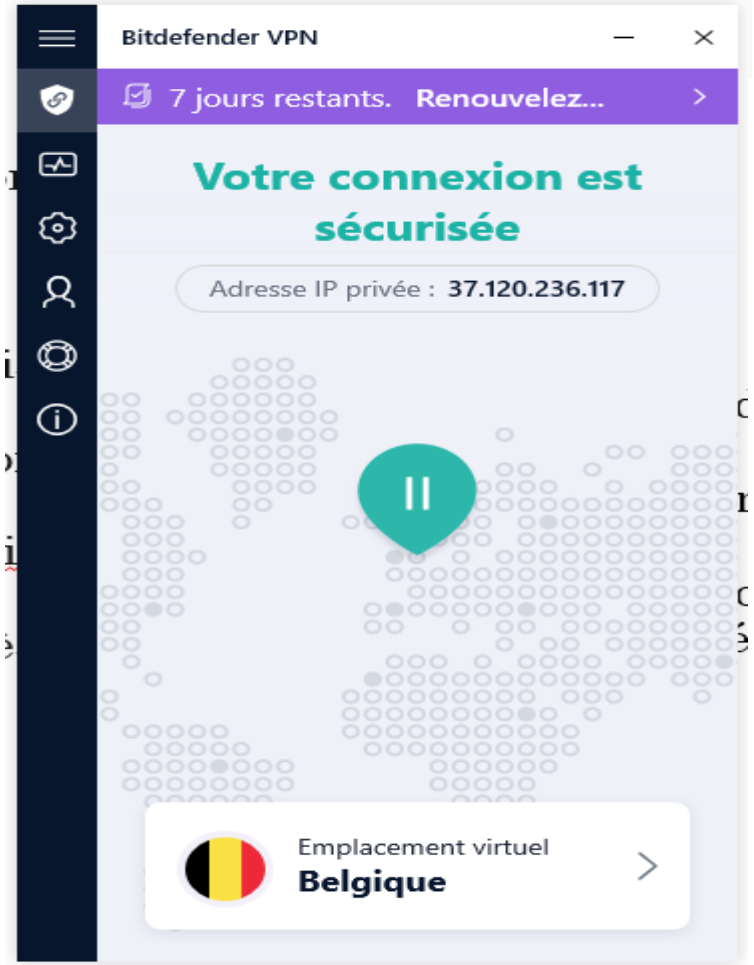
- Google
- DropBox
- WeTransfer
- Linkedin
- ZOOM
- MESSENGER
- WHATSAPP
- FACEBOOK

Privilégier :

- Office 365
  - TEAMS
  - OneDrive
  - SharePoint
  - OUTLOOK

Simple comme un mot de passe.





Les bons réflexes à adopter VPN

- Sécuriser la connexion
- Chiffrement
- Données non lisibles par des tiers
- Connexion anonyme (ou presque)
- Votre adresse IP est modifiée
- Vous avez accès au monde entier

Vidéo VPN

Wifi lieux publics / Pirates inspirants

https://www.youtube.com/watch?v=LiRVDHC3skA

https://www.youtube.com/watch?v=N_WH3rQCPi8

Dès que j ai fini d'utiliser mes données … que faire ?

https://www.youtube.com/shorts/58eztp2Dy5s

La sécurité de vos appareils mobiles

- Ne pas laissez votre sac ou vos appareils dans votre voiture
- Ne stockez pas d'informations confidentielles sans protection
- Protégez l'accès avec un code PIN
- Désactivez le Wifi et le Bluetooth quand vous ne vous en servez pas
- Contrôlez les autorisations de vos applications

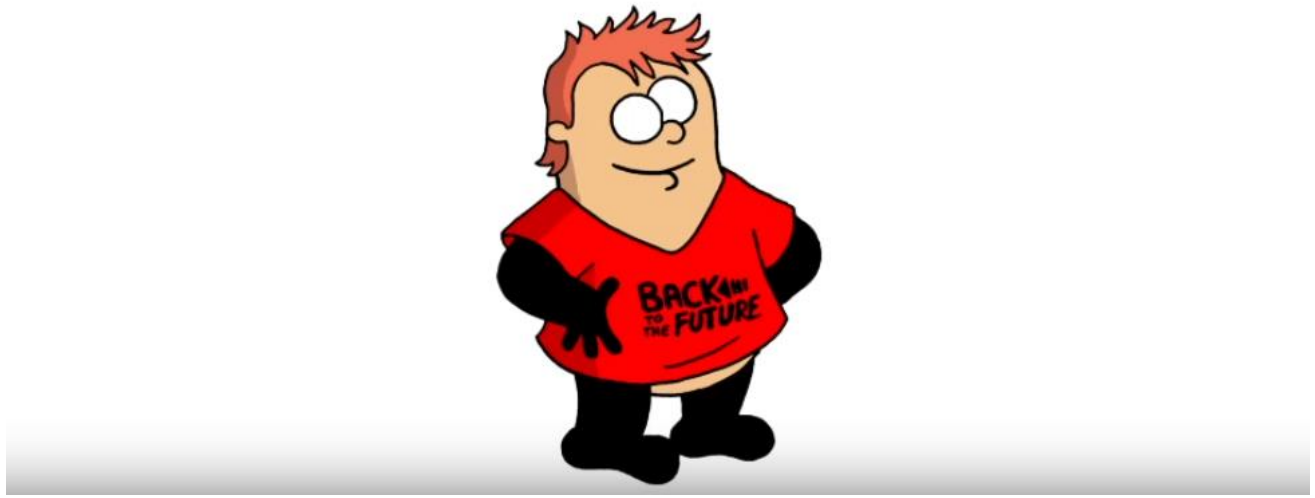
Ordinateur
Téléphone !

La sécurité sur les réseaux sociaux

- Ne communiquez pas vos données personnelles (date de naissance, adresse, N° téléphone)
- **Vérifiez vos paramètres de confidentialité**
  - Configurez les !
  - Renseignez-vous
- **Maitrisez vos publications**
- Faites attention à qui vous parlez ou chattez
- Contrôlez les applications (trop intrusives)
- Supprimez votre compte si vous ne l'utilisez plus

Les réseaux sociaux

Pause vidéo sécurité obligatoire



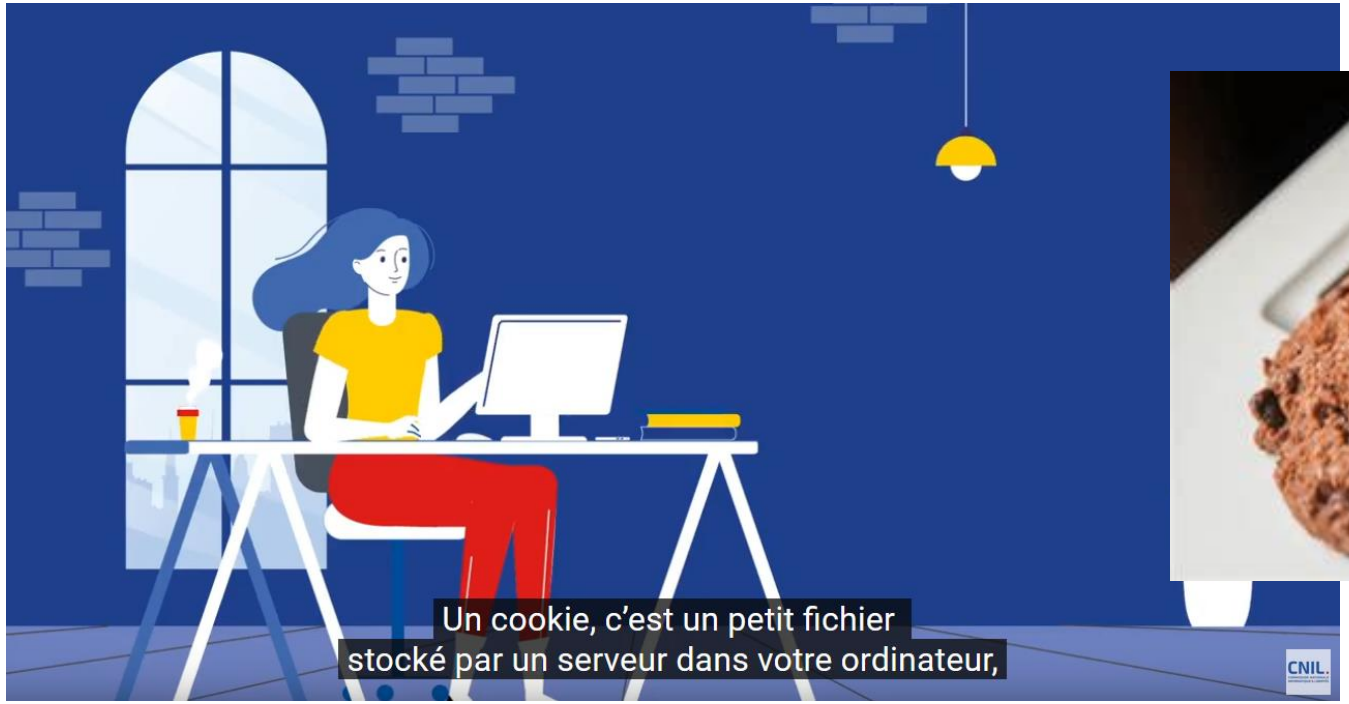
https://www.youtube.com/watch?v=kz3Zb_Y_wJw

1. Utilisez un MAX d'outils dédiés à protéger votre vie privée pour éviter de laisser des traces ! Voir les effacer assez souvent !

2. Utilisez des pseudos et pour les choses très personnelles choisissez bien vos outils !

3. Evitez de tout centraliser dans un seul endroit !

Pause vidéo sécurité obligatoire



Super CNIL is BACK !

https://www.youtube.com/watch?v=a9kiQPV_SPg

Les bons réflexes à adopter Comprendre les navigateurs

- Lorsque vous visitez un site Web, vous donnez des informations sur vous-même au propriétaire du site, sauf si des précautions sont prises.
- Votre navigation sur Internet peut être suivie par les sites que vous visitez et les partenaires de ces sites.
- Visitez un site Web sur Internet n'est jamais une connexion directe. De nombreux ordinateurs, appartenant à de nombreuses personnes différentes sont impliqués.
- Ce que vous recherchez est d'un grand intérêt pour les fournisseurs de recherche.
- Il est plus sage de faire confiance aux navigateurs Open Source car ils peuvent être plus facilement audités en termes de sécurité. (+Protection des données)
- Attention les **cookies** ça tracent.

La sécurité de vos e-mails

- Activez un message automatique en cas d'absence (Oui pour le boulot (différence interne/externe) et Non conseillé pour le privé) ;

- Mutation ou départ : transférez à son responsable tous les messages électroniques de nature professionnelle devant être traités ou nécessaires à la gestion des dossiers en cours de traitement ou à venir ;

- Archivez les messages d'ordre privé (tolérance) ;
  - Indiquez dans l'objet du message PRIVé

Mises à jour et installation

- **Eteignez votre ordinateur** à la fin de la journée est différent de le **mettre en veille**.
- Laissez les **mises à jour se télécharger et s'installer** ! Ne jamais reporter. (Ordinateur, Tablette et/ou téléphone)

- **Demandez l'autorisation à l'IT** :
  - Téléchargez un programme
  - Connectez du matériel externe (ex: pilotes imprimante, casque, écran…)

Les bonnes pratiques : Soyez vigilants