



**FUTURZO**



**Les réseaux du futur**

# Sensibilisation Cybersécurité

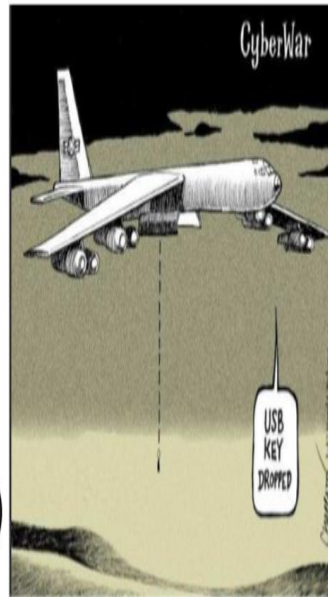


***« Tous connectés, tous impliqués, tous responsables » FIC2019 - ANSSI***

# CYBERESPACE

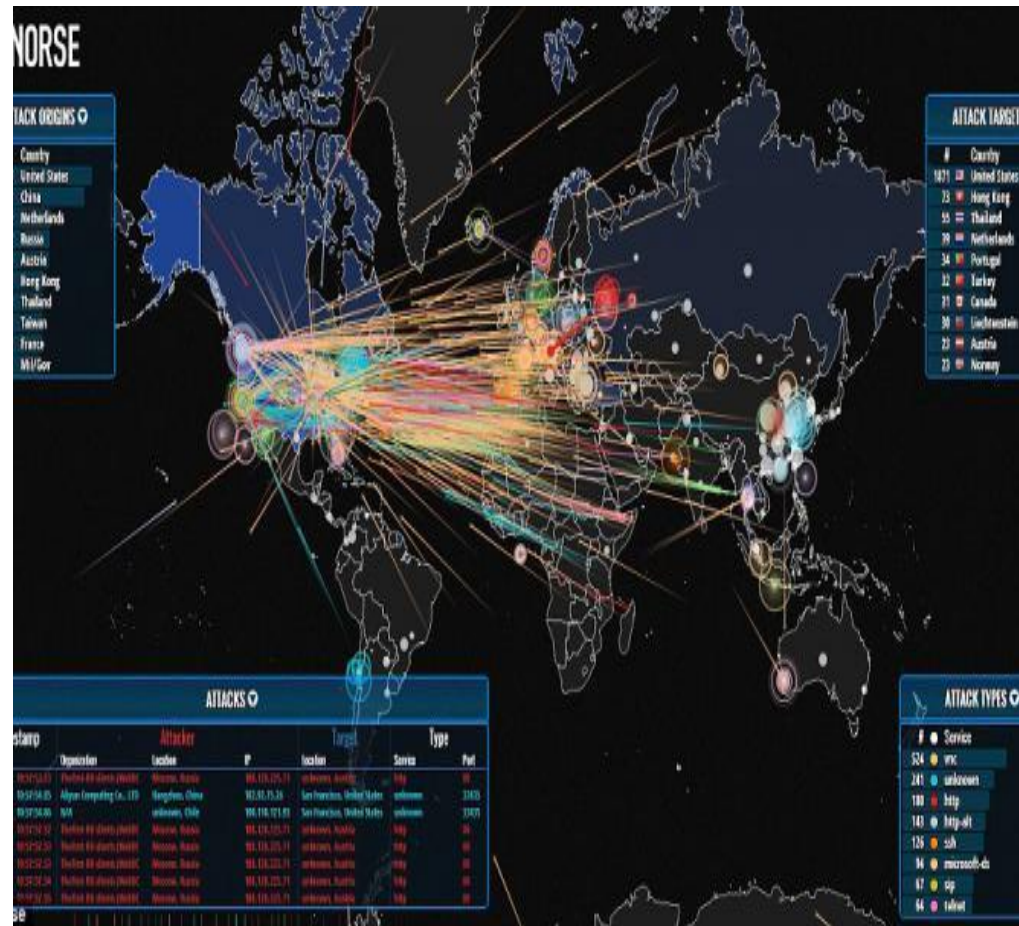
Une nouvelle dimension des conflits :

- Iran (2007) : Stuxnet
- Estonie (2007) ;
- Géorgie (2008) ;
- Ukraine (2013) ;
- Wannacry, NotPetya (2017)
- ...



Évolution des doctrines : reconnaissance d'un nouveau domaine de combat et non plus un secteur technique

- OTAN, UE ;
- US, FR, UK, ...



Les attaques sont permanentes, de plus en plus nombreuses, de plus en plus complexes et de plus en plus coûteuses.....mais il faut relativiser le risque et faire preuve de bon sens

## Quelques chiffres

**400 MILLIONS DE DOLLARS**

perte financière estimée liée aux fuites de données, provenant de 700 millions de données compromises.

**79 790 INCIDENTS**

dans 61 pays en 2014, avec 2122 cas avérés de perte de données

**38%**

quelques secondes suffisent aux attaquants pour compromettre un système. Et dans 28% des cas, il ne faut que quelques minutes pour voler les données

**82 SECONDES**

temps qui s'écoule entre l'envoi d'une campagne de phishing et le premier clic. Au total, 23% des destinataires ouvrent les emails, **11% cliquent.**

**99,9% DES VULNÉRABILITÉS EXPLOITÉES**

99,9% des vulnérabilités des systèmes sont exploitées plus d'un an après avoir été identifiées

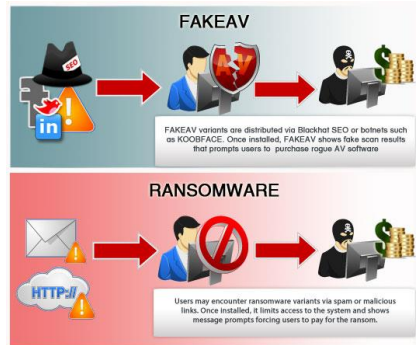
**170 MILLIONS DE MALWARES**

**30% D'ERREURS HUMAINE**

**75% des attaques : erreurs humaines, menaces internes, malwares**

# LES OBJECTIFS DES ATTAQUANTS

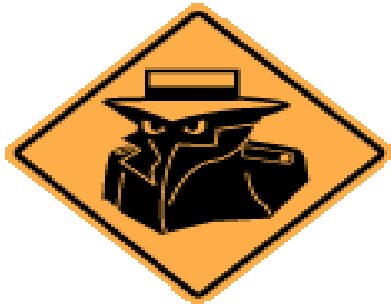
## LES TRAFICS ILLICITES



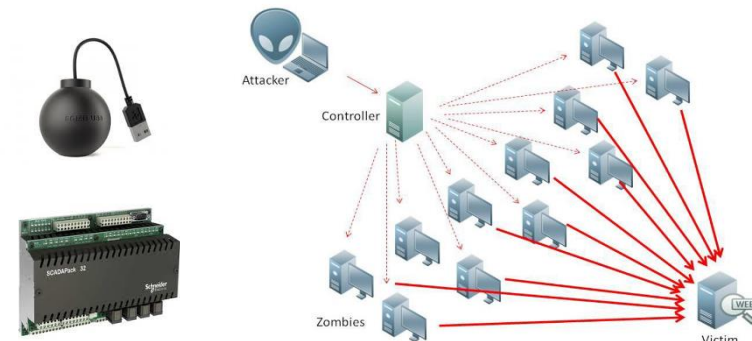
## LA DESTABILISATION



## L'ESPIONNAGE INFORMATIQUE



## LE SABOTAGE INFORMATIQUE





# CYBERATTAQUANTS





- Phishing
- Social engineering,
- Malwares,
- Ransomwares,
- SPAM, HOAX,
- Attaques par déni de service,
- RAT,
- Exploitations de failles connues ou inconnues (0-day),
- ...



# PANORAMA DE QUELQUES CYBERMENACES

## Ryuk, un ransomware qui coûte très cher aux entreprises



**Sécurité** - Les cybercriminels derrière le ransomware Ryuk exigent des sommes énormes en Bitcoin pour libérer les fichiers chiffrés dans des attaques qui semblent très ciblées.

Mercredi 22 Août 2018 par Danny Palmer

5 commentaires

## Windows Defender bloque une importante campagne de cryptomining



**Sécurité** - L'équipe de Microsoft revient sur une campagne de cryptomining détectée et bloquée par Windows Defender dans le début de la semaine. Celle-ci avait recours à la technique dite du « Process hollowing » qui lui permet de rester sous le radar des outils de détection.

Jeudi 08 Mars 2018 par Louis Adam

2 commentaires

## Le groupe Ramsay-Générale de santé victime d'une cyberattaque

19/08/2019 0 94

PARIS (TICsanté) - Ramsay-Générale de santé (RGdS) a fait l'objet depuis le 10 août d'une cyberattaque qui touche ses 120 établissements de santé en France, a appris APMnews (site du groupe APM International dont fait partie TICsanté), auprès du groupe de cliniques.

## Protonmail : face aux cybercriminels, la vantardise n'est pas une bonne tactique



**Sécurité** - L'éditeur de la messagerie sécurisée est victime d'attaques DDoS depuis maintenant deux jours. Si dans un premier temps, la société a rejeté la faute sur « un groupe russe », le site Bleeping Computer affirme que la raison de l'attaque est bien différente : il s'agit en réalité d'un groupe de cybercriminels vexés par les fanfaronnades du CTO de Protonmail sur Twitter.

Vendredi 29 Juin 2018 par Louis Adam

6 commentaires

## Piratage Facebook: 29 millions de comptes compromis

Par L'ESPRESSO avec AFP  
publié le 12/02/2018 à 19:50 - mis à jour à 19:53



## Attaque Windows : un client BitTorrent infecté déclenche l'épidémie Dofail



**Sécurité** - Les attaquants ont utilisé un client BitTorrent populaire pour diffuser des logiciels malveillants de cryptomining auprès de plus de 400.000 PC en l'espace de quelques heures.

Jeudi 15 Mars 2018 par Liam Tung

Réagissez !

## Ukraine : le malware VPNFilter utilisé pour s'attaquer à une usine de filtrage d'eau



**Sécurité** - Les services secrets ukrainiens annoncent avoir détecté et bloqué une infection par le malware VPNFilter, qui visait une usine de traitement de l'eau basée en Ukraine. Le renseignement ukrainien accuse la Russie d'être derrière cette opération.

Vendredi 13 Juillet 2018 par Louis Adam

1 commentaire

## 1,2 milliard de dollars de cryptomonnaie volés depuis 2017



**Sécurité** - La valeur des cryptomonnaies s'est envolée en 2017, suscitant l'intérêt des cybercriminels et soulignant le manque de sécurité de nombreuses entreprises engagées dans ce secteur. Résultat : les vols se multiplient et les pertes se creusent.

Vendredi 25 Mai 2018 par La rédaction de ZDNet.fr

Réagissez !

ALGÉRIE 09/06/2018 02h:35 CET

## Des hackers chinois volent une masse de données secrètes de l'US Navy (média)

AFP

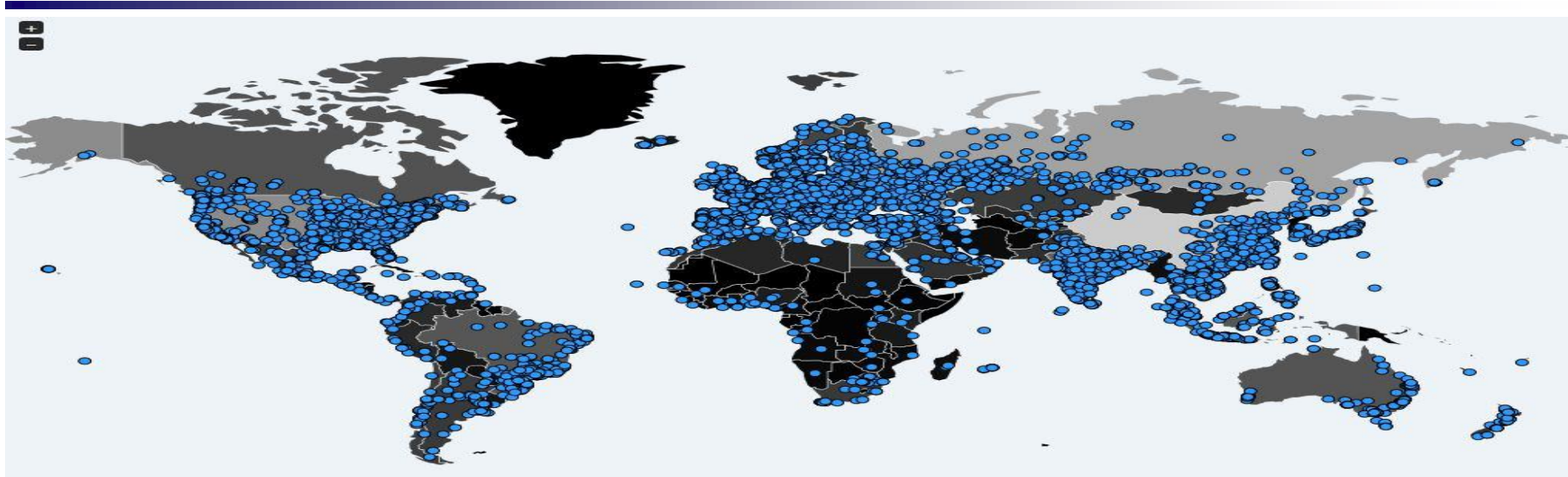
23 Mars 2021

Mairie de Signes

7



# WANACRY





# HAMECONNAGE & INGENIERIE SOCIALE

L'hameçonnage (anglais : « **phishing** ») constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire...

- 1 Réception d'un mail utilisant le logo et les couleurs de l'entreprise
- 2 Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe
- 3 Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant
- 4 Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site



## **Sur le plan opérationnel :**

- Perte de service
- Dégradation des performances

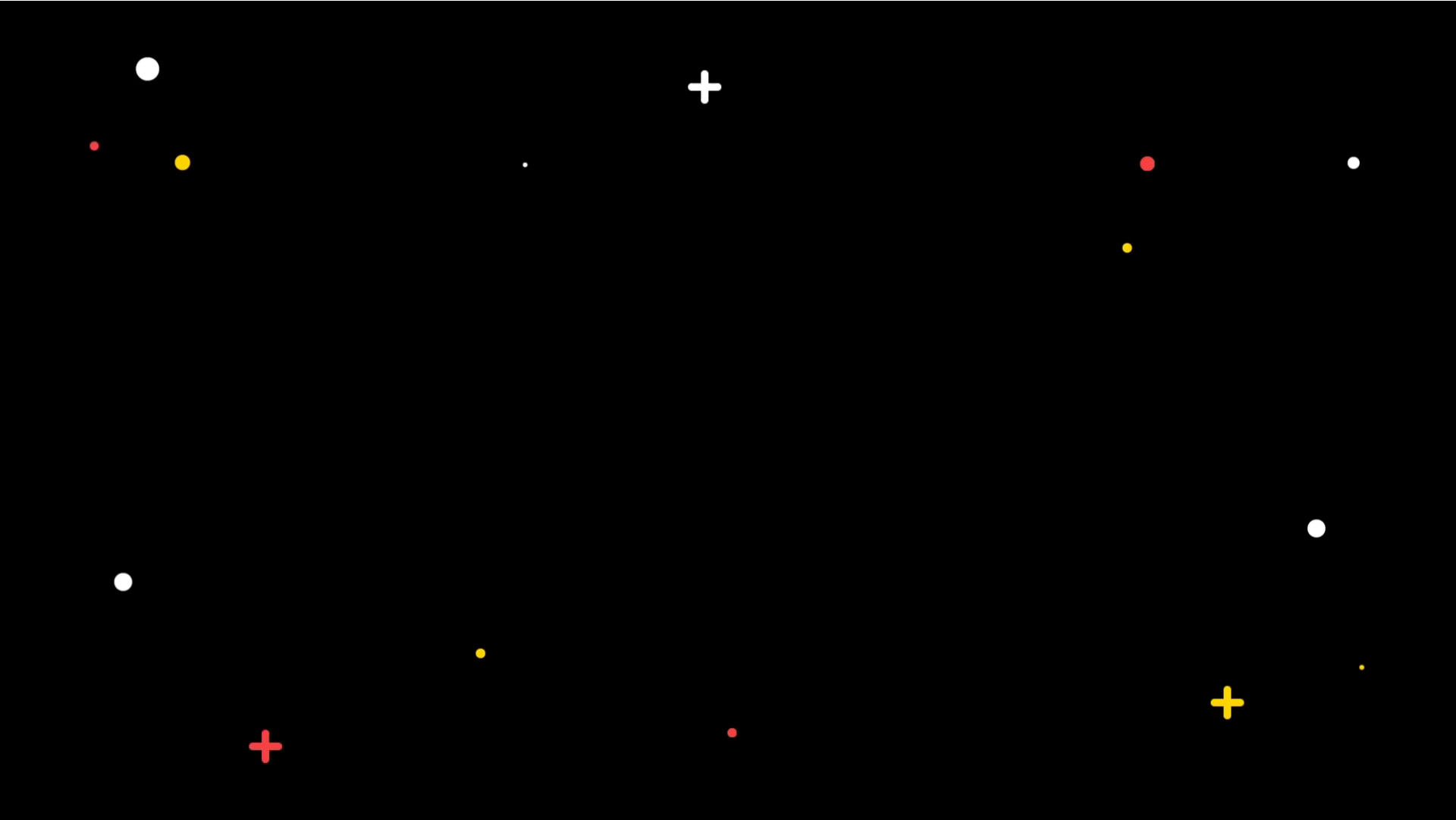
## **Sur le plan médiatique :**

- Image de la Mairie
- Désinformation

## **Sur le plan juridique :**

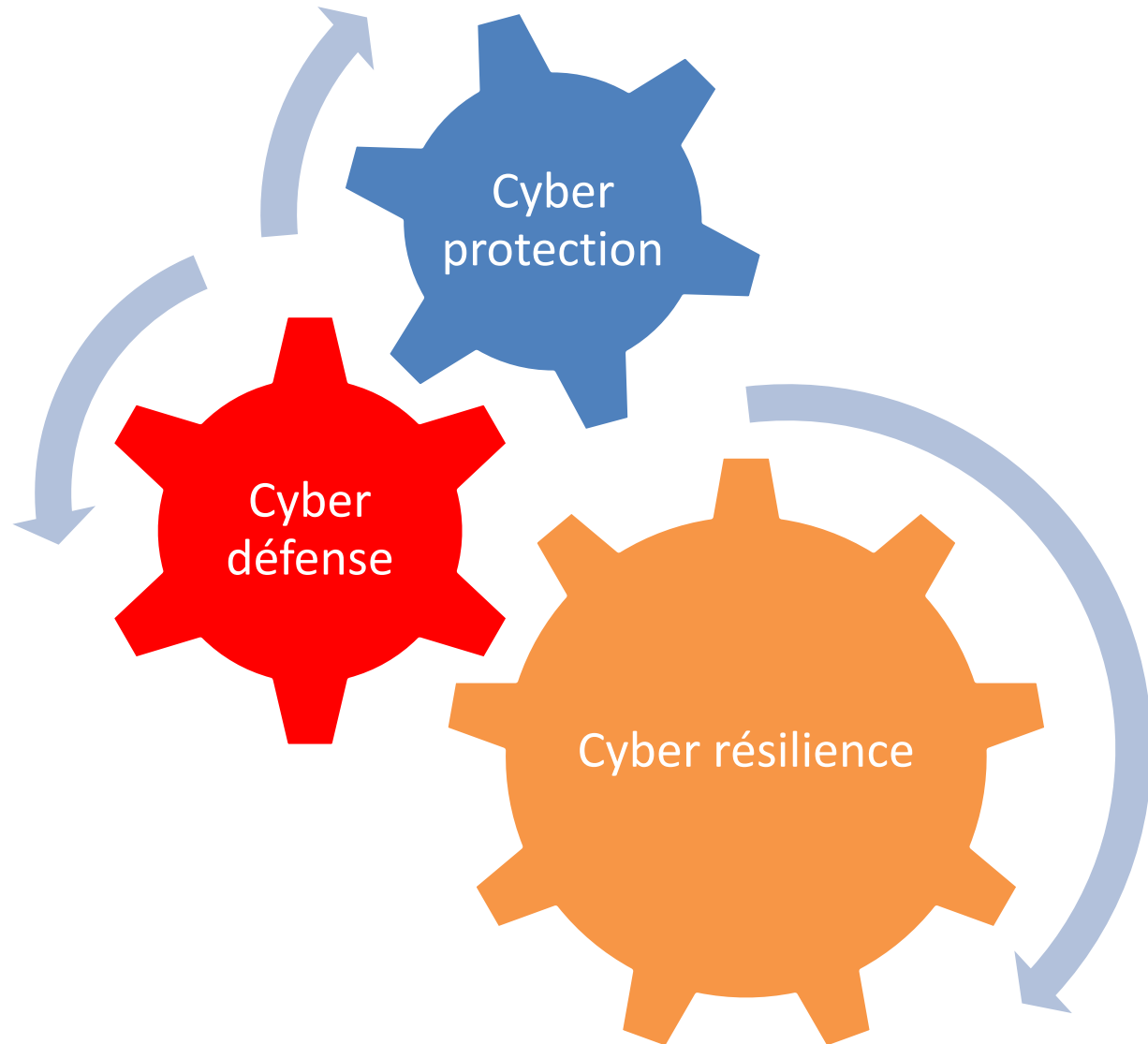
- Responsabilité civile
- Infractions pénales

# CYBER SECURITE





# CYBER SECURITE



**MAIRE DE SIGNES**

Responsable SSI



**Correspondant SSI**

M. ACHARD JACQUES



**Les utilisateurs**

# Responsabilité de l'utilisateur

---

Tout utilisateur est personnellement et légalement responsable de l'usage qu'il fait des ressources informatiques auxquelles il a accès. Il doit à son niveau contribuer à la sécurité générale de l'information de la mairie de Signes.

## **Tous les utilisateurs se doivent d'appliquer quelques règles fondamentales :**

- connaître et appliquer les consignes SSI ;
- connaître les règlements et procédures d'emploi de l'outil informatique ;
- rendre compte à la voie fonctionnelle SSI de toute anomalie constatée.



# Surfer sur la peur ??????



**Nous sommes tous vulnérables dès lors que nous sommes connectés (tablettes, téléphones, PC, montres, voitures, Smart TV, Cloud....objets connectés)**

**Il existe une parade simple :**

**Une bonne hygiène numérique et le respect de règles simples permettent d'éviter la plupart des attaques**

## Commandement N°1

Passez les supports amovibles par le sas antivirus ou le point d'insertion des données (PID) du réseau et ne connectez pas de supports personnels sur un ordinateur professionnel. (BYOD)



# Politique d'emploi des clés USB

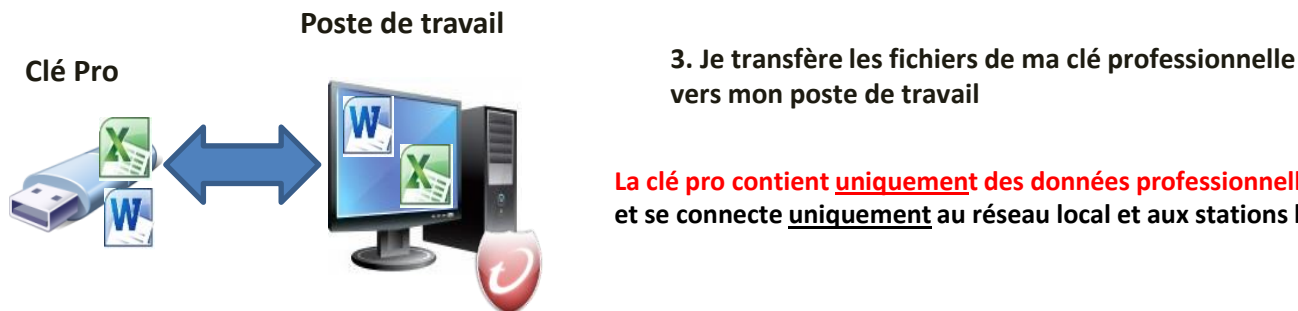
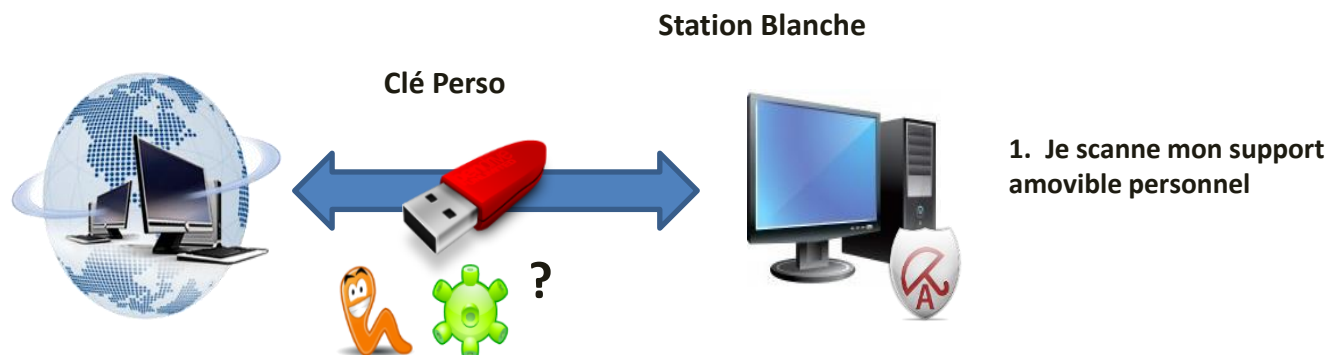
## Supports amovibles personnels :

➤ **Tolérés sur les Systèmes de la mairie à condition d'être sassy**





# Procédure d'import de données par clé USB



**La clé pro contient uniquement des données professionnelles (pas de keygen, crack, ...)**  
et se connecte uniquement au réseau local et aux stations blanches

## Commandement N°2

Effacez tous les données sensibles inutiles de vos clés USB.

**La clé USB n'est pas un outil de stockage, mais de transfert.**

## Commandement N°3

Informez immédiatement de toute détection de virus informatique votre correspondant SSI qui contactera les organismes compétents et vous guidera dans les actions à mener.



## Commandement N°4

Naviguez prudemment sur Internet.

**Il existe plusieurs risques potentiels liés à la navigation et la publication de données personnelles sur internet :**

- **Les sites internet pirates imitant des sites officiels**
- **Les sites internet défacés**
- **Les réseaux sociaux**
- **Téléchargement illégal**



## Commandement N°5

Utilisez des mots de passe véritablement robustes et secrets, ne les laissez pas accessibles.

UN MOT DE PASSE  
C'EST COMME UN **SLIP**.

Ça ne se donne pas à un inconnu.  
Ça se change régulièrement.  
Ça ne se laisse pas au bureau.



PASSWORD | ★★★★★★★★

Face à la cybercriminalité,  
adoptez les **bons réflexes**.

cybermalveillance.gouv.fr

**escrim**  
INFORMATIQUE & RESEAUX

# C'est quoi un bon mot de passe ?

mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire

La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » :

**ght5CDs%E7am**

La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » :

**aE2IP,IJ2Géa!**

Le mot de passe est **unique** pour chaque service  
**margarettatcheris110%SEXY** (Edward Snowden)

Possibilité de stockage des mots de passe :

- Logiciel VERACRYPT (fichier TXT chiffré)
- Logiciel Keepass

## Commandement N°6

Verrouillez votre session de travail lorsque vous quittez momentanément votre poste de travail.



① Je ferme ma session quand je quitte momentanément mon poste de travail

**Afin d'éviter les accès et les actions non désirés.**

## Commandement N°7

Ne communiquez votre adresse mail professionnelle qu'à des personnes de confiance.





## Commandement N°8

Soyez vigilant avec les mails que vous recevez. Vérifiez l'expéditeur, cliquez avec prudence sur les liens et ouvrez avec discernement les pièces jointes.

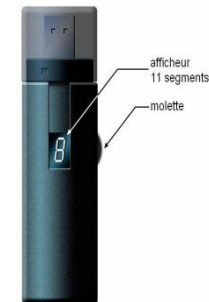


② Je suis vigilant sur l'objet et l'expéditeur des mails que je reçois



## Commandement N°9

Adaptez les moyens de transmission en fonction de la sensibilité des informations.



# Commandement N°10

Ne cherchez pas à contourner la politique de sécurité.

Ne pas importer de fichiers « illégaux » jeux (format Excel par exemple..)  
L'utilisation d'applications portables est interdite sur les réseaux du Ministère

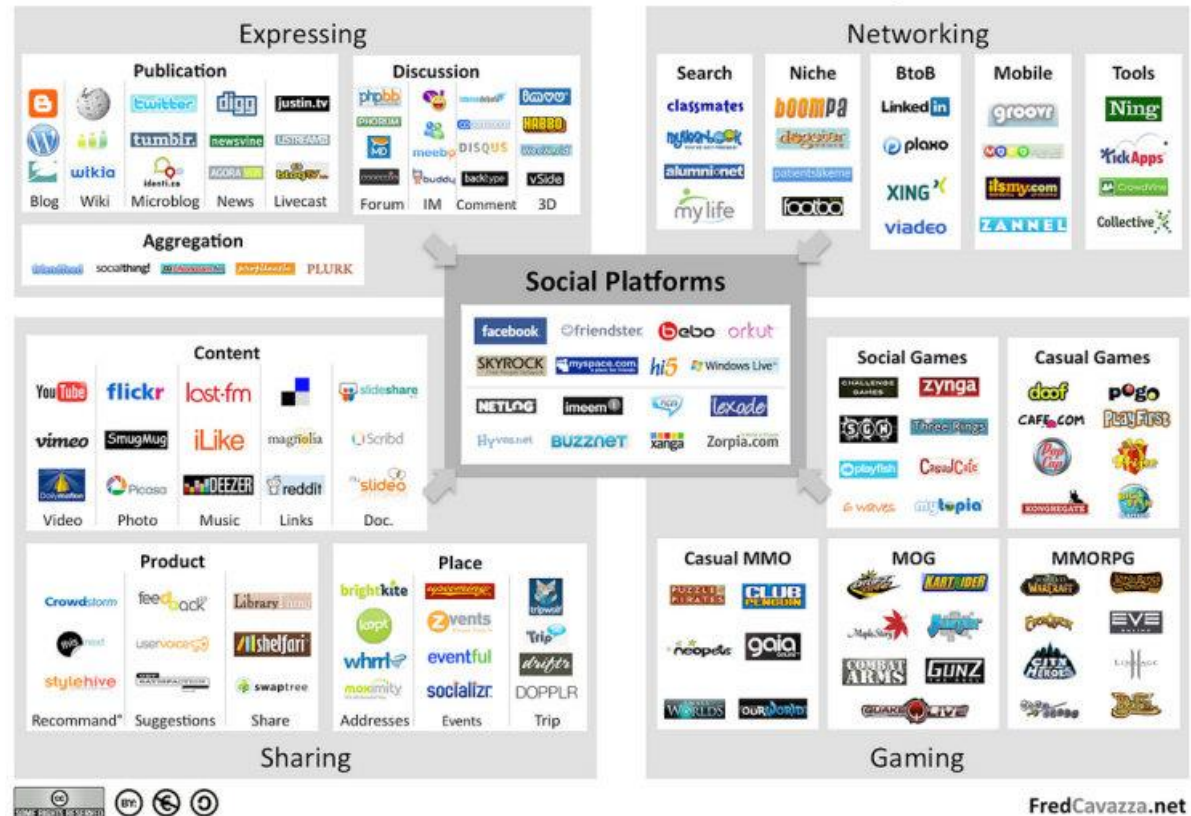
# Les réseaux sociaux



- Ne pas divulguer de données précises
- Respecter les règles relatives au RGPD et à la charte informatique
- Ne pas porter atteinte à l'image d'une personne
- Respecter les droits des personnes sur leur image
- Rester vigilant quant aux informations mises en ligne
- Tout ce que vous publiez, partagez sera difficile à effacer : **l'oubli numérique n'existe pas.**

# Cartographie de l'identité numérique

## Social Media Landscape



Chantage

Opération d'influence

Manipulation

Désinformation

Votre vie est disponible sur le WEB, et ces informations ne vous appartiennent plus.



# Questions

L'individu est au cœur de la cybersécurité

