# Poste de travail : les bonnes pratiques en sécurité

## I) Les modeles de menaces

### A) Les menaces chez les particuliers :

**Les espions (ou spywares) :**
Ce type de logiciel s'installe (à votre insu) dans un ordinateur dans le but de collecter et de transférer des informations personnelles. Ce type de virus est favorisé par l'essor d'Internet. Ils sont présents sur beaucoup de site internet.
Principal usage : Profilage des utilisateurs pour leur soumettre des publicités ciblées.

**Les chevaux de Troie (trojan) et keylogers :**
Nous en parlons dans les lignes ci-dessous

**Les vers (ou worms) :**
Ce type de logiciel utilise les différentes ressources du système et les connexions de l'ordinateur (réseau / internet) pour se propager et se reproduire.
Pour se propager, il utilise les failles des applications et des systèmes d'exploitations (d'où les mises à jour logicielles de sécurité)

En plus de son action principale : se propager , il abrite très souvent un code malveillant ayant pour but de nuire aux ressources des hôtes qu'il a infecté.
En passant du simple ralentissement à la paralysie de la machine ou/et du réseau informatique qu'il a infecté.

### B) Les menaces chez les professionnels :

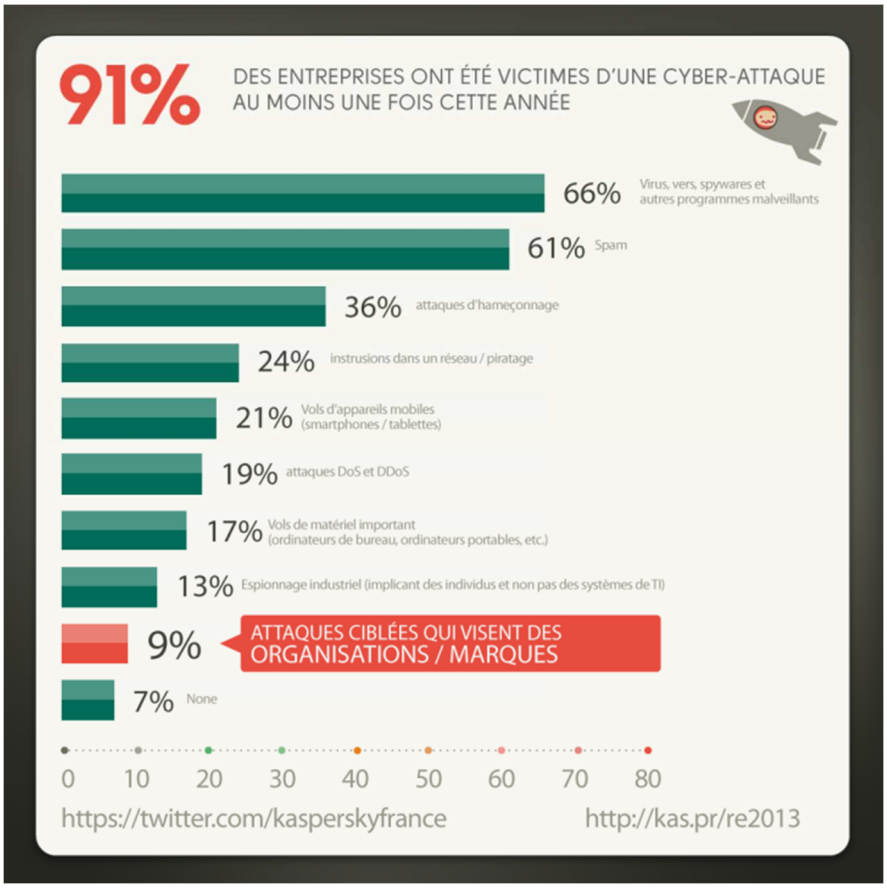
### C)

## Quels risques pour les données informatiques ?

Il existe différents types de risques pour les données d'une entreprise, les principaux sont :

- les virus et programmes malveillants,
- les emails frauduleux,
- le piratage,
- l'espionnage industriel,

- la perte d'information confidentielles,
- l'erreur de manipulation.




# II) Les outils malveillants

## Le phishing (ou hameçonnage)

Le phishing est une technique par laquelle des personnes malveillantes se font passer pour des entreprises ou des organismes financiers qui vous sont familiers en envoyant des courriels frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.

## Les logiciels malveillants

## (virus, chevaux de Troie, vers informatiques)

Les logiciels malveillants ont en commun la capacité d'exécuter une ou plusieurs des actions suivantes une fois qu'ils ont contaminé votre dispositif numérique :

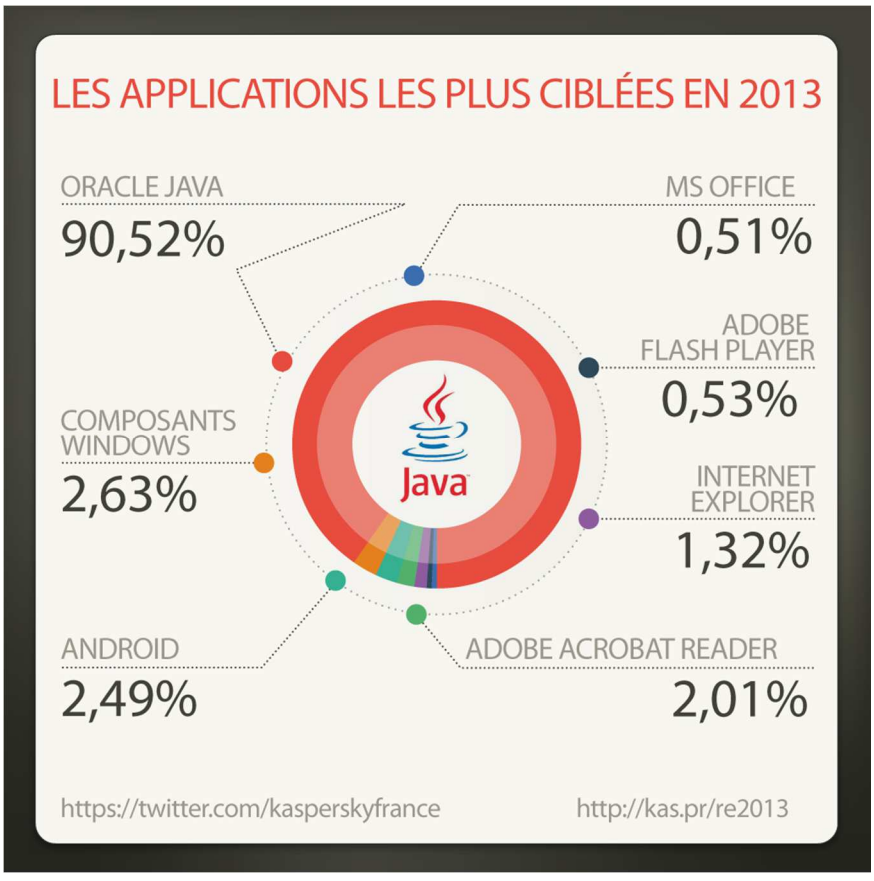
- Endommager votre système
- Prendre les commandes de votre ordinateur

- Changer le fonctionnement de votre système. Un type courant de logiciels malveillants modifie votre navigateur vous laissant voir du contenu Web modifié (notamment des bannières publicitaires différentes) ou vous dirige vers de faux sites Web dans le but de recueillir vos données personnelles. La modification du contenu Web peut être difficilement repérable car le nom du site reste inchangé (url).
- Récupérer vos données personnelles. Certains types de programmes malveillants peuvent lire les données stockées dans votre système ou saisies au clavier, dont vos renseignements financiers ou vos noms d'utilisateur et vos mots de passe, puis les transmettre à leur concepteur.

## Les attaques sur les mots de passe

Pour accéder à vos données personnelles et effectuer des opérations frauduleuses, les personnes malveillantes peuvent usurper votre identité en s'attaquant à vos mots de passe.
Plusieurs techniques sont connues :

- des logiciels permettent de générer tous les mots de passe possibles
- d'autres utilisent des mots issus de liste, notamment ceux du dictionnaire.
- Une autre méthode consiste simplement à deviner le mot de passe, en fonction d'éléments que l'attaquant aura pu obtenir sur le propriétaire du mot de passe et de ses proches (nom, prénom, date de naissance…).



# III) La prévention

## Comment se protéger ?

## Contre le phising :

Les banques et organismes sociaux (CAF, mutuelles, etc.) ou les entreprises commerciales **ne demandent jamais à leurs clients de venir saisir leurs informations personnelles dans un courrier électronique**.

Pour se connecter au site de sa banque il vaut mieux **entrer manuellement l'adresse réticulaire (URL) du site dans votre navigateur.**

**Préférez saisir des informations personnelles (coordonnées bancaires, identifiants…) sur des sites internet sécurisés** : un cadenas apparaît dans le navigateur et l'adresse du site commence par HTTPS au lieu de HTTP.

**Ne cliquez pas sur les liens contenus dans les courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.

Méfiez-vous des pages internet suspectes de validation d'opérations sensibles ou d'une lenteur inhabituelle de vos outils internet.

**En cas de doute ou de problème, prenez contact rapidement avec votre agence bancaire ou l'organisme qui aurait envoyé ce courriel.**

## Contre les logiciels malveillants :

Il est préférable de **ne jamais télécharger un fichier à moins d'avoir la certitude de sa légitimité et de celle de sa source**. Lorsque vous téléchargez des fichiers, vous permettez à un autre ordinateur de sauvegarder quelque chose sur votre disque dur. Cela peut permettre l'installation d'un logiciel malveillant sur votre poste de travail, logiciel qui peut ne pas être détecté par des antivirus à jour, dans le cas où il s'agit d'une variante récente.

**Il ne faut jamais ouvrir une pièce jointe sans que l'expéditeur ait confirmé son intention de vous l'envoyer** car elle peut contenir un logiciel malveillant.

**Avant de cliquer sur un lien, laissez-y votre curseur pendant un instant pour vous assurer que l'adresse URL (adresse Web) qui s'affiche y correspond**. Car même si vous ne visitez pas de sites malveillants intentionnellement, cliquer sur le mauvais lien peut vous y conduire.

**Il est également important d'équiper son poste de travail d'un anti-virus et d'un pare-feu et de mettre régulièrement ses logiciels à jour**.

## Contre les attaques sur les mots de passe :

**Plus il y a de caractères et plus leur espace de départ (types de caractères) est grand, plus ces types d'attaques mettront du temps à aboutir** : un mot de passe long (8 à 12 caractères de préférence) utilisant des types de caractères différents ne peut ainsi être trouvé en un temps raisonnable par un attaquant ayant des moyens conventionnels.

**Le choix d’un mot de passe ne faisant aucune référence à un mot connu du dictionnaire ou à des références personnelles** rendra les attaques plus complexes.