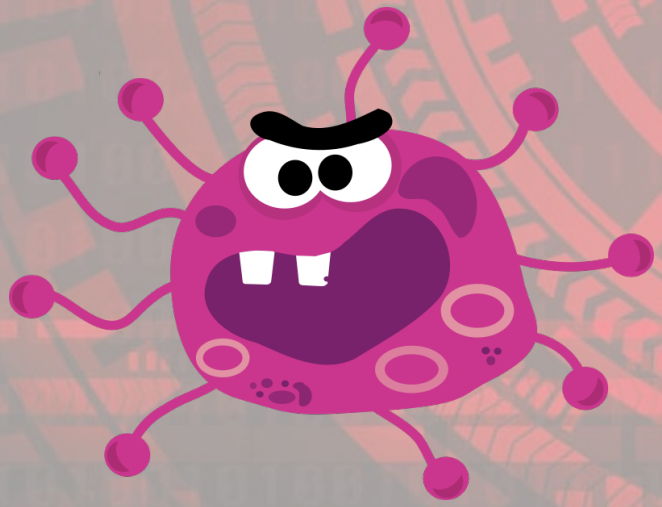
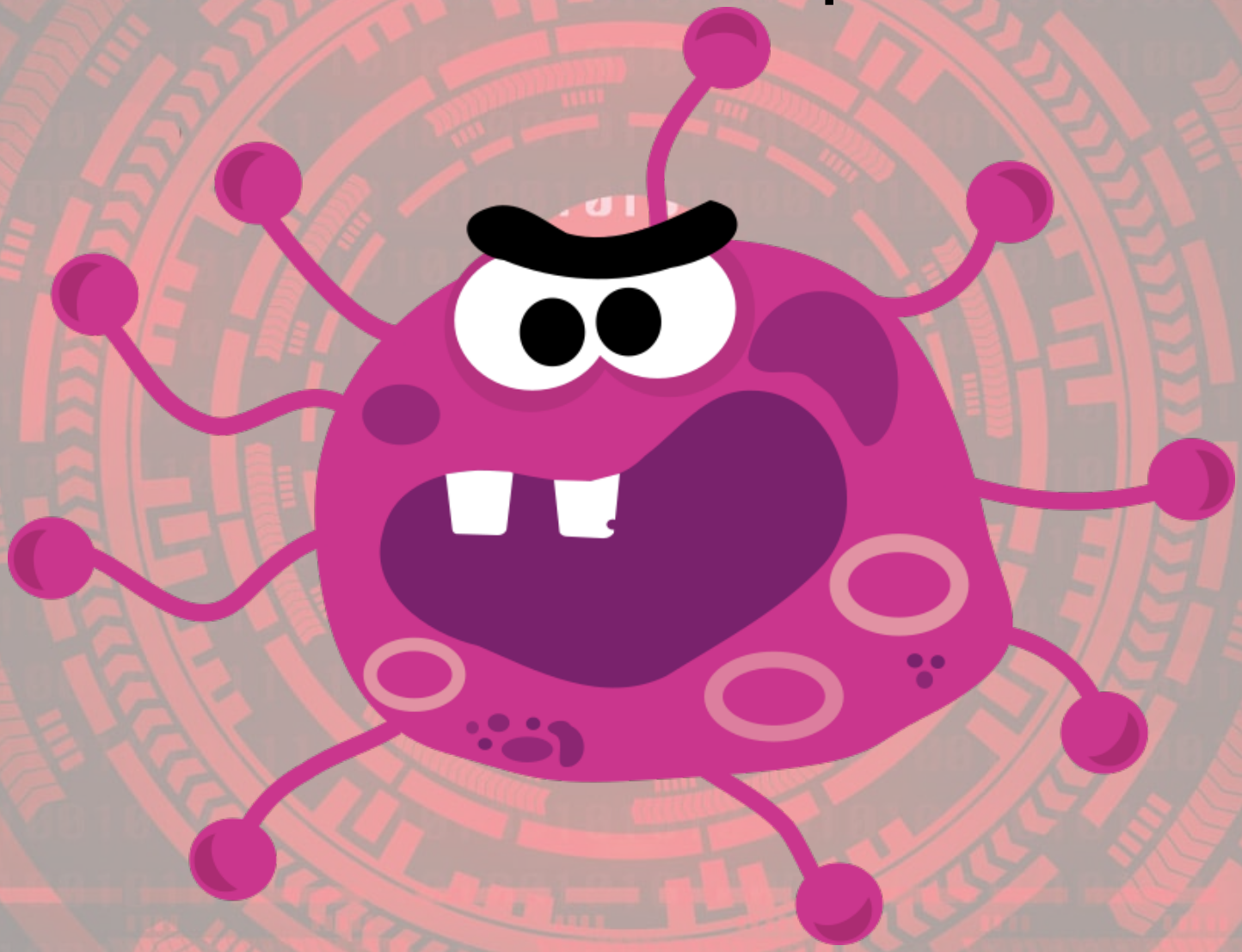
Apprendre à reconnaître les arnaques sur Internet

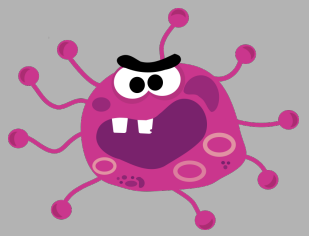


Djan GICQUEL

Logiciels malveillants
Les classiques



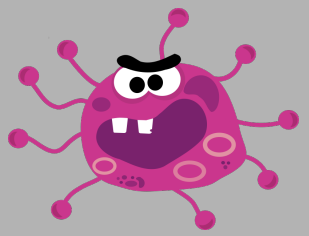
Virus



Définition : S'infiltre dans le système via un hôte qu'il parasite

S'en prémunir : Ne télécharger que des logiciels de confiance, ne pas ouvrir de pièce jointe d'expéditeur inconnu, garder son système à jour, utiliser un antivirus et le garder à jour

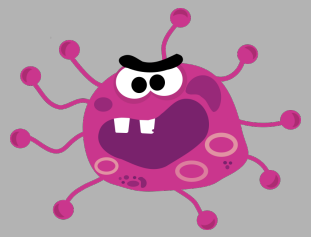
Ver



Définition : Se réplique de machines en machines pour saturer les réseau et les cycles de processeur

S'en prémunir : Ne télécharger que des logiciels de confiance, ne pas ouvrir de pièce jointe d'expéditeur inconnu, garder son système à jour, utiliser un antivirus et le garder à jour

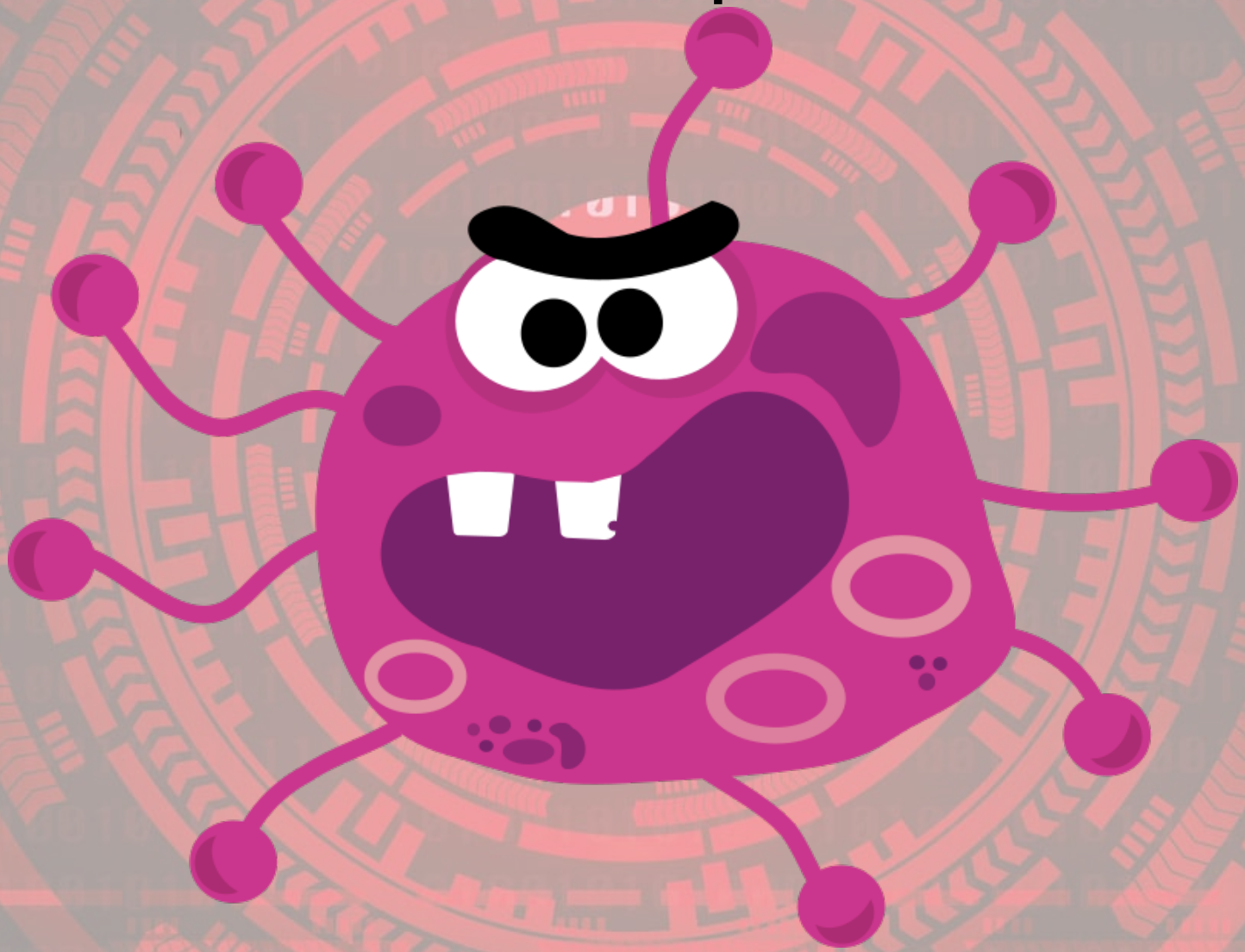
Trojan



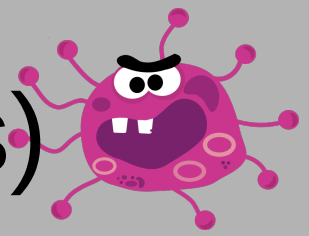
Définition : Reste en sommeil et attends un déclencheur distant ou une date précise

S'en prémunir : Ne télécharger que des logiciels de confiance, ne pas ouvrir de pièce jointe d'expéditeur inconnu, garder son système à jour, utiliser un antivirus et le garder à jour, utiliser un pare-feu

Logiciels malveillants
Les contemporains



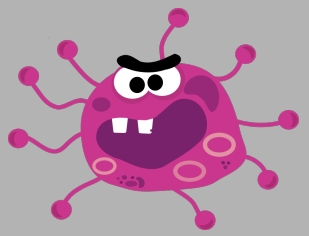
Adwares (logiciels publicitaires)

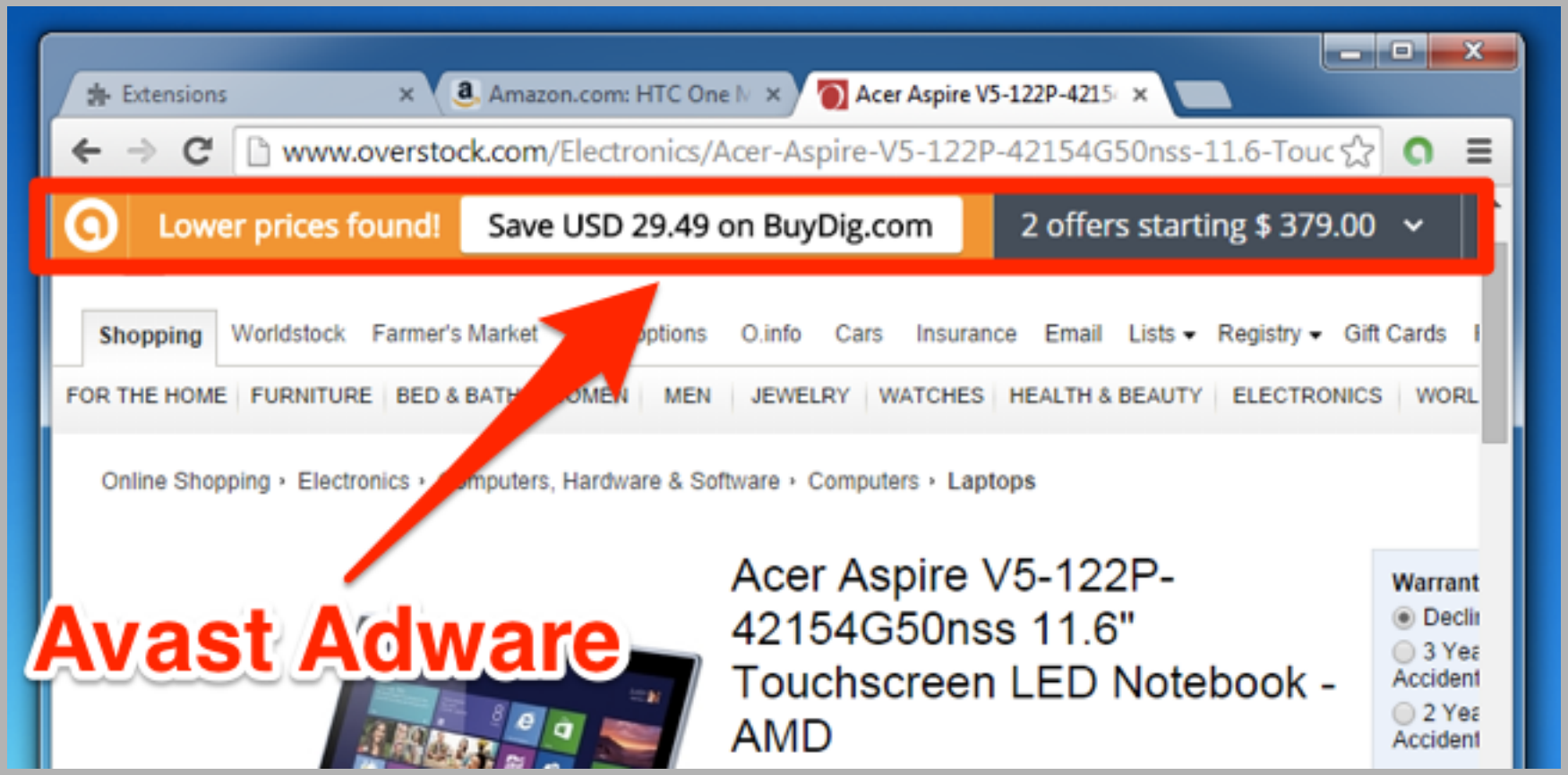


Définition : programme publicitaire qui utilise le processeur, la bande passante et ralenti l'OS

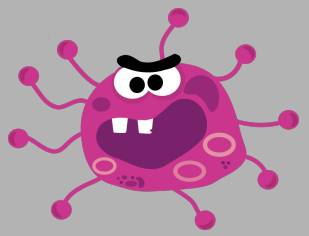
S’en prémunir : Ne pas télécharger sur les sites grand publics (01net, clubic, softonic…) et télécharger uniquement depuis des sites de confiance, utiliser des logiciels libres, utiliser un navigateur libre (Mozilla Firefox) et n’installer que des extensions de confiance

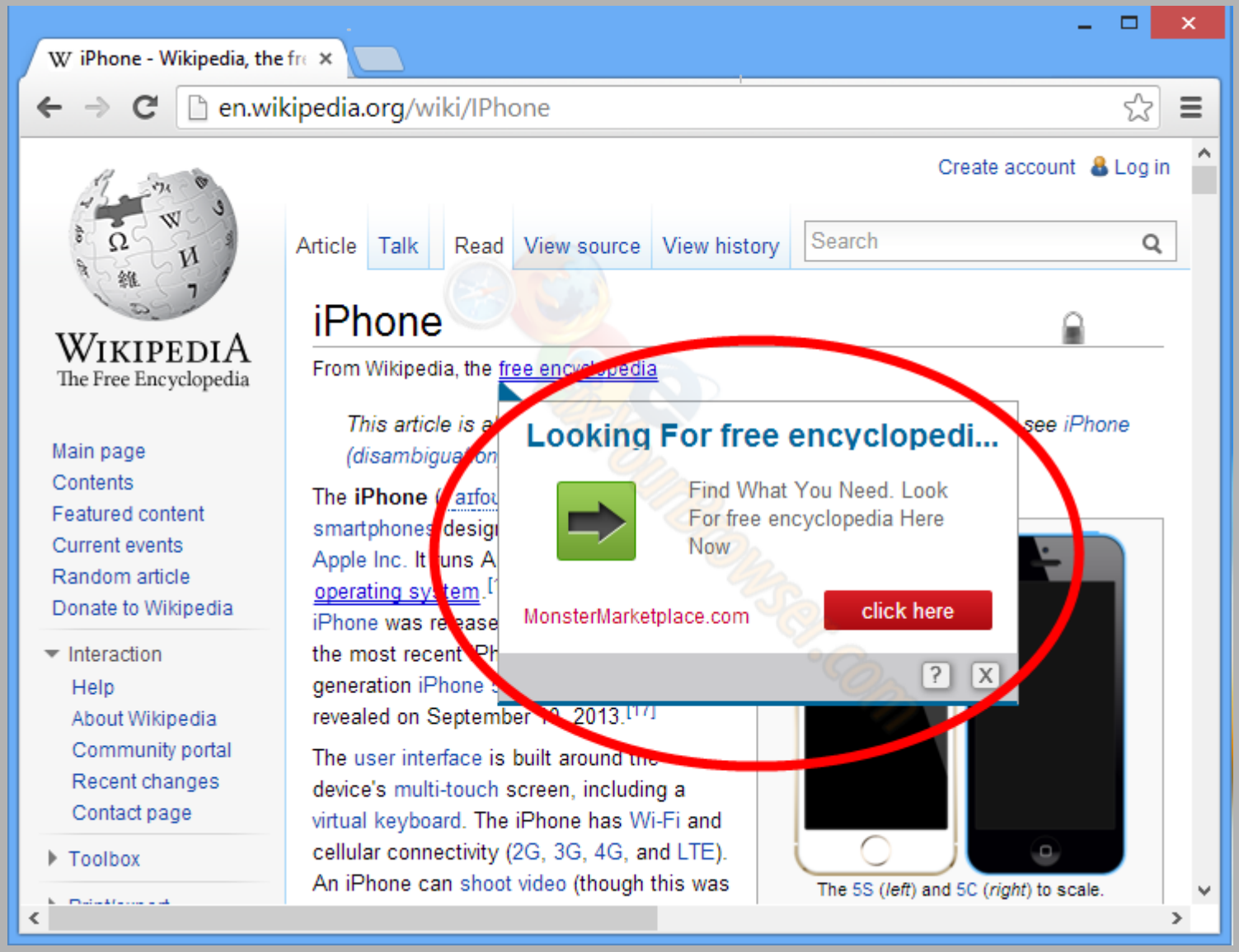
Exemple Adwares



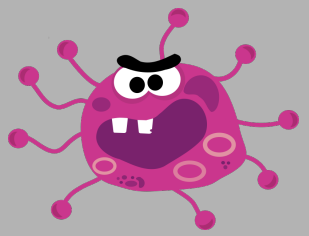


Exemple Adwares





Cryptolockers/Ransomwares

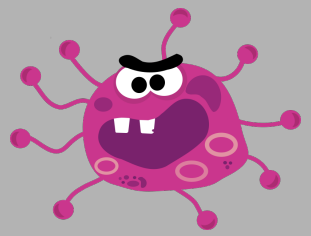


Définition : chiffre les fichiers du disque dur et demande une rançon conséquente pour les libérer

S’en prémunir : sauvegarder régulièrement ses données, utiliser un antivirus, faire les mise à jours de sécurité de son système

Exemple cryptolocker/ransomware

Bloatwares/Crapwares

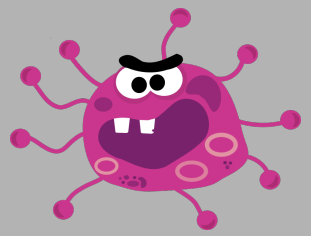


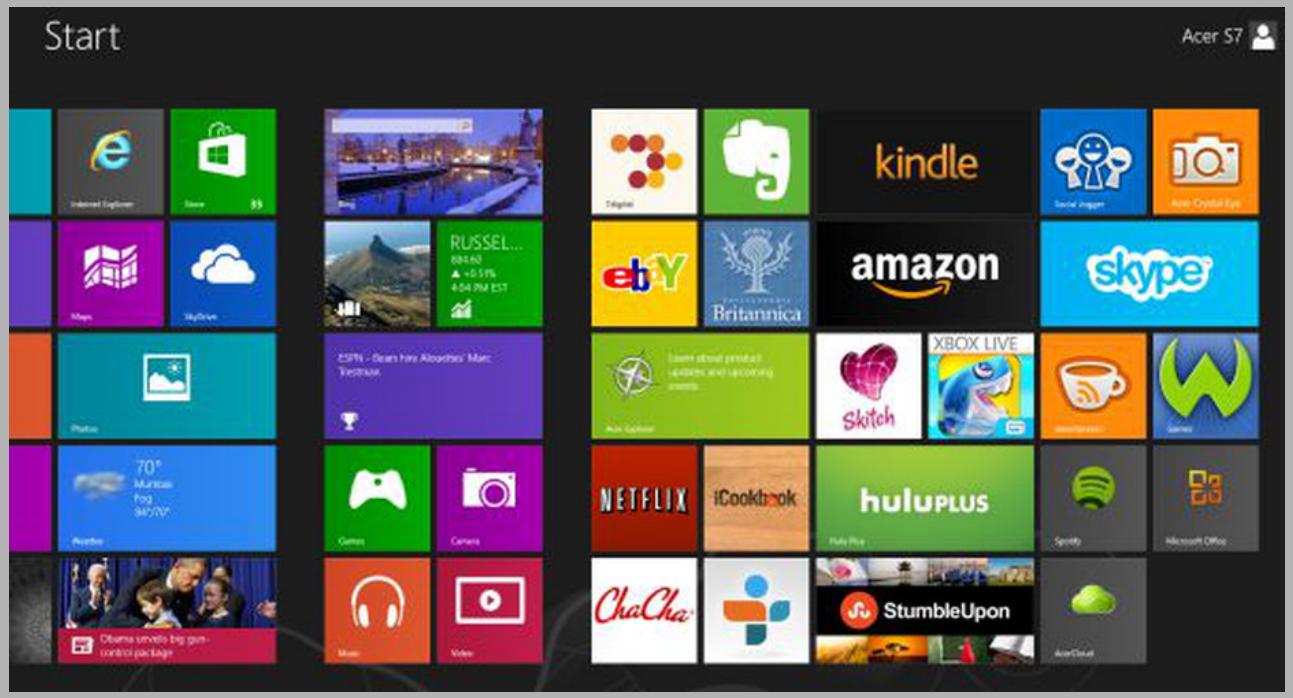
Définition : Logiciels préinstallés par le constructeur et totalement inutiles qui consomme de l'espace disque et des cycles processeurs

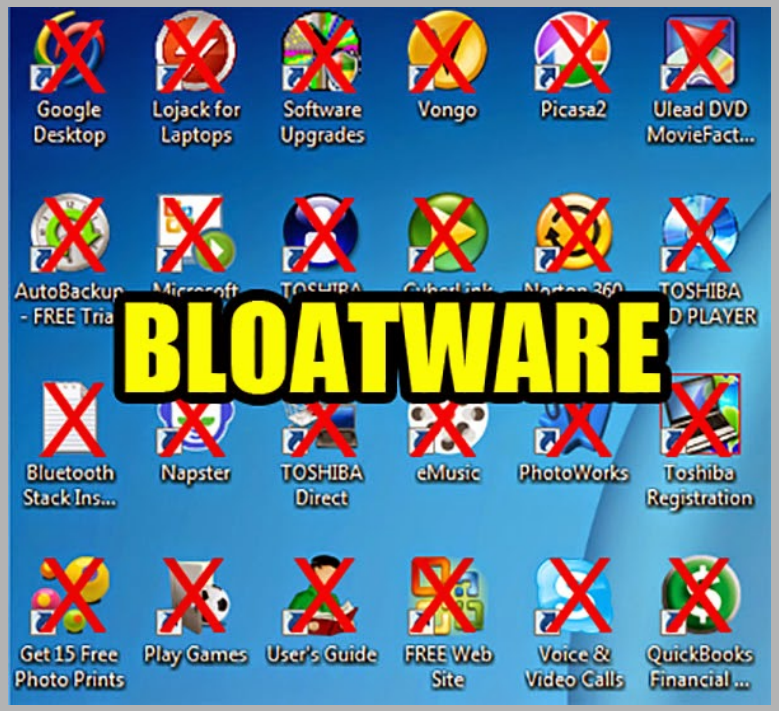
S’en prémunir : Lors de l’achat d’un ordinateur, formater le disque dur, faire une installation propre de Windows. Si ce n’est pas possible supprimer à la main les logiciels constructeurs.

Vérifier sur shouldiremoveit

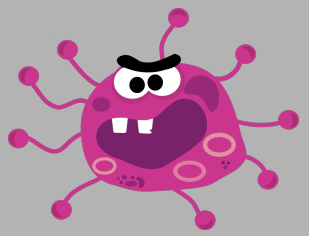
Exemple bloatwares







Les contemporains (suite)



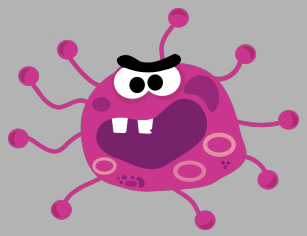
System Booster

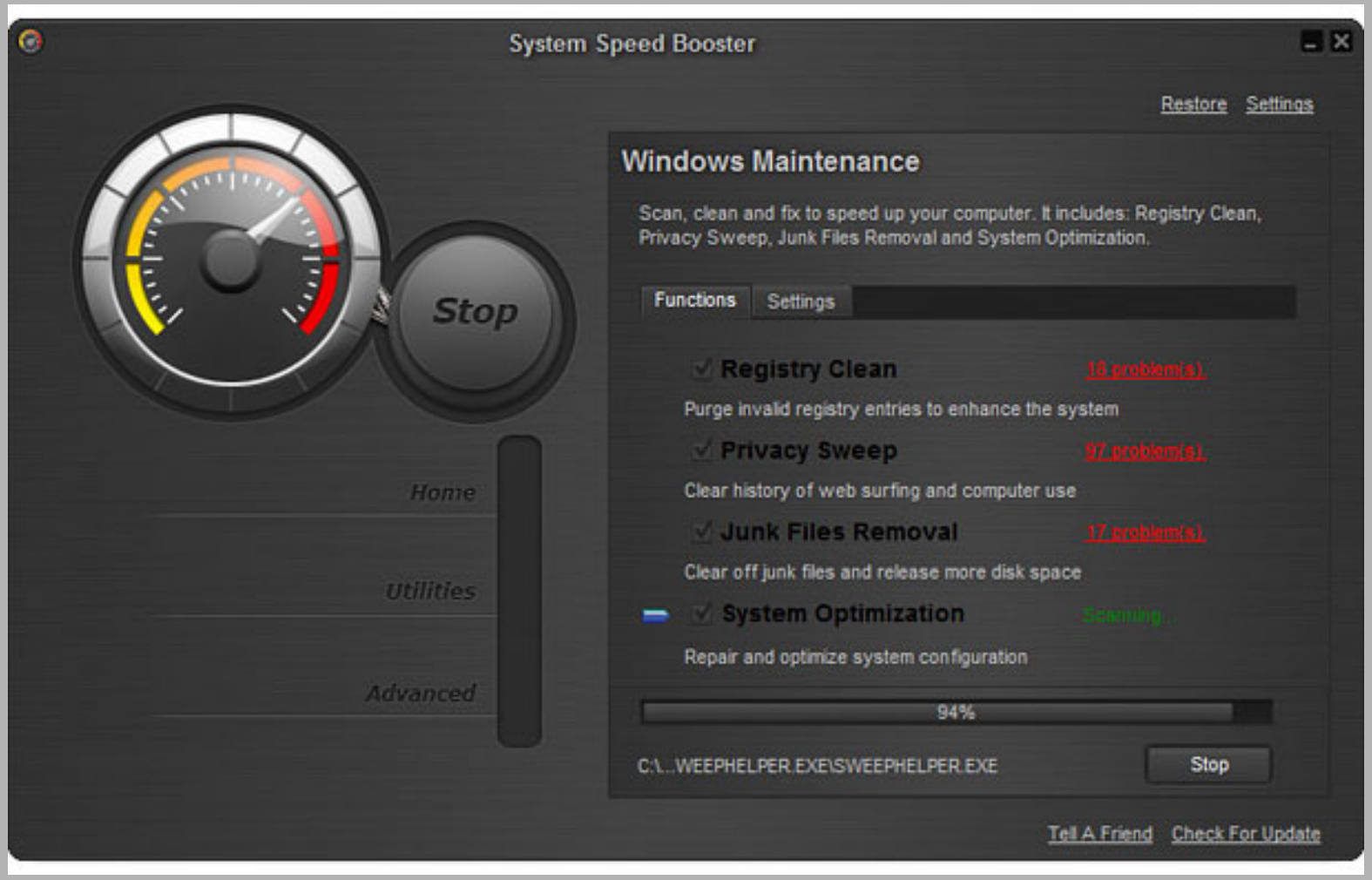
Un encart dans une page web prétendant que votre système est lent et qu’il faut le nettoyer.

Explication : En fait ce logiciel va ralentir le système et installer des publicités

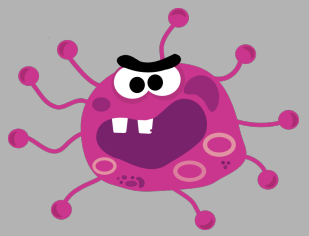
Action à réaliser : N’installer que des logiciels de confiance

Exemple system boosters





Les contemporains (suite)



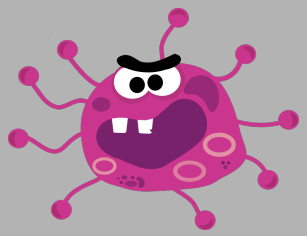
Faux anti-virus

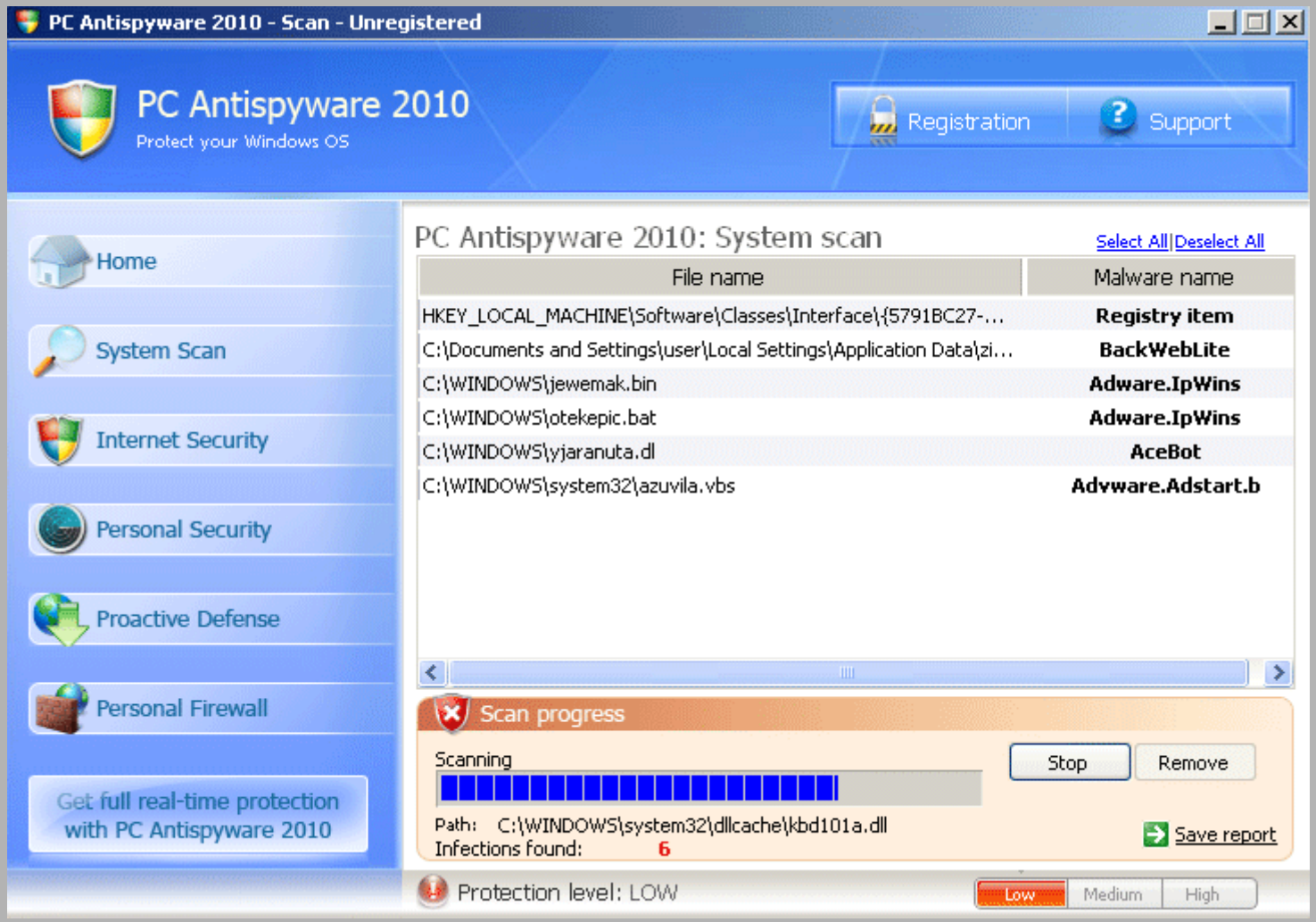
Un encart dans une page web prétendant que votre système est vérolé et qu’il faut le désinfecter

Explication : Lorsque vous cliquez sur le lien vous téléchargez un virus sur votre ordinateur

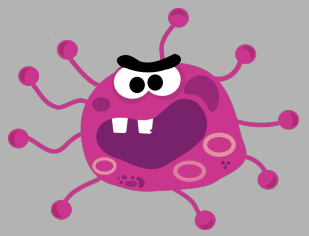
Action à réaliser : Ne pas télécharger ce logiciel, utiliser un bloqueur de publicité et ne pas télécharger de logiciels de sources inconnues ou douteuses

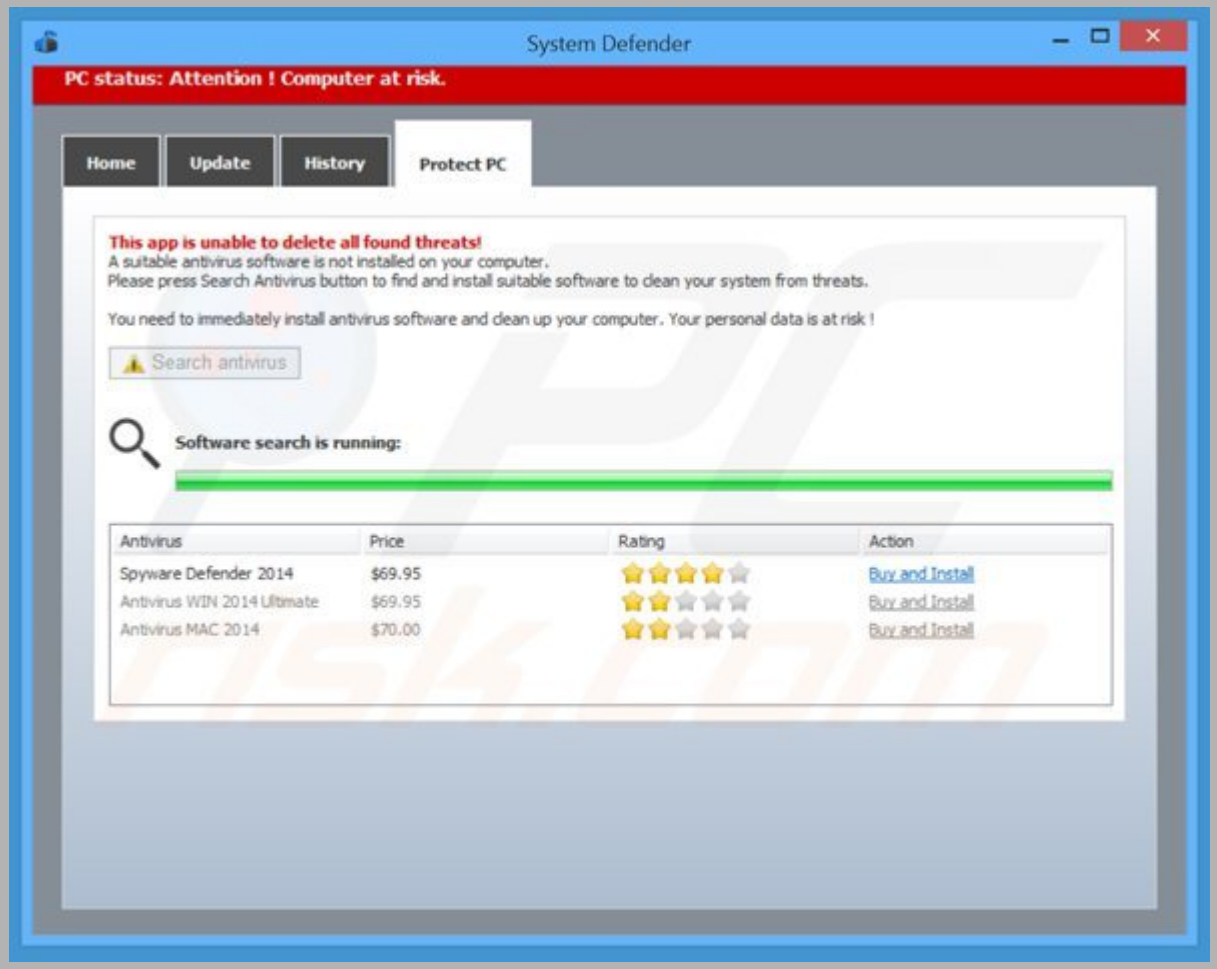
Exemple faux antivirus



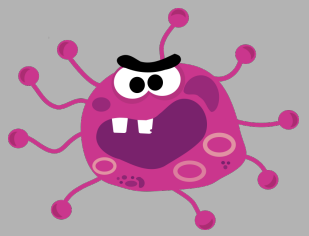


Exemple faux antivirus





Les contemporains (suite)



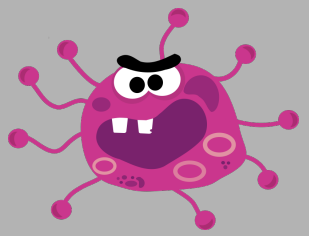
«Optimiseurs» de batteries

Dans les stores sur les smartphones on trouve de nombreuses applications qui promettent d’optimiser le système et d’économiser la batterie

Explication : Ce sont en fait des logiciels publicitaires qui vont drainer la batterie en se connectant en permanence à internet

Action à réaliser : Ne pas télécharger ces logiciels, couper les fonctions sans fil (wifi, connexion mobile, GPS, bluetooth) lorsqu’elle ne sont pas utilisés

«Optimiseurs» de batteries



Pratiques malveillantes

Par courriel

Fausses loteries (plus rare)
Vous recevez un courriel qui explique que vous avez gagné à la loterie Microsoft
Action à réaliser : supprimer immédiatement l’émail sans le lire

SPAM
Vous recevez une newsletter à laquelle vous ne vous êtes jamais inscrit
Action à réaliser : Supprimer le mail sans le lire et le classer en courrier indésirable dans votre messagerie. Ne pas cliquer sur les liens.

SCAM / Phishing
Courriel d’une personne prétendant être riche héritière et avoir besoin de quelqu’un pour transférer une grosse somme d’argent
Action à réaliser : Supprimer le courriel dès réception ou le classer en indésirable

Protection SSL

Les antivirus moderne intègre parfois une fonction appelée «protection SSL» ou «interception SSL».

Explication : Cela casse la sécurité du modèle https basé sur la confiance des certificats. C’est une attaque homme du milieu où l’éditeur de l’antivirus peut voir les informations échangés de manière sécurisés de même qu’un attaquant.

Action à réaliser : Ne pas utiliser ces fonction et désinstaller si possible les antivirus qui intègre ces fonctionnalités, faire vérifier les certificats système par un professionnel

Piratage de comptes

Un pirate réussit à rentrer dans une base de données d’un serveur et à en extraire des informations privées (identifiant, mot de passes, codes de CB…)

S’en prémunir : Ça ne dépend pas de vous !

Action à réaliser : Utiliser de «bons mots de passes» ou mieux un gestionnaire de mot de passe

Fichier vidéo : Campagne Hack Academy JENNY

Arnaque par sms

Alerte SFR: Une e-sim a été commandée sur votre espace client. S'il ne s'agit pas de vous, merci de vous rendre sur : https://sfr-esim.contact/

Crit'Air :
Nos agents ont constaté que votre véhicule n'était pas muni de la vignette règlementaire Crit'Air 2022
veuillez la récupérer sous peine de contravention dans les prochaines 48 h
sur le lien ci-joint :

https://critair-support.fr

Votre solde pour la formation arrive à échéance. Consultez votre solde et réclamez votre formation 100% financée par l'état sur: https://1cpf.com
STOP au 36100

Assurance-Maladie : Expiration de votre carte vitale, un agissement de votre part est requis. Cliquez ci-dessous: http://ameli-assurance.app

Arnaque par sms

Info ANTAI :

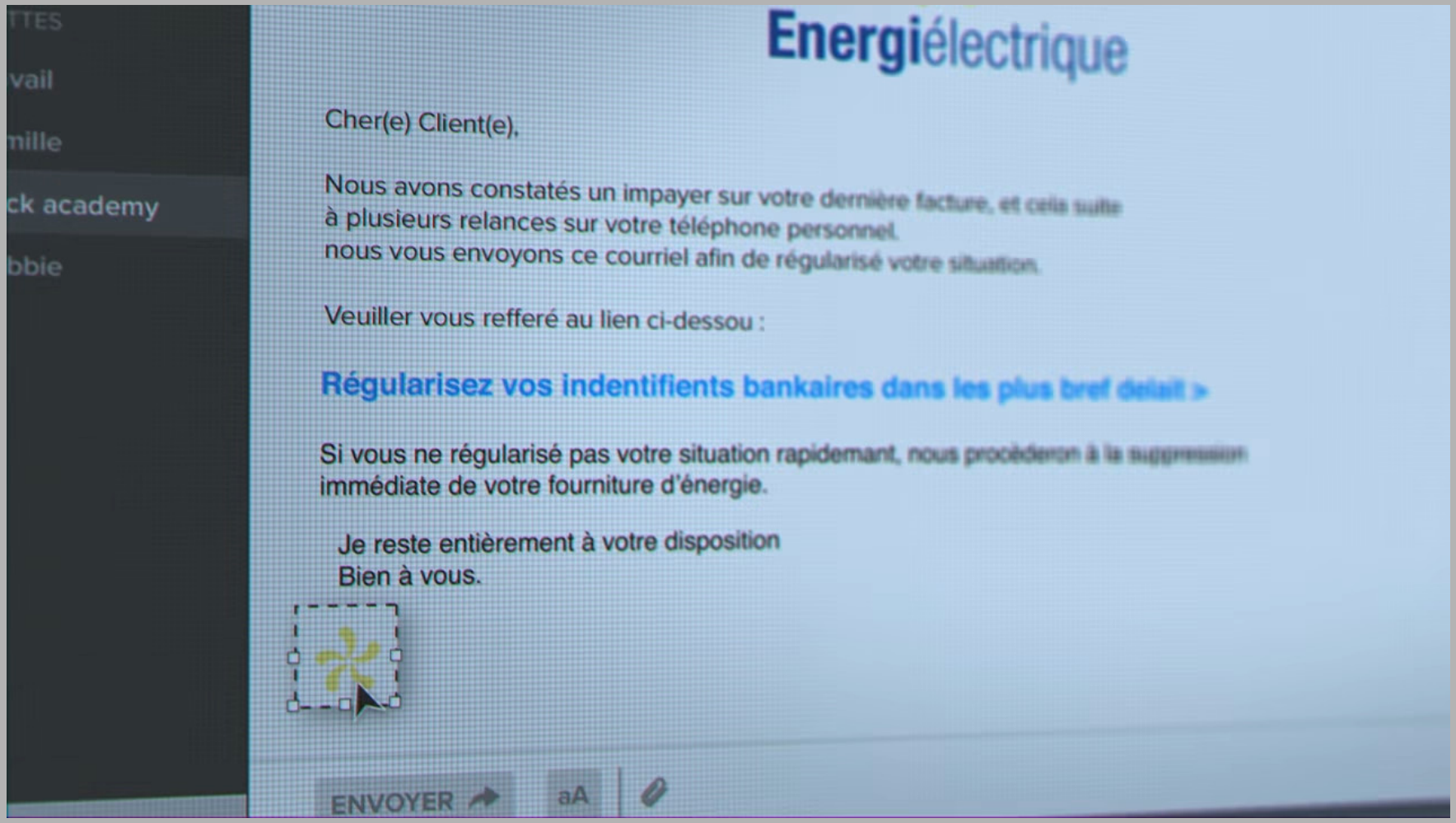
Vous avez un retard de paiement de 35,00€

Dossier référence 20753099. Consulter mon dossier d'infraction via :

https://paie-suivis.info

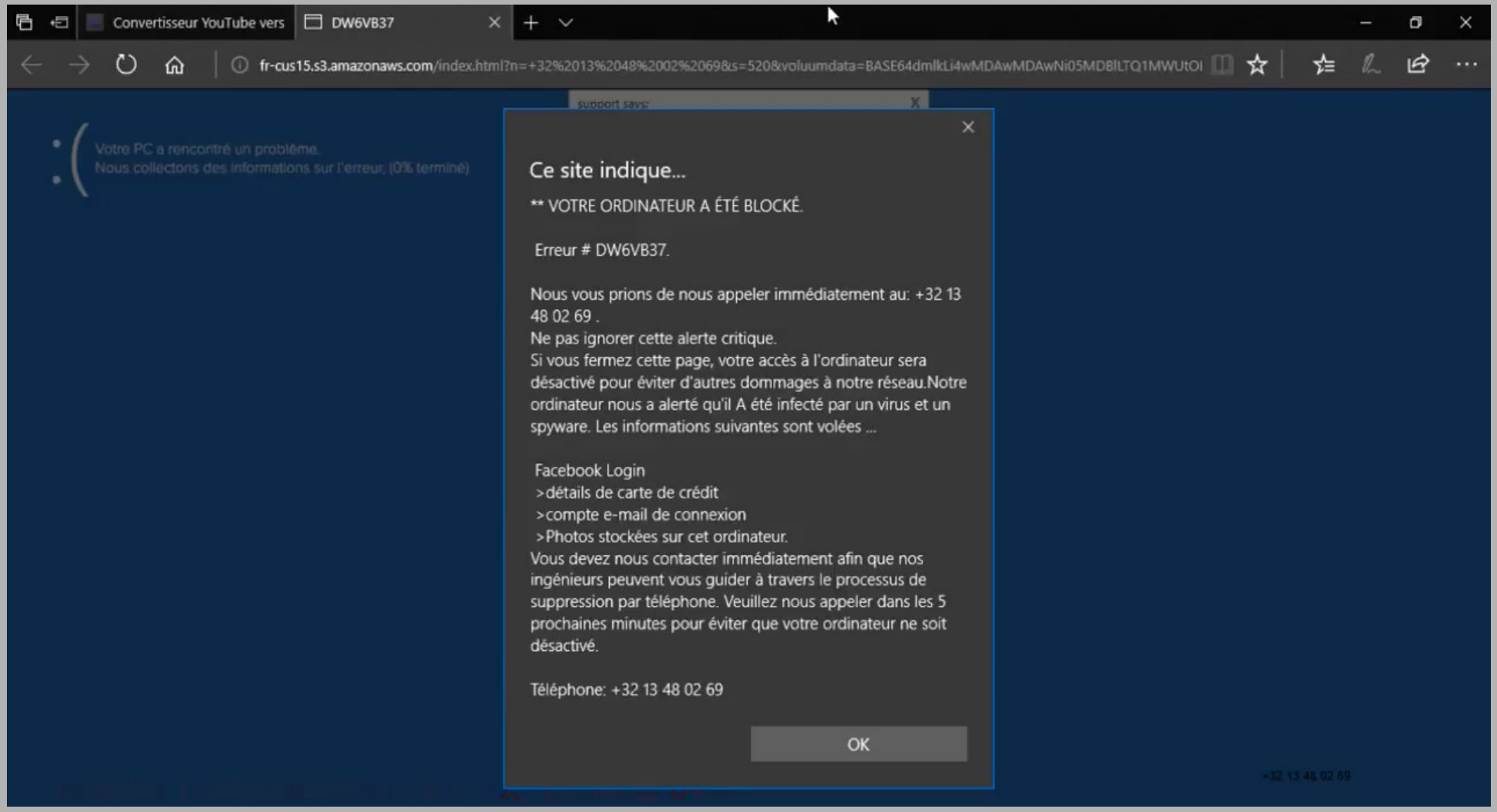
EDF : Votre dernière facture a été refusée par votre banque. Veuillez mettre à jour votre mandat de prélèvement SEPA sur sepa-prelevement.com

Phishing



- Fichier vidéo : Campagne Hack Academy WILLY

Arnaque au faux support technique



Fichier vidéo : Alerte critique de Microsoft

Usurpation d’identité

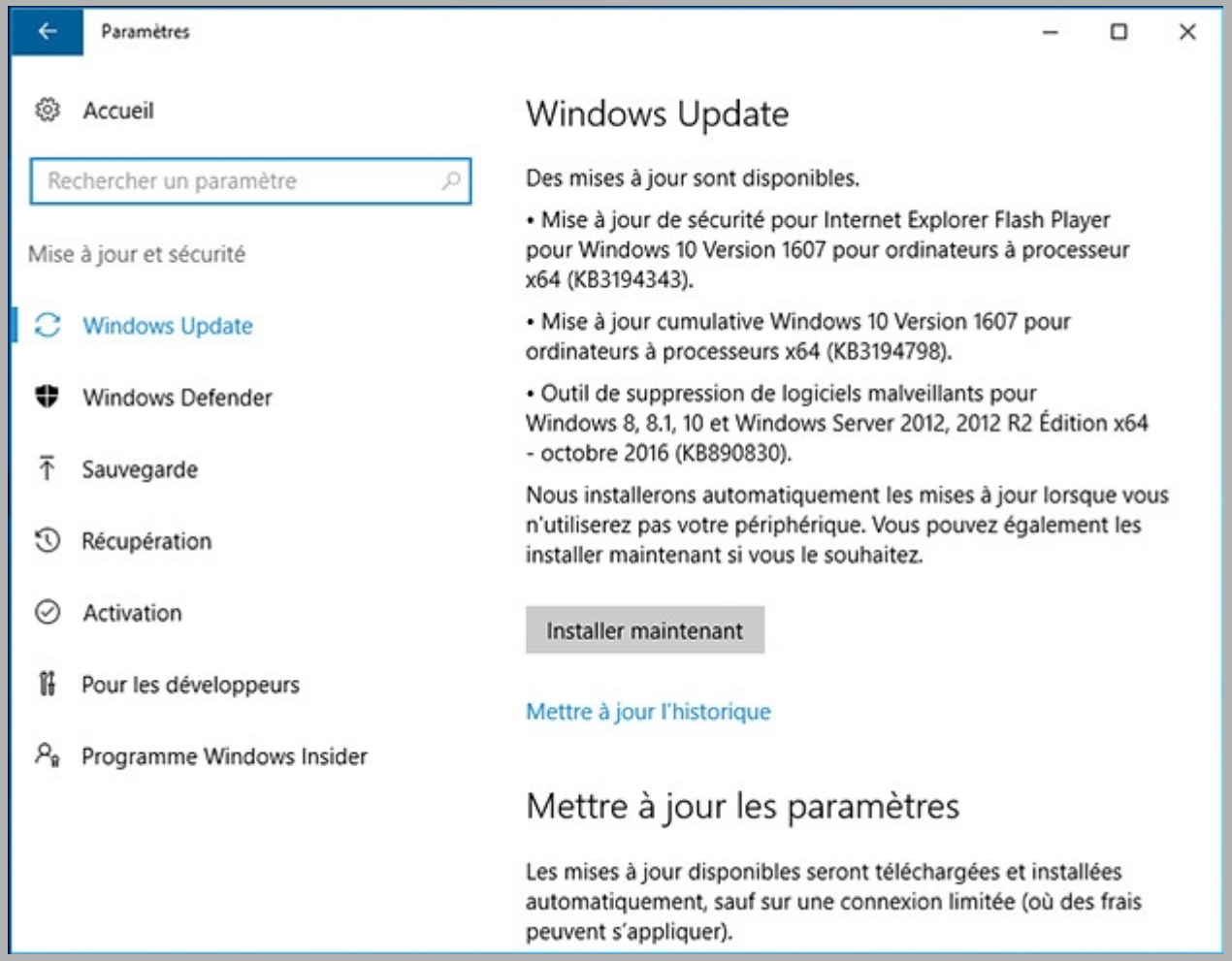
«Utilisation de données personnelles propres à vous identifier sans votre accord. Une fois volées, ces informations peuvent servir aux usurpateurs pour nuire à votre réputation, réaliser des opérations financières ou commettre des actes répréhensibles en votre nom.»

Source : economie.gouv.fr

Usurpation d’identité, s’en prémunir

- choisir un «bon mot de passe»
- garder ses mots de passe pour soi
- prendre des précautions lorsqu’on utilise pas son ordinateur
- vérifier l’authenticité d’un expéditeur avant d’envoyer des informations personnelles ou sensibles par mail (leboncoin)
- utiliser plusieurs adresses email et des alias
- être attentif à ses relevés de compte bancaire
- détruire tout papier comportant des informations personnelles avant de le jeter

Faire les mises à jour de sécurité



Gestionnaire de mise à jour de Windows 10
Démarrer → Paramètres → Mise à jour

Télécharger des logiciels depuis des sources fiables

Utiliser uniquement les sites officiels des éditeurs (recherche Wikipedia pour l’adresse officielle)

Sur smartphone regarder les avis et les permissions avant de télécharger

Utiliser du logiciel libre : code ouvert, moins de virus

- https://framalibre.org
- https://prism-break.org/fr/
- https://f-droid.org

Bloquer la publicité et les pisteurs

« La publicité est source de ralentissement du chargement des pages et de surcharge du processeur »

Sur les sites grand public

publicité
<u>+ pisteurs</u>
= 2/3 du contenu

→ Utiliser Mozilla Firefox avec uBlockOrigin

Utiliser de bons mots de passes

phrase de passe ; quelques mots n’ayant aucun rapport les uns avec les autres

« pouvoir couplé désert camion »

Une vraie phrase

« J’apprends la sécurité numérique. »

Mot de passe générés aléatoirement

« y3VZpqLioEoXwu3uHdRo »

Gestionnaire de mot de passe

- un seul mot de passe à retenir
- mot de passes générés aléatoirement
- saisie automatique
- reste en local (+ sécurité)

Informations et tutoriels :
https://www.djan-gicquel.fr/keepass

Sauvegarder ses données

- de façon régulière = minimum tous les mois
- moyen fiable = disque dur externe (~ 50€)
- Sauvegarde locale
  - plus de Confidentialité
  - plus écologique
  - temps d’accès réduit = restauration rapide
- les données doivent pouvoir être lue si le PC ne démarre plus : logiciel libre
- les données doivent être restaurées gratuitement

Sauvegarder ses données

- de façon régulière = minimum tous les mois
- moyen fiable = disque dur externe (~ 50€)
  - de locale
  - plus de
  - plus é
  - accès réduit = restauration rap
- les données doivent pouvoir être lue si le PC ne démarre plus : logiciel libre
- les données doivent être restaurées gratuitement

Le cloud n'est pas une sauvegarde !

Le cloud n'est pas une sauvegarde !

Sauvegarder ses données : méthode

Copier-coller
- espace disque
- long
- pas d’historique

Logiciel de sauvegarde
- historique
- gain de place
- gain de temps

Les logiciels que je recommande

Anti adware/malware
- Malwarebytes et ADWcleaner

Navigateur web
- Mozilla Firefox avec des extensions protectrices

Client de courriel
- Mozilla Thunderbird et son antispam adaptatif

Et si vous le pouvez utiliser un système sécurisé comme GNU/Linux

Pour aller plus loin, suivre Sandoz

https://youtube.com/channel/UCnC8KCcp2-DYfPY4_bKIc0A
Ou chercher «Sandoz» sur Youtube

Merci pour votre attention et participation !

Accompagnement personnalisé à la sécurité et la confidentialité numérique

https://numethique.djan-gicquel.fr