La sécurité sur le WEB

8 novembre 2018

Claude Maury

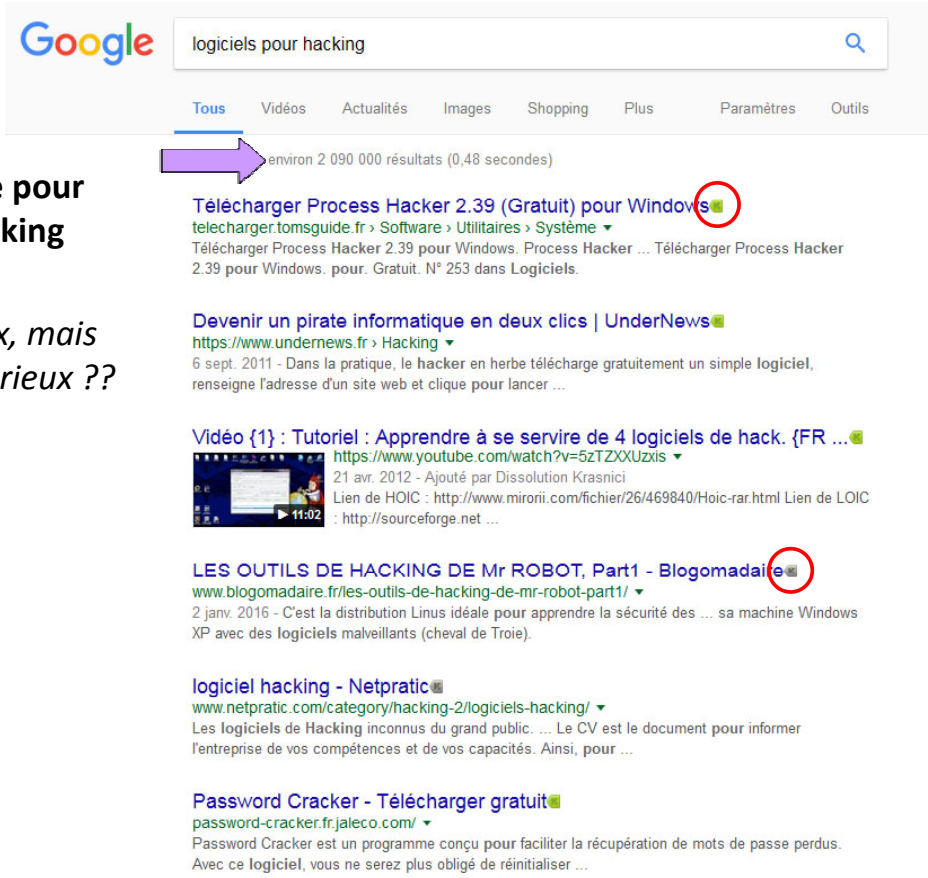
SI VIS PACEM, PARA BELLUM

Si tu veux la paix, prépare-toi à la guerre.

Horizons nouveaux

Un terrain fertile pour amateurs de hacking

Des sites douteux, mais aussi des sites sérieux ??



Stratégie sécuritaire

Sun Tzu – l'art de la guerre - VI^{ème} siècle av. J.-C.

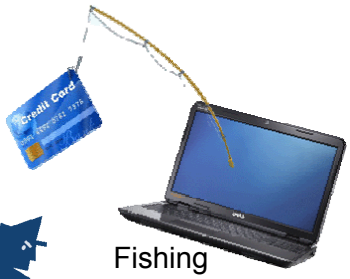
- ***Connais ton ennemi et connais-toi toi-même; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.***
- ***Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales.***
- ***Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites.***

Profils des pirates

- Les chapeaux blancs – hackers éthiques.
- Les chapeaux noirs - véritables cybercriminels.
- Les chapeaux gris – c'est l'exploit informatique qui les motivent.
- Les chapeaux bleus - ont pour rôle de trouver les vulnérabilités des systèmes pour les corriger.
- Les script kiddies - vandalisent des systèmes informatiques dans le but de s'amuser.
- Les crackers - spécialisés dans le cassage de codes, de mots de passes et de logiciels dans le but d'en tirer profit.
- Les hacktivistes – agissent pour défendre une cause, transgressent les lois (ex : Anonymous, RTmark, ..) .

Panorama des attaques

Harcèlement et fake news (désinformation)



Fishing (hameçonnage)

DDOS – Dénis de Services

Usurpation d'identité

Cyber war

Social engineering

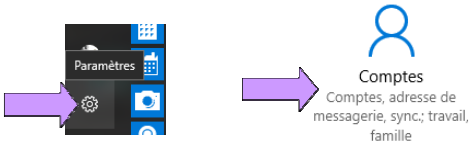
Racket informatique

Spyware – logiciel espion

La protection basique du PC

- N'utilisez pas le compte administrateur de votre PC pour vos opérations, ayez un compte utilisateur
- Protégez le compte administrateur par un bon mot de passe
- Effectuez les mises à jour du système et des logiciels
- Utilisez une protection internet complète (ex. : Mc Affee, Norton, Kaspersky, etc..)
- Si vous prêtez votre PC, ouvrez un compte visiteur
- Attention aux programmes téléchargés gratuitement
  - Les programmes gratuits Open source sont fiables
- **Sauvegardez périodiquement vos fichiers**

Modifier ses droits d'accès

- Pour W10 : 

- Pour W7 : ⇨ Panneau de configuration ⇨ Comptes utilisateurs
- Créez un nouveau compte « Bidule » avec les droits administrateurs
  - Ne pas le nommer Admin ou autres synonymes
- A partir de ce nouveau compte, enlevez les droits administrateur de votre compte usuel
- Vous utilisez dorénavant votre compte usuel sans droit d'administration
  - En cas d'attaque lors d'une session sur internet, le pirate n'aura pas les droits d'administration de votre PC

Solidité des mots de passe

- Si le mot de passe contient *N* caractères indépendants et uniformément distribués, le nombre maximum d'essais nécessaires se monte alors à :
  - 10^N si le mot de passe ne contient que des chiffres
  - 26^N si le mot de passe ne contient que des lettres de l'alphabet totalement en minuscules ou en majuscules ;
  - 52^N si le mot de passe ne contient que des lettres de l'alphabet, avec un mélange de minuscules et de majuscules ;
  - 62^N si le mot de passe mélange les majuscules et les minuscules ainsi que les chiffres.
- Créez un séquestre de vos mots de passe :
  - Une feuille Excel avec accès par un mot de passe
  - Un logiciel qui chiffre le fichier de vos mots passe (ex: KeePass d'Open Source)

Créer un mot de passe solide

- N'employez pas le même nom d'utilisateur ni le même mot de passe pour tous les services.
- Ne pas enregistrer par défaut vos mots de passe pour vos différents login
- Comment créer un bon mot de passe ?
  - Catégorisez vos mots de passe (les passe-partout, les professionnels, les privés, etc.)
  - Changez-les périodiquement, **ne changez jamais un mot de passe sur une demande email avec un lien pour le changement**
  - Evitez les signes spéciaux et caractères accentués si vous voyagez souvent
  - Exemples de mot de passe :
    - 7649 = 10^4 essais = 10'000 essais
    - **Vma4RMdln** ⇨ Vaut mieux avoir 4 Roues Motrices dans la neige = 62^9 essais = 13'537'086'546'263'600 (13'537 billions d'essais)
    - (cheville phonétique) **RVarit6k7** ⇨ Hervé a hérité 6 cassettes = 62^9 essais

Gérer sa mailbox

- Utilisez un service Webmail (ex : gmail.com) au lieu d'une messagerie PC (ex : Outlook de MS Office)
- N'utilisez pas votre messagerie professionnelle à titre privé
- Utilisez 2 mailboxs privées différentes
  1) Mailbox personnelle pour la correspondance administrative, amis, et privée
  2) Mailbox poubelle pour tous les comptes achats, concours, etc..
- Eviter une adresse email nominative (prévention des spams)
- Utilisez la fonction « Liste noire » pour les spams

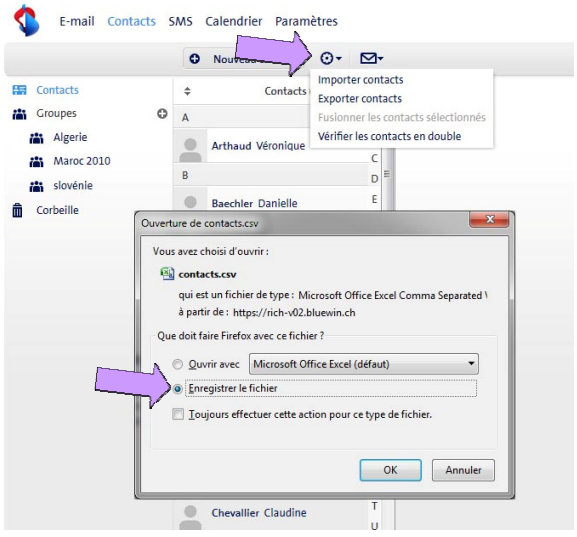
Un anti-virus protège uniquement des virus, pas des autres attaques internet

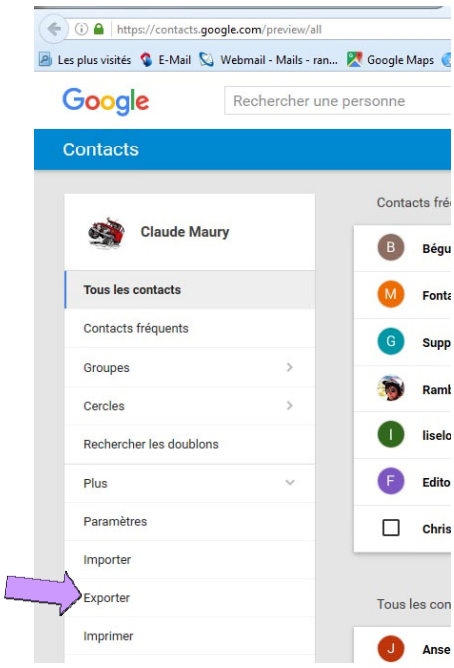
Gérer sa mailbox (2)

- Créez des dossiers dans votre mailbox pour gérer les messages en attente
- Ne pas conserver dans votre mailbox tout ce qui est confidentiel,
  - Sauvegardez ces messages sous forme .PDF dans des dossiers autres que la mailbox avec le logiciel gratuit **PDFCreator** disponible sur http://www.pdfforge.org/
- Ne cliquez pas sur des liens proposés par des correspondants inconnus
  - Si besoin est pour un lien connu, connectez-vous sur le site en question
- Utilisez BCC *(Blind Carbone Copy)*/CCI *(Copie Carbone Invisible)* pour tous vos messages adressés à un groupe de personnes afin de préserver leurs sphères privées
  - Attention aux listes de distribution de gags, utilisez le BCC

Sauvegarder ses contacts email

Créez un dossier de sauvegarde de ses contacts dans Mes Documents





Votre email a été piraté !

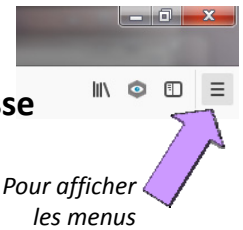
- Changez immédiatement tous vos mots de passe de vos comptes bancaires et annulez votre carte de crédit
- **Vous loger sur votre messagerie et utilisez la procédure « j'ai oublié mon mot de passe »** pour le changer par un nouveau mot de passe solide, ce qui bloquera le hacker
- Si cela ne fonctionne pas, tentez de faire annuler ce compte email auprès du prestataire, puis
  - Créez un nouvel email (autre adresse et autre mot de passe)
  - Restaurez la sauvegarde de votre répertoire dans ce nouveau compte
  - Envoyez un message (en BCC) à tous vos contacts demandant de :
    - Ne pas réagir au dernier mail reçu de votre part par l'adresse piratée
    - De notez votre nouvelle adresse

Si c'est l'email d'un(e) ami(e)

- Ne répondez pas à cet email, le mettre dans la poubelle
- Supprimez son adresse email de votre répertoire
- Appelez votre ami(e) pour vous assurer qu'il/elle est au courant du piratage et donnez-lui les conseils ci-dessus

Sécuriser sa navigation internet

- Utilisez **Firefox** qui est le moins fouineur des navigateurs
- Attribuez votre navigateur Firefox : « Navigateur par défaut »
- Utilisez la navigation privée autant que possible
- Paramètres importants (menu Options): Options



  - **Ne pas enregistrer les identifiants et les mots de passe**
  - Définir où enregistrer les téléchargements par défaut
  - Bloquer le pistage de vos activités sur internet
  - Bloquer les contenus dangereux ou trompeurs
  - Ne pas laisser installer des modules complémentaires par défaut
  - Ouvrir un nouvel onglet au lieu d'une nouvelle fenêtre
  - Bloquer les fenêtres Popup
  - **Ne jamais conserver l'historique**

Pour télécharger et installer Firefox
https://www.mozilla.org/fr/firefox/

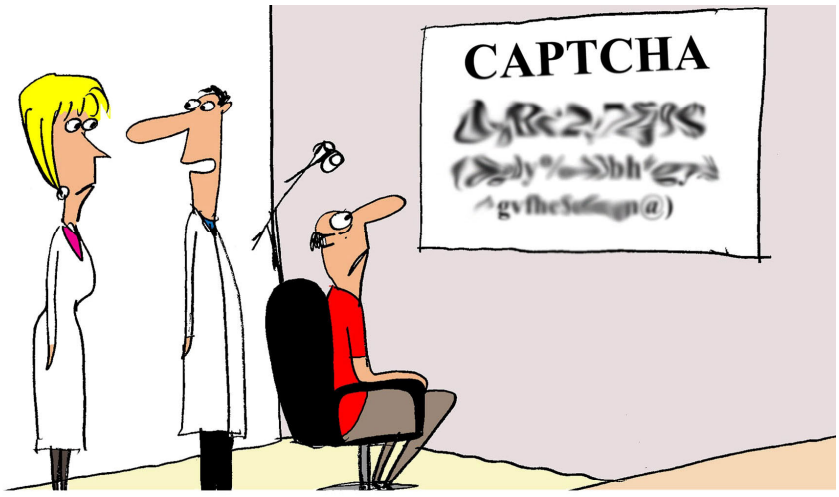
Connexion internet sécurisée

- https signifie que la connexion est sécurisée, mais pas forcément le bon site atteint
- Une authentification forte garantit la sécurité sur le site (ex. : les banques envoient après le login un code accès sur votre mobile)
- Un bon logiciel de protection internet indique si le site est douteux ou pas. Ce n'est pas le cas d'un antivirus

Un anti-virus protège uniquement des virus, pas des autres attaques internet

Pourquoi des Captchas

- Le terme **CAPTCHA** est une marque commerciale de l'université Carnegie-Mellon désignant une famille de tests permettant de s'assurer qu'une réponse n'est pas générée par un ordinateur.



J'ai augmenté mon chiffre d'affaires depuis que j'ai remplacé le Tableau des yeux par un Captcha

Faire ses achats en toute sécurité

- Utilisez une carte de crédit à prépaiement ou le service Pay-Pal
- Evitez de laisser enregistrer votre n° de carte sur les sites d'achats, de réservations, etc..
- Contrôlez la fiabilité du site qui est indiquée par votre logiciel de protection internet
  - En cas de litige, le site douteux sera aux abonnés absents
- Si l'on vous demande votre n° de carte de crédit ou bancaire par messagerie, téléphonez pour le transmettre
- Ne conservez pas la trace de vos achats dans votre messagerie
- A savoir que les banques ne communiquent jamais par email

Protégez votre sphère privée

- Respectez la sphère privée de tierces personnes, ne publiez pas leurs données personnelles et ne mettez pas leur nom sur des photos.
- Utilisez Cci ou Bcc pour vos groupe de communication email
- Utilisez des pseudonymes.

La confidentialité sur Facebook

5 paramètres indispensables de confidentialité à activer :

1) **Qui peut voir mon contenu ?** : Sélectionnez Amis, et Amis seulement. Ce qui implique, évidemment, qu'il vous faudra ne pas accepter n'importe quel Ami
2) **Examinez tous les contenus dans lesquels vous êtes identifié :** Sélectionnez **OUI**, et rien d'autre. Vous serez ainsi alerté de tout ce qui se postera, et où vous êtes taggé.
3) **Limiter l'audience de mes publications ?** Limitez-vous à vos Amis. Ignorez Amis de mes Amis et, pire encore, Tout le Monde.
4) **Qui peut me contacter ?** Contentez-vous d'Amis, *à moins que vous n'ayez une utilisation professionnelle de Facebook.*
5) **Souhaitez vous que d'autres moteurs de recherche aient un lieu avec votre journal ?** Modifiez le paramètre à **NON**, *à moins qu'il s'agisse d'une page Facebook à strict but professionnel ou médiatique.*

Les smartphones

1) N'enregistrez pas d'informations confidentielles dans votre smartphone
2) Ne désactivez pas le code PIN et changez celui proposé par défaut.
3) Définissez un délai de verrouillage automatique. Cela empêche l'accès aux informations contenues dans le smartphone en cas de perte ou de vol.
4) Notez le numéro « IMEI - *International Mobile Equipment Identity* » du smartphone pour le bloquer en cas de perte ou de vol.
   - *Identification unique de série de l'appareil - *#06# pour l'afficher*
5) Réglez les paramètres du smartphone ou dans les applications de géolocalisation afin de toujours contrôler quand et par qui vous acceptez d'être géolocalisé.
6) Désactivez le GPS ou le WiFi quand vous ne vous servez plus d'une application de nécessitant la géolocalisation.

La confidentialité sous W10

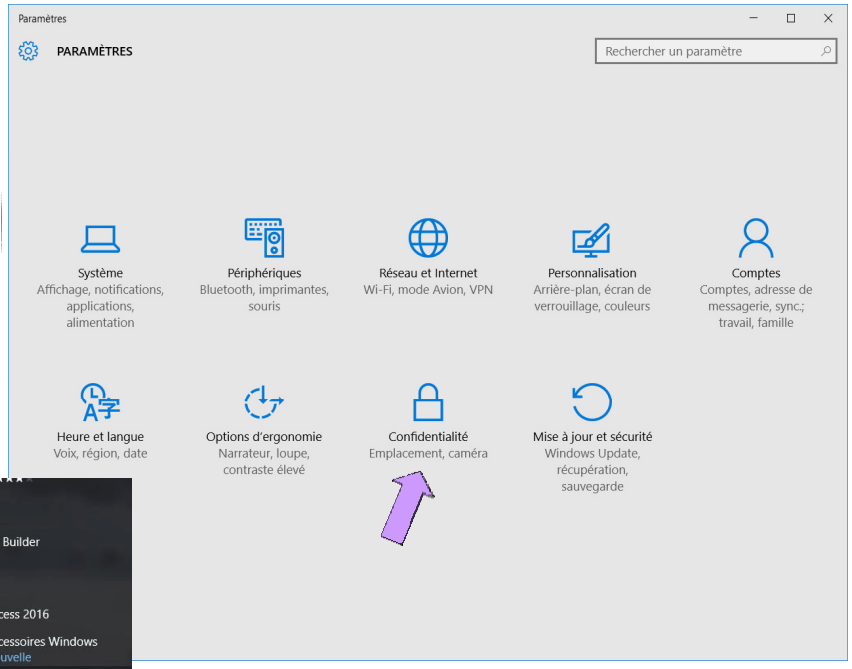
Sphère privée

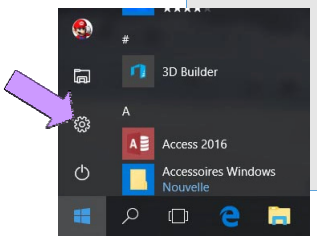
Windows 10 sera plus transparent

Le système d'exploitation Windows 10 de Microsoft sera plus transparent dès les prochaines mises à jour prévues en 2017. L'entreprise a accepté les recommandations du préposé fédéral à la protection des données, à la suite d'une procédure lancée contre elle en 2015. Les adaptations sont prévues à l'échelle mondiale, a indiqué hier le préposé. Microsoft annonce également sur son blog que la nouvelle version du système d'exploitation préservera davantage la sphère privée de l'utilisateur.

ATS

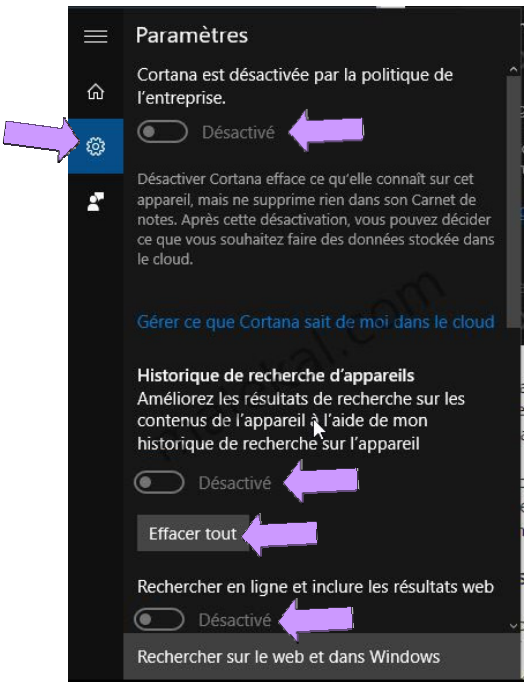
Tribune de Genève
12/jan/2017



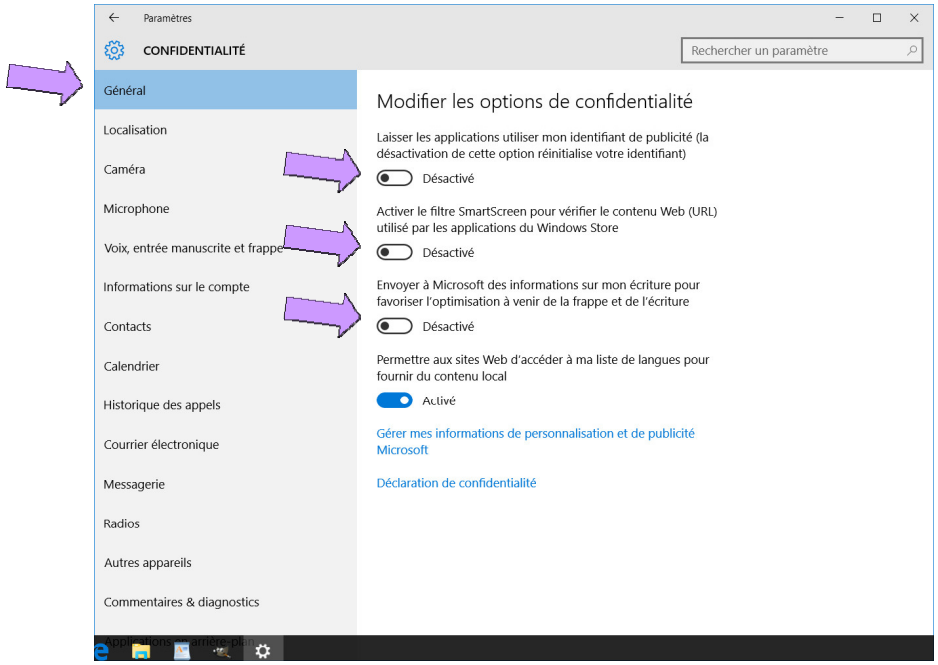


Désactiver Cortana

- Ouvrir Cortana en cliquant sur son icône
- Cliquez sur la roue dentée à gauche
- Cliquez sur le bouton Effacer tout
- Désactivez les 3 options



La confidentialité sous W10



En résumé

Une bonne sécurité internet, c'est :

20% de technologie

80% de bonnes pratiques