Guide de la cyber-sécurité

Publié par l'Association mondiale des journaux et des éditeurs de médias d'information
Pour le Forum de la Presse Arabe Indépendante
Novembre 2013
Écrit par Alan Pearce

Si les forces de l'ordre ou les services de renseignement veulent surveiller l'accès à Internet de quelqu'un – lire ses e-mails et messages publiés sur les médias sociaux, récupérer ses contacts, savoir ce qu'il recherche et télécharge, et écouter ses appels – alors ils le peuvent et ce, peu importe les ordonnances judiciaires et les mandats. Cela signifie qu'absolument tout peut être espionné.

En général, ils obtiennent l'accès aux ordinateurs et aux smartphones par le biais de ce qu'on appelle « l'ingénierie sociale », l'art d'inciter les utilisateurs à visiter des sites web malicieux puis de les convaincre de donner des informations confidentielles, ou bien en implantant secrètement des logiciels malveillants dans leur système (méthode connue sous le nom de « drive-by download » ou « infection par téléchargement ») et par courriel.

Méfiez-vous des messages publiés sur les réseaux sociaux et des e-mails contenant des liens attrayants, dont la plupart sont souvent raccourcis afin que vous ignoriez vers quoi vous vous dirigez. Ces URL courtes peuvent être agrandies sur LongURL.org.

Ne cliquez jamais sur des pièces jointes ou des liens si vous n'êtes pas sûr de leur origine. Si vous devez ouvrir une pièce jointe suspecte, déconnectez-vous d'Internet d'abord et lancez-la via le « bac à sable » d'un anti-virus.

Si vous avez l'habitude de lire des documents sensibles et pensez pouvoir être observé, utilisez un ordinateur distinct non relié à Internet – c'est ce qu'on appelle l'« air-gapping ».

Il est primordial de sécuriser les réseaux sans fil de votre domicile et de votre bureau en changeant le mot de passe administrateur du routeur sans fil.

Vous pouvez facilement attirer l'attention par des recherches sur des sujets sensibles sur Internet ou simplement en faisant partie de la liste des contacts d'un suspect.

Soudain, l'Internet devient un lieu très dangereux pour les journalistes.

Toutefois, en étant à l'affût des dangers et en combinant les outils et techniques énumérés ci-dessous, il est possible de ne pas attirer l'attention dans un premier temps et de rester indétectable.

Lors du choix d'un mot de passe, optez pour une expression facilement mémorisable plutôt que pour un vrai mot du dictionnaire. Par exemple, « I Like Lots Of Vinegar On My Fish And Chips » peut être abrégé par ILLOVOMFAC. Vous devez y ajouter des chiffres et des caractères non-alphanumériques, ainsi qu'un mélange de majuscules et minuscules, ce votre code d'accès deviendra a priori très difficile à déchiffrer.

S'il n'est pas trop tard, ne publiez jamais d'informations personnelles sur les réseaux sociaux – votre date de naissance, vos liens familiaux, votre adresse, vos projets de voyage, des photos permettant de vous identifier, etc.

Un logiciel gratuit et en libre accès (open source) est généralement préférable à son équivalent payant, car il peut être testé par des développeurs et les dispositifs d'enregistrement ou portes dérobées (backdoors) peuvent être identifiés. Tous les logiciels de cryptage propriétaire doivent être manipulés avec le plus grand soin.

Tous les liens fournis dans ce guide doivent être ouverts dans votre navigateur. Les liens Web profonds indiqués par le signe <!> ne peuvent être ouverts que dans un navigateur Tor-Firefox que vous apprendrez à configurer ici.

Sachez qu'aucun système ou logiciel ne peut être sécurisé à 100 % !

Installer des protections

Le navigateur le plus soucieux de la sécurité est sans doute Mozilla Firefox, disponible aussi en arabe. Mais tout d'abord, passez une minute ou deux à ajuster vos *paramètres* :

- Cliquez sur le logo Firefox et sélectionnez *Options/Options.*
- Dans la boîte de dialogue, ouvrez *Confidentialité* puis cochez l'option *Avertir les sites Web que je ne veux pas être suivi*. Il existe une option pour *Toujours utiliser le mode de navigation privée.* Décochez *Accepter les cookies*. Cochez *Effacer l'historique après la fermeture de Firefox*. Sous *Historique,* sélectionnez *Utiliser les paramètres personnalisés pour l'historique* puis *Ne jamais se rappeler de l'historique.*
- Sous *Sécurité*, cochez *M'avertir lorsque les sites essaient d'installer des add-ons*. Retirez toutes les exceptions. Cochez *Bloquer les sites d'attaque rapportés* et *Bloquer les sites de contrefaçon déclarés*. Décochez *Se souvenir des mots de passe pour les sites*.
- Dans l'onglet *Avancé*, sous *Général* cochez *Me prévenir quand des sites Web tentent de rediriger ou de recharger la page*. Sous *Réseau* cochez *Dites-moi quand un site Web demande de stocker des données pour une utilisation hors ligne*. Cochez *Ignorer la gestion automatique du cache* ou mettez la taille du cache à 0.

Il existe un certain nombre d'add-ons de sécurité gratuits pour Firefox. Installez pour cela les éléments suivants :

HTTPS Finder ou HTTPS Everywhere
Do Not Track Me
BetterPrivacy
QuickJava
DownThemAll

N'utilisez pas Google pour les recherches sensibles, utilisez Secret Search Labs ou iXQuick.

Pour une navigation rapide et anonyme, utilisez AllNetTools, Guardster ou Anonymouse. Les Réseaux privés virtuels gratuits (VPN) contiennent FreeVPN et ProXPN.

Effacez vos traces avec CCleaner et supprimez définitivement les données sensibles avec Heidi Eraser. Installez un logiciel anti-virus gratuit de AVG ou Avast.

Utiliser Tor

Tor est un réseau caché du Web profond dans lequel l'identité et la localisation des utilisateurs sont cryptées et masquées, offrant ainsi le parfait anonymat. Commencez par télécharger gratuitement Tor/Firefox bundle. Une version arabe du navigateur peut être trouvée ici .Elle est sûre et facile à installer. Il suffit de suivre les instructions à l'écran et une passerelle vers le Web profond peut être configurée en quelques minutes sans compétences particulières. Ajoutez également un exécuteur HTTPS, comme HTTPS Everywhere. Ajoutez également Do Not Track Me.

Sur la page d'ouverture, là où s'affiche le message « Votre adresse IP semble être... », apparaît alors une suite de nombres qui n'a absolument rien à voir avec votre ordinateur. Vous êtes désormais anonyme et donc libre d'explorer Tor ou de bifurquer vers le Web de surface avec un risque très faible d'être surveillé.

Points d'entrée vers le Web profond

- Le Wiki invisible <!> http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page
- Tor*Dossier* <!> dppmfxaacucguzpc.onion
- Tor*Liens* <!> torlinkbgs6aabns.onion
- Tor*Forum Aide* <!> http://zntpwh6qmsbvek6p.onion/forum/

Si vous avez des difficultés à ouvrir un site Web profond, réessayez tout simplement un peu plus tard et il peut réapparaître. La disponibilité du site Web profond peut être vérifiée sur *Is it up?* <!> http://zw3crggtadila2sg.onion/downornot/

Pour encore plus de sécurité, accédez à Tor directement depuis une clé USB, une carte SD, un disque dur portable ou un CD/DVD. Ceux-ci peuvent être utilisés sur n'importe quel ordinateur connecté à Internet. Installez Tor/Firefox et d'autres programmes utiles directement sur le périphérique.

Applications portables recommandées

- PortableApps.com – large gamme de logiciels open source pour appareils portables
- KeePass Portable
- Notepad Portable Text Editor
- VLC Media Player Portable
- IrfanView Portable
- GIMP Portable
- Sumatra PDF Portable
- Eraser Portable
- 7-Zip Portable

Communications sécurisées

E-mail : Continuez à utiliser votre compte de messagerie existant pour une utilisation générale, de sorte que les agences aient quelque chose à surveiller et sans éveiller les soupçons en stoppant toute communication. Pour toute correspondance sensible, utilisez Tor ou un VPN et inscrivez-vous anonymement auprès d'un service de courrier électronique gratuit basé sur le Web (mais évitez les fournisseurs tels que Hotmail, Gmail, etc.). Pensez à utiliser un ordinateur séparé pour ces activités.

L'adresse e-mail peut également être cryptée au sein du message, ainsi que n'importe quelle pièce jointe, mais cela peut en soi attirer l'attention.

Désactivez *les paramètres HTML* de votre e-mail et choisissez le mode *texte simple*.

Messagerie secrète : PrivNote, pour des messages gratuits qui s'autodétruisent. SpamMimic, qui convertit les messages simples en *texte spam.* PasteOnion <!> http://xqz3u5drneuzhaeo.onion/users/boi/, pour coller et partager des textes, images, etc. sur le Web profond.

Messagerie privée : Tor*PM* <!> http://4eiruntyxxbgfv7o.onion/pm/. Simple*PM* <!> http://4v6veu7nsxklglnu.onion/SimplePM.php.

Chat profond : Tor*Chat* <!> http://lotjbov3gzzf23hc.onion/index.php/group/torchat, messagerie instantanée peer-to-peer. EFG Chat <!> http://xqz3u5drneuzhaeo.onion/users/efgchat/index.php?chat=lobby.

Réseaux sociaux profonds : Tor*StatusNet* <!> http://lotjbov3gzzf23hc.onion/. Tor*Book* <!> http://ay5kwknh6znfmcbb.onion/torbook/. Tor*Square* <!> http://ay5kwknh6znfmcbb.onion/torsquare/.

Smartphones & appareils mobiles

Ne laissez jamais votre smartphone ou tout autre appareil numérique sans surveillance. Si des policiers ou d'autres personnes veulent l'examiner, ne pas les laisser seuls avec votre appareil. De même, soyez très prudent lorsque vous rechargez votre téléphone. Il ne faut que quelques secondes pour insérer des logiciels espions dans l'appareil.

Pour les utilisateurs d'Android, une bonne option gratuite pour se protéger contre les virus, les logiciels malveillants et les logiciels espions est AVG Mobilation. Lookout protège les appareils iOS ou Android des réseaux Wi-Fi non sécurisés, des applications malveillantes, des liens frauduleux, etc.

Un VPN mobile vous aidera à vous masquer en public. Hotspot Shield crypte tout le trafic d'un smartphone à travers un réseau privé virtuel pour cacher votre identité et éviter d'être suivi. Il vous permet également de visualiser les contenus interdits et d'accéder aux versions mobiles de Twitter et Facebook si leurs services sont toujours bloqués là où vous trouvez.

- Placez un code de sécurité sur votre smartphone en plus du code SIM et engagez la fonction de verrouillage automatique.

- Désactivez les connexions réseau et coupez les pontages. Ne diffusez pas le nom de votre appareil Bluetooth et désactivez les connexions Wi-Fi automatisées.
- Désactivez la géo-localisation et le positionnement GPS via les *Paramètres*.
- Autant que possible, connectez-vous aux réseaux 2G, 3G ou 4G, plutôt qu'aux services Wi-Fi gratuits.
- Lorsque vous couvrez des manifestations etc., remplacez la carte SD dans le téléphone par une carte de rechange qui ne contient pas vos données personnelles ni vos contacts en cas d'arrestation. De même, passez en mode avion pour éviter d'être suivi.
- Évitez de connecter des périphériques personnels au réseau ou ordinateur de bureau.
- Mettez à jour régulièrement vos appareils afin de maintenir vos systèmes d'exploitation en conformité avec les améliorations qui sont apportées régulièrement à la sécurité.
- Retirez la batterie ou laissez votre téléphone lors d'une rencontre avec des contacts, etc.

Applications de sécurité

Vous pouvez prendre votre smartphone sur Tor et garder tout hors de portée des radars en utilisant des applications pour Android et iOS avec accès aux Web de surface et de profondeur, ainsi qu'aux MP et e-mails sans être surveillé ni bloqué.

- **Messagerie secrète** — Heml.is sécurise le système de messagerie pour iPhone et Android. Secret SMS pour iOS cryptera les messages entre utilisateurs et les dissimulera.
- **Caméras secrètes** — Secret Video Recorder Pro pour Android et iOS. Secret Camera pour iOS et Mobile Hidden Camera pour Android.
- **Audio secret** — Secret Audio Recording pour Android et Spy Recorder pour iOS.
- **Enregistrement des appels** — Top Secret Call Recorder pour Android et Call Log Pro pour iOS.
- **Compartiment secret** — dossiers secrets pour Android et iOS.
- **Supprimer les preuves** — Il existe des broyeurs pour Android et iOS.

Cacher et transférer des données secrètes

- Onion File Hosting <!> http://f4om2jzqkad5zpxv.onion/hosting/login
- Anonyshares <!> http://4eiruntyxxbgfv7o.onion/anonyshares.html
- Onion File Sharing - <!> http://f3ew3p7s6lbftqm5.onion/
- sTORage - <!> http://utovvyhaflle76gh.onion/
- QicPic <!> http://xqz3u5drneuzhaeo.onion/users/qicpic/
- OneSwarm
- Pastebin

Programmes gratuits recommandés

- Comodo Personal Firewall
- Lavasoft's Ad-Aware
- Spybot Search and Destroy
- Anti-Trojans
- Crap Cleaner
- Avast Free Antivirus
- AVG Anti-Virus Free Edition