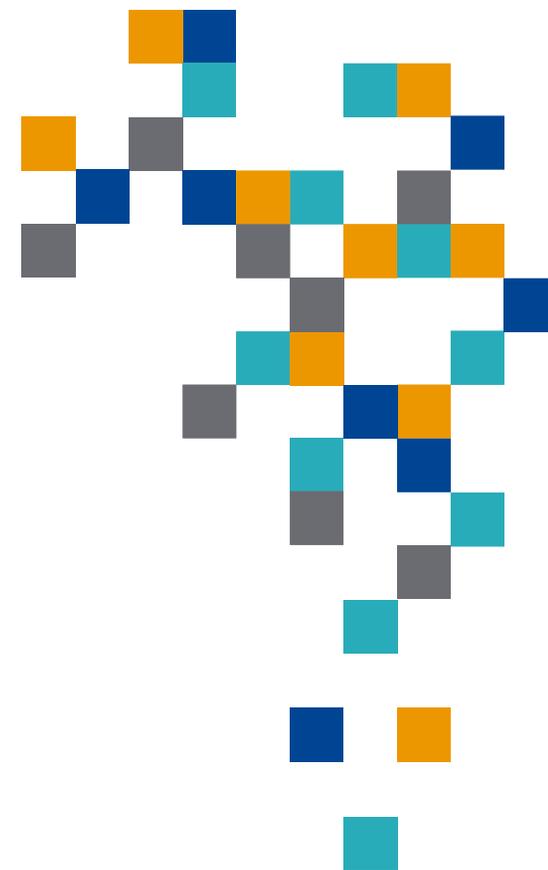


**CYBERSÉCURITÉ: 18 SECRETS QUE  
LES PIRATES INFORMATIQUES NE  
VEULENT PAS QUE VOUS SACHIEZ**



PRÉSENTÉ PAR ALAIN WAGNER

# Des statistiques qui dérangent

---

- 30 000 ordinateurs infectés par jour
- 8 nouveaux utilisateurs d'internet à la seconde
- 250 000 nouveaux virus par jour
- 80% des attaques sont effectuées sur des entreprises
- 99% des gens ne font pas de copies de sauvegarde
- 4 milliards d'adresses de courriel
- 200 milliards de courriels par jour
- 18 millions d'identifiants sont compromis chaque jour
- 21 h chaque année passée à reconfiguré un mot de passe



# Les différents types de cyberattaque

---



- L'installation de programmes espions et de programmes pirates.
- Le phishing : une technique de fraude dans laquelle les cybercriminels se font passer pour un tiers de confiance afin d'obtenir des renseignements sensibles tels que les noms d'utilisateurs, les mots passe ou les détails des cartes de crédit.
- Les dénis de service sur des sites.
- Les intrusions .
- Le vol d'informations .
- Le ransomware: un malware prend en otage des données personnelles et une rançon est demandée en échange de la clef de chiffrement des données cryptées.
- Le rebond vers un faux site.
- Attaque par brute force (trouver un mot de passe en testant successivement toutes les combinaisons possibles)

## 1 – Les pirates envoient des courriels personnalisés.

---

### ■ Le harponnage est l'hameçonnage.

- Le hameçonnage est une attaque d'ingénierie sociale, dans laquelle le criminel usurpe l'identité d'une entité digne de confiance tout en demandant des informations sensibles aux victimes.
- Le harponnage est un cybercrime qui utilise les courriels pour mener des attaques ciblées contre des individus et des entreprises.



# 1 – Les pirates envoient des courriels personnalisés.

---



## ■ Que faire ?

- Vérifiez les liens URL, incorrects ou inhabituels en survolant les hyperliens afin de voir l'adresse URL utilisée.
- Si vous avez des pièces jointes ou un corps de message qui est en fait une image, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens à moins d'être certain que le message provient d'une source fiable.

# 1 – Exemples de courriel dangereux.



De : Swisscom Admin

Aujourd'hui, 13:05

A : undisclosed-recipients

Objet : Votre facture - septembre

 Facture\_09.zip

Cher client,

Veillez trouver ci-joint votre facture référence F09D567 pour le mois de septembre.

Cordialement,

Swisscom  
Service à la clientèle

# 1 – Exemples de courriel dangereux.

De : Swisscom Admin  
A : undisclosed-recipients  
Objet : Votre facture - septembre

 Facture\_09.zip

Cher client,

Veillez trouver ci-joint votre facture référencée pour le mois de septembre.

Cordialement,

Swisscom  
Service à la clientèle

Aujourd'hui, 13:05

Il ne faut jamais ouvrir une pièce jointe si vous ne connaissez pas l'expéditeur.

Ouvrir ce fichier pourrait installer des virus ou des fichiers malveillants sur votre ordinateur.



# 1 – Exemples de courriel dangereux.

---



ws

De : AFC

Oct. 1, 16:27

A : Cécile Keller

Objet : Message important de l'Administration Fiscale Cantonale

---

Si ce message n'apparaît pas directement, veuillez cliquer sur ce lien :

[www.afc.ch/file/cecile\\_keller.jsp/](http://www.afc.ch/file/cecile_keller.jsp/)

# 1 – Exemples de courriel dangereux.

De : AFC  
A : Cécile Keller  
Objet : Message important de l'Administration Fiscale

---

Si ce message n'apparaît pas directement, veuillez cliquer sur le lien ci-dessous :

[www.afc.ch/file/cecile\\_keller.jsp/](http://www.afc.ch/file/cecile_keller.jsp/)

Si vous cliquez sur ce lien, un programme malveillant pourrait être téléchargé sur votre ordinateur.

Il faut toujours être vigilant. Survoler l'URL avec votre souris: une URL s'affiche. Comparez-le avec le contenu du courriel. S'ils sont différents ou si l'adresse vous paraît suspecte, ne cliquez pas.

# 1 – Exemples de courriel dangereux.

De : Isaac Kosongo

Oct. 1, 18:45

A : Cecile Keller

Objet : Bonjour !

Chère madame,

Quand ma mère mourut en octobre 1984 mon père s'occupa de moi. Avant la mort de mon père, le 29 juin 2000, dans un hôpital privé mon père me fit venir à son chevet et m'expliqua qu'il avait mis de côté une somme de quinze millions de dollars à mon intention, dans une banque locale, à mon nom. Il m'a aussi expliqué qu'il avait été empoisonné par ses associés et que je devrais trouver une partenaire habitant à l'étranger, de mon choix, pour pouvoir faire transférer cette somme à l'étranger et l'investir.

C'est ainsi que je vous sollicite en tout bien tout honneur. Je vous verserai 25% de la somme pour le service rendu. Pour plus d'éclaircissements, contactez moi sur cet e-mail : [isaac\\_k@hotmail.com](mailto:isaac_k@hotmail.com) !



# 1 – Exemples de courriel dangereux.

De : Isaac Kosongo

A : Cecile Keller

Objet : Bonjour !

Chère madame,

Quand ma mère mourut en octobre 1984 m  
Avant la mort de mon père, le 29 ju  
père me fit venir à son cheve  
somme de quinze millions de dollars à mon  
locale, à mon nom. Il m'a aussi expliqué qu'il  
ses associés et que je devrais trouver une part  
l'étranger, de mon choix, pour pouvoir faire transfé  
l'étranger et l'investir.

C'est ainsi que je vous sollicite en tout bien tout honneur. Je vous verserai  
25% de la somme pour le service rendu. Pour plus d'éclaircissements,  
contactez moi sur cet e-mail : [isaac\\_k@hotmail.com](mailto:isaac_k@hotmail.com) !

Tout le contenu est suspect.  
Cette technique est connue  
depuis plusieurs années pour  
escroquer des individus, parfois  
pour des sommes d'argent  
importantes.

**Ne répondez jamais à ce type  
de message.**

**Les techniques de ces  
personnes malveillantes  
continuent d'évoluer et il faut  
être vigilant.**

# 1 – Comment lire une adresse URL ?

---



1

Vérifier que le nom de domaine existe vraiment, en particulier s'il vous semble farfelu !

2

Assurez-vous que le nom de la société précède le nom de domaine.

3

Vérifiez le protocole. Une société sérieuse aura toujours un protocole HTTPS en début d'adresse.

4

Vérifiez qu'un cadenas précède l'adresse URL. Il permet de reconnaître le certificat d'authenticité et prouver une connexion sécurisée.



Les conseils d'Alain

# 1 – Comment reconnaître un message frauduleux ?



- 1 Utilisation d'image d'une entreprise connue
- 2 Caractères menaçant ou alarmiste
- 3 Promesses d'argent facile
- 4 Fautes d'orthographe ou de syntaxe
- 5 Adresses de courriel et URL suspects
- 6 Pièces jointes suspectes



Les conseils d'Alain

## 2 – Les pirates ont bien du temps devant eux.

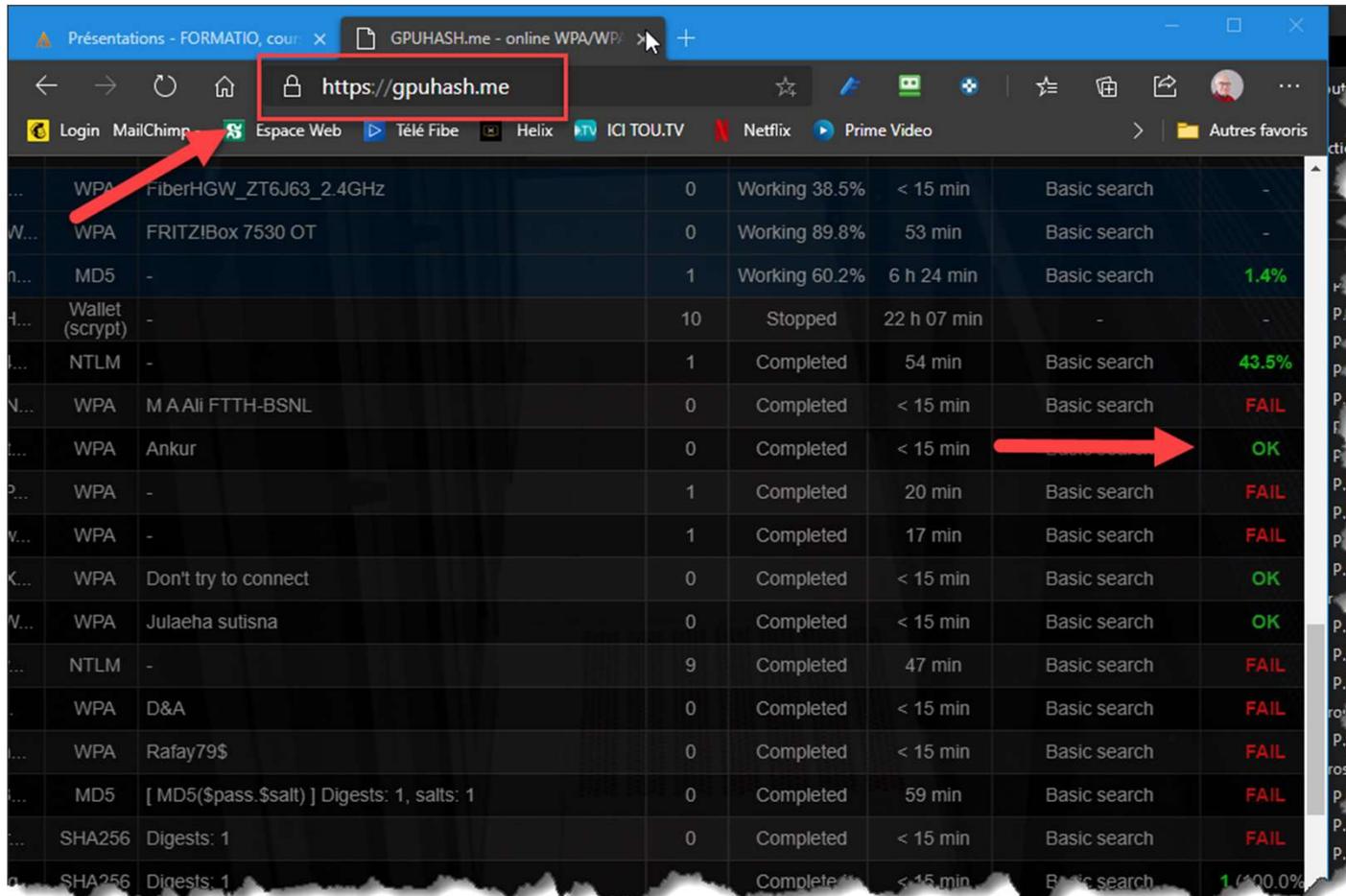
---

■ **Les pirates informatiques ont des programmes qui testent systématiquement des millions de mots de passe possibles.**

- Voir ma présentation du 17 septembre 2020 (introduction à la cryptographie)
- Les pirates dorment et vivent leur vie, alors que leur programme est en cours, testant une infinité de combinaison de mots de passe.



## 2 – Les pirates ont bien du temps devant eux.



Protocol	Target	Attempts	Status	Progress	Time	Method	Result
WPA	FiberHGW_ZT6J63_2.4GHz	0	Working	38.5%	< 15 min	Basic search	-
WPA	FRITZiBox 7530 OT	0	Working	89.8%	53 min	Basic search	-
MD5	-	1	Working	60.2%	6 h 24 min	Basic search	1.4%
Wallet (scrypt)	-	10	Stopped	-	22 h 07 min	-	-
NTLM	-	1	Completed	-	54 min	Basic search	43.5%
WPA	M A Ali FTTH-BSNL	0	Completed	-	< 15 min	Basic search	FAIL
WPA	Ankur	0	Completed	-	< 15 min	Basic search	OK
WPA	-	1	Completed	-	20 min	Basic search	FAIL
WPA	-	1	Completed	-	17 min	Basic search	FAIL
WPA	Don't try to connect	0	Completed	-	< 15 min	Basic search	OK
WPA	Julaeha sutisna	0	Completed	-	< 15 min	Basic search	OK
NTLM	-	9	Completed	-	47 min	Basic search	FAIL
WPA	D&A	0	Completed	-	< 15 min	Basic search	FAIL
WPA	Rafay79\$	0	Completed	-	< 15 min	Basic search	FAIL
MD5	[ MD5(\$pass.\$salt) ] Digests: 1, salts: 1	0	Completed	-	59 min	Basic search	FAIL
SHA256	Digests: 1	0	Completed	-	< 15 min	Basic search	FAIL
SHA256	Digests: 1	0	Completed	-	< 15 min	Basic search	1 (100.0%)

## 2 – Les pirates ont bien du temps devant eux.



1

Utilisez une phrase secrète plutôt qu'un mot de passe.

2

Incluez des caractères spéciaux, des chiffres et des lettres majuscules et minuscules.

3

Utilisez un gestionnaire de mots de passe qui génère et mémorise des mots de passe aléatoires.

4

Attention à ne pas enregistrer les mots de passe pour les comptes bancaires au cas où le gestionnaire de mots de passe serait piraté.



Les conseils d'Alain

### 3 – Les pirates adorent la fonction Bluetooth

---



- Si vous laissez la fonction Bluetooth activée après avoir utilisé des écouteurs mains libres,
  - Les pirates peuvent facilement se connecter à votre téléphone et voler vos données.

## 3 – Les pirates adorent la fonction Bluetooth



1

Désactivez la fonction Bluetooth après l'avoir utilisée ou réglez la visibilité comme non détectable.

2

Exigez un code de sécurité lorsque vous associez un nouvel appareil Bluetooth.



Les conseils d'Alain

## 4 – Les pirates se fauillent pendant que vous surfez sur Internet

---



### ■ Téléchargement à la volée

- Vous visitez ce qui semble être un site Web parfaitement inoffensif, mais en arrière-plan, vous êtes redirigé vers une série d'autres sites qui vous attaquent.
- Souvent, le propriétaire du site Web ne sait pas que ce dernier est compromis.

## 4 – Les pirates se fauillent pendant que vous surfez sur Internet

---



### ■ Redirection 301 ou 302

- Il n'est pas rare de voir des personnes malintentionnées recourir au détournement d'URL. Elles utilisent les redirections 302 volontairement pour orienter les pages vers leur propre contenu.

### ■ Interception de clic

- Ces méthodes utilisent des scripts non autorisés pour modifier les gestionnaires d'événements d'un site Web, pirater le clic et le curseur de la souris de l'utilisateur et le rediriger vers un autre élément ou section d'une page Web (rémunération pour publicité).

## 4 – Les pirates se faufilent pendant que vous surfez sur Internet



**301**  
Permanent\* Everyone is redirected to the new location, Page B.

**302**  
Temporary\* Visitors and bots are redirected. Juice is left behind.

The diagram shows two rows. The top row, labeled '301 Permanent', features icons of people and a pitcher of juice on both sides of a document icon labeled 'A' with an arrow pointing to a document icon labeled 'B'. The bottom row, labeled '302 Temporary', features icons of people and a pitcher of juice on both sides of a document icon labeled 'A' with an arrow pointing to a document icon labeled 'B'. The juice pitcher icon in the 302 row is empty, while it is full in the 301 row.

## 4 – Les pirates se fauillent pendant que vous surfez sur Internet

---



1

Assurez-vous d'installer toutes les mises à jour de votre navigateur ou utilisez un navigateur qui se met à jour automatiquement.



Les conseils d'Alain

## 5 – Les pirates peuvent infiltrer vos appareils intelligents.

---



- **Votre appareil intelligent est essentiellement un ordinateur.**
  - Tout ce qui est connecté à Internet dans votre maison, de votre réfrigérateur à votre système de climatisation peut être piraté.
    - Des pirates ont détourné un interphone de surveillance pour bébé et communiquer avec le bambin.
    - Il a été également démontré qu'il est facile d'allumer la caméra d'un téléviseur intelligent afin d'espionner les habitants d'une demeure.

## 5 – Les pirates peuvent infiltrer vos appareils intelligents.

### IP camera default password list

Camera Manufacturer	Username	Password
3xLogic	admin	12345
ACTi	Admin	123456
ACTi	admin	123456
Amcrest	admin	admin
American Dynamics	admin	admin
American Dynamics	admin	9999
Arecont Vision	admin	<blank>
AvertX	admin	1234
Avigilon	admin	admin
Avigilon	administrator	<blank>
Axis	root	pass
Axis	root	<blank>
Basler	admin	admin
Bosch	<blank>	<blank>

## 5 – Les pirates peuvent infiltrer vos appareils intelligents.



1

Lors de la configuration d'appareils intelligents, changez **toujours** le mot de passe par défaut.

2

Faites **toujours** les mises à jour recommandées pour vos appareils.



Les conseils d'Alain

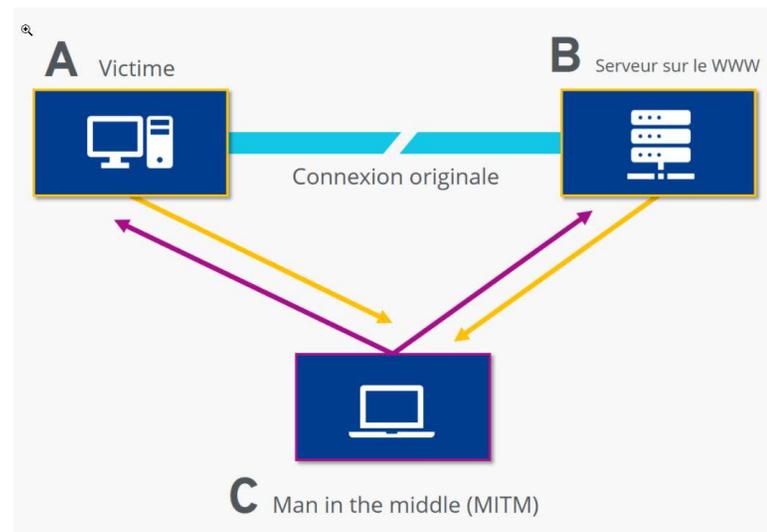
## 6 – Les pirates espionnent les réseaux Wi-Fi publics gratuits.

---



- **Même si vous êtes connecté à un réseau public légitime.**
  - Une attaque de l'intercepteur, aussi appelée '**attaque de l'homme du milieu**', peut permettre à des pirates d'intercepter les communications sans que vous puissiez vous douter que le canal a été compromis.

## 6 – Les pirates espionnent les réseaux Wi-Fi publics gratuits.



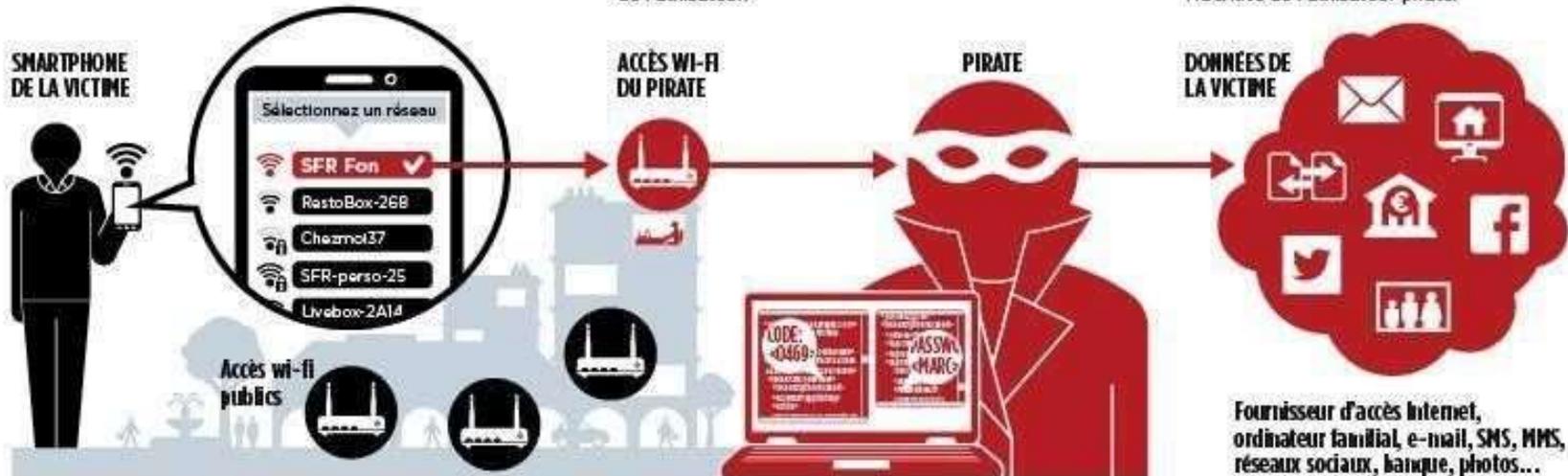
## 6 – Les pirates espionnent les réseaux Wi-Fi publics gratuits.

### De vrais-faux réseaux wi-fi pour pirater un smartphone

Un utilisateur recherche un réseau wi-fi ouvert dans un lieu public.

Un pirate propose un faux réseau public qui lui permet d'enregistrer les données de l'utilisateur.

Le pirate intercepte les mots de passe et les identifiants. Il peut maintenant usurper l'identité de l'utilisateur piraté.



## 6 – Les pirates espionnent les réseaux Wi-Fi publics gratuits.

- 1 Évitez si possible le Wi-Fi public, en particulier les réseaux non sécurisés sans mot de passe.
- 2 Inscrivez-vous à un service de réseau privé virtuel (VPN).
- 3 Si vous utilisez un service Wi-Fi public, évitez les transactions financières.
- 4 Utilisez une extension HTTPS pour crypter vos communications.



Les conseils d'Alain

## 7 – Les pirates vous attirent avec des vidéos ‘choquantes’

---

- Un ami vient de publier une vidéo d’un animal incroyable trouvé en Afrique.
- Si vous cliquez sur le lien, vous êtes invité à télécharger un lecteur multimédia qui installera des logiciels malveillants.

## 7 – Les pirates vous attirent avec des vidéos ‘choquantes’



1

Saisissez le titre de la vidéo dans votre barre de recherche et voyez si elle est sur un site de lecteur vidéo officiel. S’il s’agit d’une arnaque, quelqu’un l’aura déjà signalée.



Les conseils d’Alain

## 8 – Les pirates profitent des fautes de frappe

---

### ■ Les faux sites avec des URL légèrement modifiées.

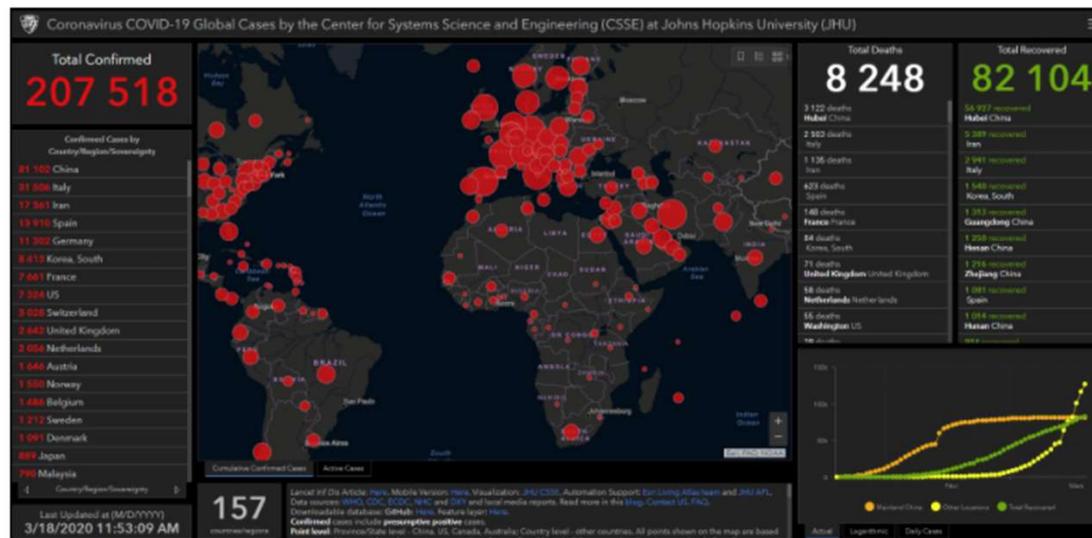
- Comme **micrososft.com** ou **chse.com** ressemblent aux vraies adresses et aux sites que vous voulez visiter. Ils sont conçus pour voler vos données ou installer des logiciels malveillants.

## 8 – Les pirates profitent des fautes de frappe

Des chercheurs en informatique nous ont avertis au début du mois de mars que près de **50% des noms de domaines utilisant coronavirus** sont à risque d'infecter notre ordinateur ou notre téléphone intelligent.

L'un de sites qu'il faut À TOUT PRIX ÉVITER est **corona-virus-map.com**.

Ce site nous invite à installer une carte sur l'évolution de la maladie. Le piège est que cette carte est identique à **la vraie carte** utilisée par certains médias et qui a été créée par l'Université Johns-Hopkins à Baltimore aux États-Unis.



*Des pirates informatiques s'amusent à créer de fausse version de la carte de l'Université Johns-Hopkins sur la Covid-19.*

## 8 – Les pirates profitent des fautes de frappe

---



1

Surveillé attentivement l'orthographe.



Les conseils d'Alain

## 9 – Les pirates déchiffrent votre mot de passe sur des sites ' faciles'

---

■ **Il est prouvé que la majorité des gens utilisent le même mot de passe pour plusieurs sites Web.**

- Il est donc facile pour un pirate de s'introduire dans un forum de randonnée par exemple, obtiendra votre adresse courriel et votre mot de passe, puis accédera à votre compte courriel avec le même mot de passe.
- Si cela fonctionne, il cherchera des courriel de banque, accédera à votre compte en essayant le même mot de passe.

## 9 – Les pirates déchiffrent votre mot de passe sur des sites ' faciles'

Créez un mot de passe robuste [www.pensezcybersecurite.gc.ca/fr/accueil](http://www.pensezcybersecurite.gc.ca/fr/accueil)



## 9 – Les pirates déchiffrent votre mot de passe sur des sites 'faciles'

La double identification

<https://youtu.be/Zfz2rjbWTSI>



## 9 – Les pirates déchiffrent votre mot de passe sur des sites faciles.



1

Utilisez l'authentification à deux facteurs, une fonctionnalité simple.

2

En plus de votre mot de passe, un site peut vous demander de saisir un code généré aléatoirement envoyé sur votre cellulaire pour vous connecter.



Les conseils d'Alain

## 10 – Les pirates peuvent pénétrer dans les routeurs au cryptage WEP

---

- De nombreux routeurs reposent encore sur un type de cryptage appelé WEP (Wired Equivalent Privacy).
- Ces routeurs peuvent facilement être piratés avec des logiciels disponibles à grande échelle.

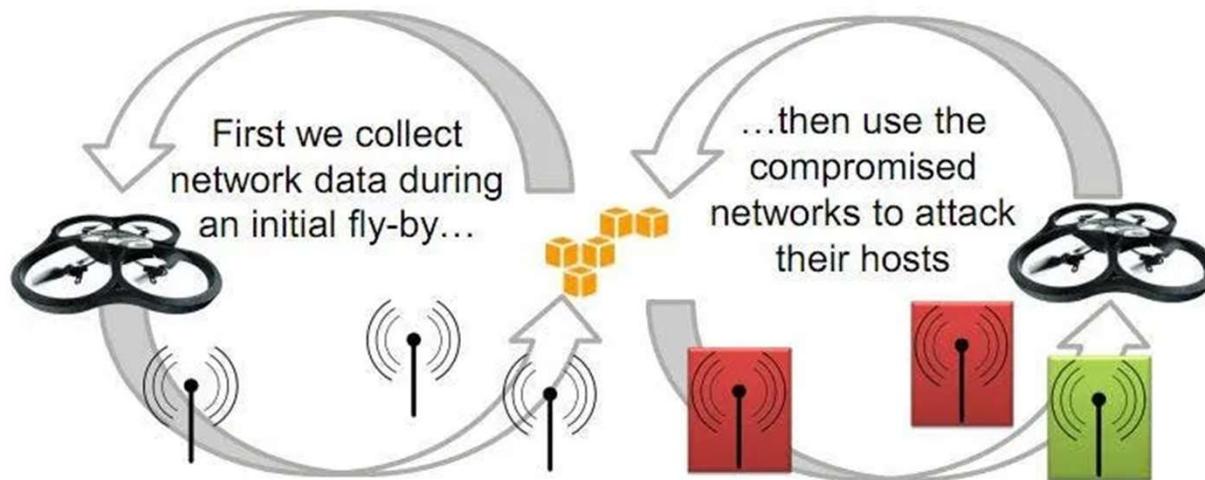
## 10 – Les pirates peuvent pénétrer dans les routeurs au cryptage WEP.



### Un piratage en trois voyages

La méthode d'attaque proposée se déroule en plusieurs étapes.

1. D'abord le drone va effectuer un vol de reconnaissance pour repérer et enregistrer les informations sur tous les réseaux sans-fil que le pirate pourrait cracker (SSID, type de cryptage, adresses MAC...). Il s'agit typiquement de réseaux ouverts, ou encore protégés par WEP ou certaines variantes du WPA. Le pirate contrôle le drone depuis un ordinateur et tous ses déplacements sont enregistrés grâce au GPS.



2. Lors d'un deuxième voyage, le drone peut automatiquement retrouver les points d'accès vulnérables et, cette fois, tenter de casser leur cryptage. Par un souci évident de discrétion et d'autonomie – l'AR Drone n'est guère capable de voler plus d'un quart d'heure –, les chercheurs estiment que le drone devrait effectuer une bonne partie de son travail posé, moteurs éteints.

La puissance de calcul de l'ordinateur qu'il embarque étant très limitée, il lui est impossible de casser la protection d'un point d'accès, qui réclame du calcul intensif.

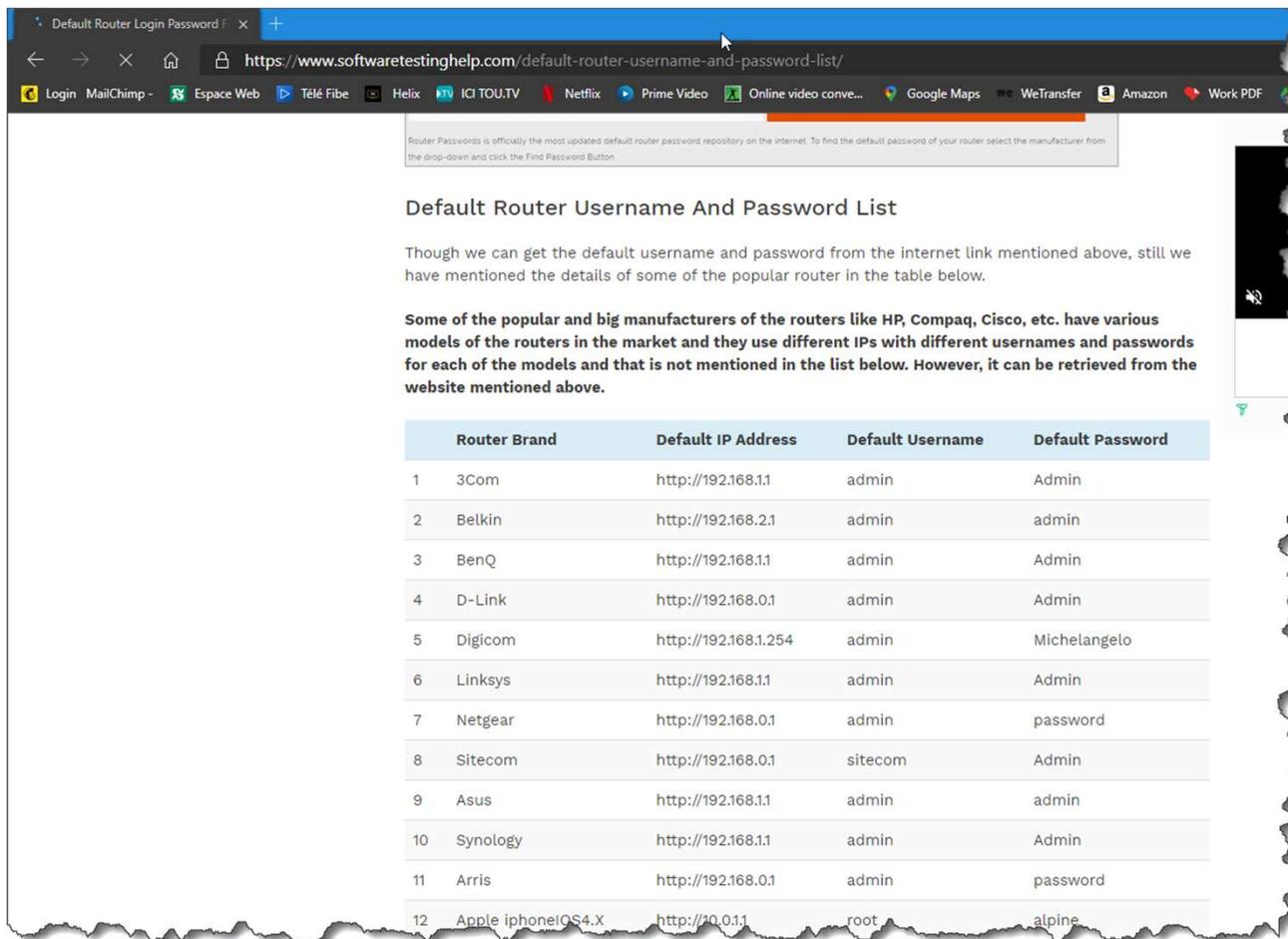
3. Un troisième voyage permet au drone d'attaquer et d'infecter effectivement les ordinateurs des réseaux dont il a désormais la clé, en utilisant des *exploits* connus des hackers, que les chercheurs décrivent également dans leur article. Ensuite, le drone peut revenir à plusieurs reprises pour donner de nouvelles commandes aux malheureux ordinateurs qu'il a asservis...

## Cryptage WEP remplacé par cryptage WPA.

- Aujourd'hui, pour protéger nos données, notre ordinateur et notre modem Internet communiquent dans un langage codé, appelé WPA. Ce protocole permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité.
- Pour se comprendre mutuellement, à l'instant où on les allume, ils s'envoient une clé, sorte de mode d'emploi pour déchiffrer leur langage codé. Eux seuls peuvent alors se comprendre et leur communication reste secrète.
- Mais tout repose sur l'envoi de cette clé. Si elle est interceptée par un pirate, ce dernier peut alors comprendre tout ce qui se dit.
- Et c'est là qu'intervient les problèmes.



## 10 – Les pirates peuvent pénétrer dans les routeurs.



Router Passwords is officially the most updated default router password repository on the internet. To find the default password of your router select the manufacturer from the drop-down and click the Find Password Button.

### Default Router Username And Password List

Though we can get the default username and password from the internet link mentioned above, still we have mentioned the details of some of the popular router in the table below.

**Some of the popular and big manufacturers of the routers like HP, Compaq, Cisco, etc. have various models of the routers in the market and they use different IPs with different usernames and passwords for each of the models and that is not mentioned in the list below. However, it can be retrieved from the website mentioned above.**

	Router Brand	Default IP Address	Default Username	Default Password
1	3Com	http://192.168.1.1	admin	Admin
2	Belkin	http://192.168.2.1	admin	admin
3	BenQ	http://192.168.1.1	admin	Admin
4	D-Link	http://192.168.0.1	admin	Admin
5	Digicom	http://192.168.1.254	admin	Michelangelo
6	Linksys	http://192.168.1.1	admin	Admin
7	Netgear	http://192.168.0.1	admin	password
8	Sitecom	http://192.168.0.1	sitecom	Admin
9	Asus	http://192.168.1.1	admin	admin
10	Synology	http://192.168.1.1	admin	Admin
11	Arris	http://192.168.0.1	admin	password
12	Apple iPhone/iOS4.X	http://10.0.1.1	root	alpine

## 10 – Les pirates peuvent pénétrer dans les routeurs au cryptage WEP.

1

Assurez-vous que votre routeur utilise le cryptage WPA, voir WPA2 (Wi-Fi Protected Access).

2

Modifiez votre mot de passe Wi-Fi prédéfini.



Les conseils d'Alain

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance.

---



### ■ Vous pouvez recevoir un faux avertissement:

- De la part de votre banque
- De votre compagnie de carte de crédit
- D'une confirmation de commande d'un détaillant
- Une invitation à rejoindre un réseau social

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance



De : Account Maintenance

Oct. 2, 08:50

A : Cecile Keller

Objet : eBay account update



Dear eBay member,

We regret to inform you that your eBay account could be suspended if you don't update your information.

To resolve this problem, please visit the link below and enter your account information.

<http://signin.ebay.com@10.19.32.4/>

eBay Support Team

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance

De : Account Maintenance  
A : Cecile Keller  
Objet : eBay account update

Oct. 2, 08:50



Dear eBay member,

We regret to inform you that your eBay account could be at risk if you don't update your information.

To resolve this problem, please visit the link below to update your account information.

<http://signin.ebay.com@10.19.32.4/>

eBay Support Team

Vous pouvez voir le véritable lien en survolant avec la souris et déduire qu'il s'agit de harponnage car l'URL est suspect !

Si vous cliquez sur le lien et vous entrez vos informations, votre compte ebay risque d'être détourné et utilisé de façon frauduleuse.

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance



De : Service Communication

Oct. 1, 12:38

A : undisclosed-recipients

Objet : Newsletter FINMA

---

Cher(e) client(e),

Vous avez été désinscrit(e) de la newsletter de l'Autorité Fédérale de Surveillance des Marchés Financiers.

Pour vous réinscrire, veuillez cliquer [ici](#).

Cordialement,

FINMA  
Service Communication

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance

De : Service Communication

A : undisclosed-recipients

Objet : Newsletter FINMA

Cher(e) client(e),

Vous avez été désinscrit(e) de la newsletter de l'Auto  
Surveillance des Marchés Financiers.

Pour vous réinscrire, veuillez cliquer [ici](#).

Cordialement,

FINMA

Service Communication

Oct. 1, 12:38

Si vous n'êtes pas inscrit à cette  
Newsletter, vous devez être  
vigilant.

**Vérifier toujours l'URL avant de  
cliquer !**

S'il s'agit d'un courriel de  
harponnage, un programme  
malveillant pourrait être  
téléchargé.

## 11 – Les pirates usurpent l'identité d'entreprises digne de confiance.

- 1 La plupart des entreprises ne vous demandent jamais les informations de votre compte.
- 2 Vous pouvez parfois repérer ces arnaques en appuyant sur Répondre à tous et en cherchant des adresse étranges.
- 3 Les fautes d'orthographe sont de bons indicateurs.
- 4 Vérifiez que le courriel a été envoyé uniquement à vous.



Les conseils d'Alain

## 12 – Les pirates commencent par débiter de petits montants

---



- **Le logiciel Cyberthieves** peut tester un numéro de carte volée en débitant une petite somme de moins de 10\$ pour voir si quelqu'un le remarque.
- À la mi-février, des voleurs ont versé 1,75 million de dollars de l'université Harvard à une source non autorisée.

## 12 – Les pirates commencent par débiter de petits montants.

---

### Logiciels malveillants appelés Lokibot

- Également connu sous le nom de Lokibot, Loki PWS et Loki-bot, ce malware cheval de Troie cible les systèmes d'exploitation Windows et Android. Il est conçu pour infiltrer les systèmes et voler des informations sensibles telles que vos noms d'utilisateur et mots de passe, votre portefeuille de crypto-monnaie et d'autres informations d'identification.
- Signalé pour la première fois en 2015, il est devenu l'un des voleurs d'informations les plus répandus. En raison de son interface et de sa base de code simples, il est utilisé par un large éventail de cybercriminels, y compris des opérateurs moyennement qualifiés qui sont nouveaux dans la cybercriminalité.

**Note:** Ce programme est polymorphe, ce qui signifie qu'il peut changer sa représentation à chaque téléchargement.



## 12 – Les pirates commencent par débiter de petits montants.

---



1

Vérifiez vos transactions en ligne régulièrement, voire quotidiennement.

2

Si vous constatez un retrait que vous n'avez pas effectué, signalez-le immédiatement à l'émetteur de votre carte.



Les conseils d'Alain

## 13 – Les pirates peuvent pirater votre guichet automatique

---

### ■ Les escrocs installent des skimmers pour voler les informations de votre carte.

- Une caméra cachée ou une fine pellicule appliquée sur le clavier capture votre NIP.
- Les escrocs ont même un moyen de cibler les guichets automatiques à distance.



## 13 – Les pirates peuvent pirater votre guichet automatique.

### VOLS AUX DISTRBUTEURS



- ♦ Sur cette première diapo, vous apercevez un individu apparemment occupé à retirer de l'argent de ce distributeur automatique de billets (DAB).

## 13 – Les pirates peuvent pirater votre guichet automatique



1

Utilisez les guichets automatiques directement dans les banques.

2

Chaque fois que vous utilisez un guichet automatique, donnez un petit coup sur la zone où la carte doit être insérée pour s'assurer que tout est sécuritaire et fait partie de la machine.



Les conseils d'Alain

## ■ Les applications volent des informations confidentielles.

- Ils vous abonnent à des services premium.
- Vous téléchargez la version gratuite d'un jeu payant. Elle vous demande toutes sortes d'accès et vous dites 'oui, oui, oui' à toutes les autorisations. La première chose que vous saurez, c'est que votre argent a été volé.



## 14 – Les pirates comptent sur de fausses versions gratuites d'applications populaires.



1

Avant d'installer une application, vérifiez les commentaires et le nombre de téléchargements. Les pirates peuvent faire de fausses évaluations positives, mais ils ne peuvent pas empêcher les avertissements sur l'application.

2

La plupart des fausses applications doivent être téléchargées directement à partir d'un site Web. Assurez-vous de les télécharger à partir d'une plateforme officielle.



Les conseils d'Alain



- Avec le Wi-Fi activé, votre appareil essaiera constamment de se connecter à des réseaux connus.
- Les pirates peuvent facilement les identifier et mettre en place des réseaux malveillants qui se feront passer pour eux.

## 15 – Les pirates aiment que vous laissez toujours le Wi-Fi activé

---



1

Prenez l'habitude de désactiver votre Wi-Fi chaque fois que vous quittez votre domicile.



Les conseils d'Alain

## 16 – Les pirates vous trompent avec de fausses mises à jour.

---

- Vous devriez mettre à jour votre logiciel.
- Les pirates peuvent vous envoyer des fausses mises à jour qui installeront des programmes malveillants sur votre ordinateur.

## 16 – Les pirates vous trompent avec de fausses mises à jour.



1

Si vous recevez un message concernant une mise à jour, accédez au site Web du fournisseur du logiciel et vérifiez si elle est présente sur le site.

2

Essayez de fermer votre navigateur Web pour voir si la fenêtre contextuelle disparaît. Si tel est le cas, il s'agit probablement d'un faux message.



Les conseils d'Alain

## 17 – Les pirates peuvent craquer des détaillants soi-disant sûrs.



- Les experts affirment que les grandes entreprises continueront d'être piratées jusqu'à ce qu'elles soient mieux outillées pour protéger leurs données.
- Les pirates vendent vos informations sur le marché noir.
- Les criminels les utilisent ensuite pour fabriquer des cartes contrefaites.

## 17 – Les pirates peuvent craquer des détaillants soi-disant sûrs.

---



1

Ne sauvegardez pas vos informations bancaires lorsque vous effectuez des achats en ligne.

2

Faites vos achats en tant qu'invité lorsque vous le pouvez.



Les conseils d'Alain

## 18 – Conseils de sécurité d'anciennes victimes de piratage.

---

- Essayez de ne pas demander de cartes de crédit en ligne. Votre numéro de sécurité sociale sera requis et une fois qu'il est sur Internet, il s'y trouve pour toujours.
- Lorsque vous vous connectez à un compte en ligne, ne cochez jamais la case ' Se souvenir de moi'.
- Envisagez de geler votre cote de crédit auprès des bureaux de crédit et de la faire dégeler lorsque vous en aurez besoin.

# QUESTIONS ?

