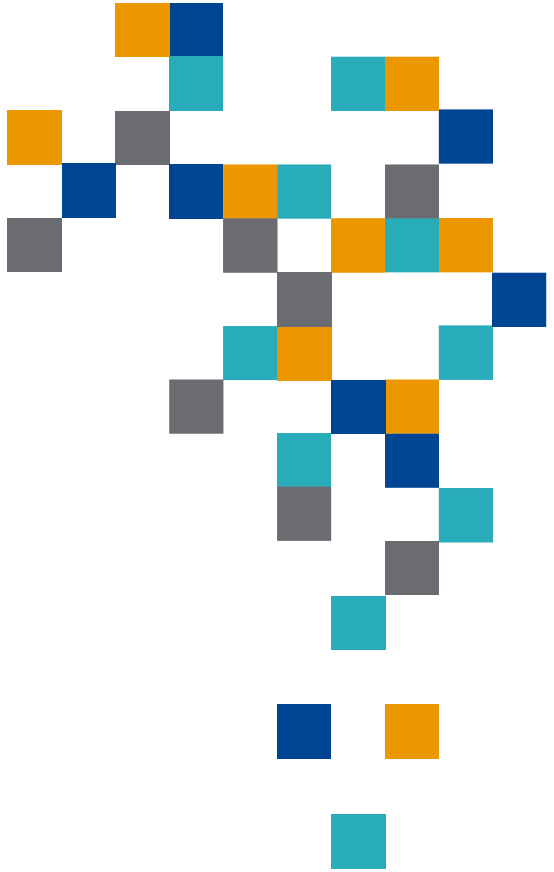
FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE



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

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

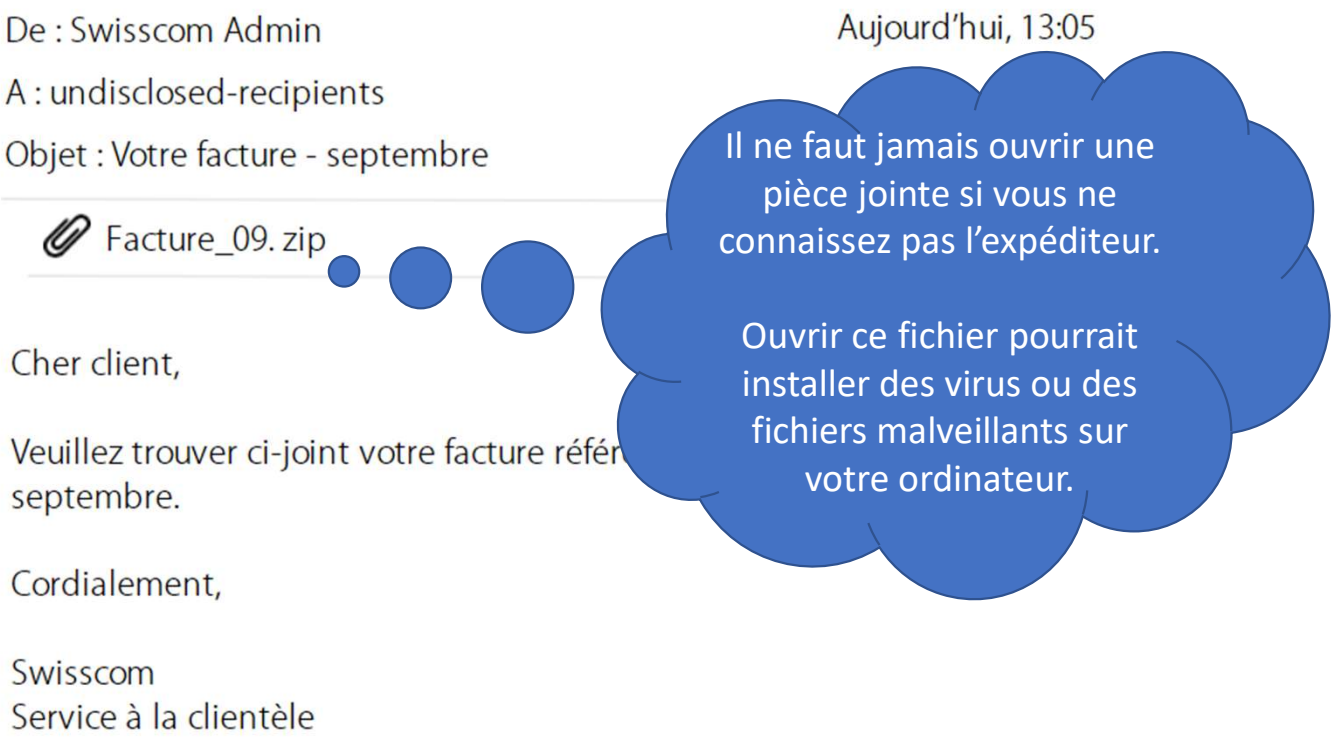
Cher client,

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

Cordialement,

Swisscom
Service à la clientèle

1 – Exemples de courriel dangereux.



1 – Exemples de courriel dangereux.

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/

1 – Exemples de courriel dangereux.

De : AFC

A : Cécile Keller

Objet : Message important de l'Administration Fiscale

Si ce message n'apparaît pas directement, veuill[illegible] cli

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 mois sur cet e-mail : 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 chev
somme de quinze millions de
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 transf
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 mois sur cet e-mail : 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 ?

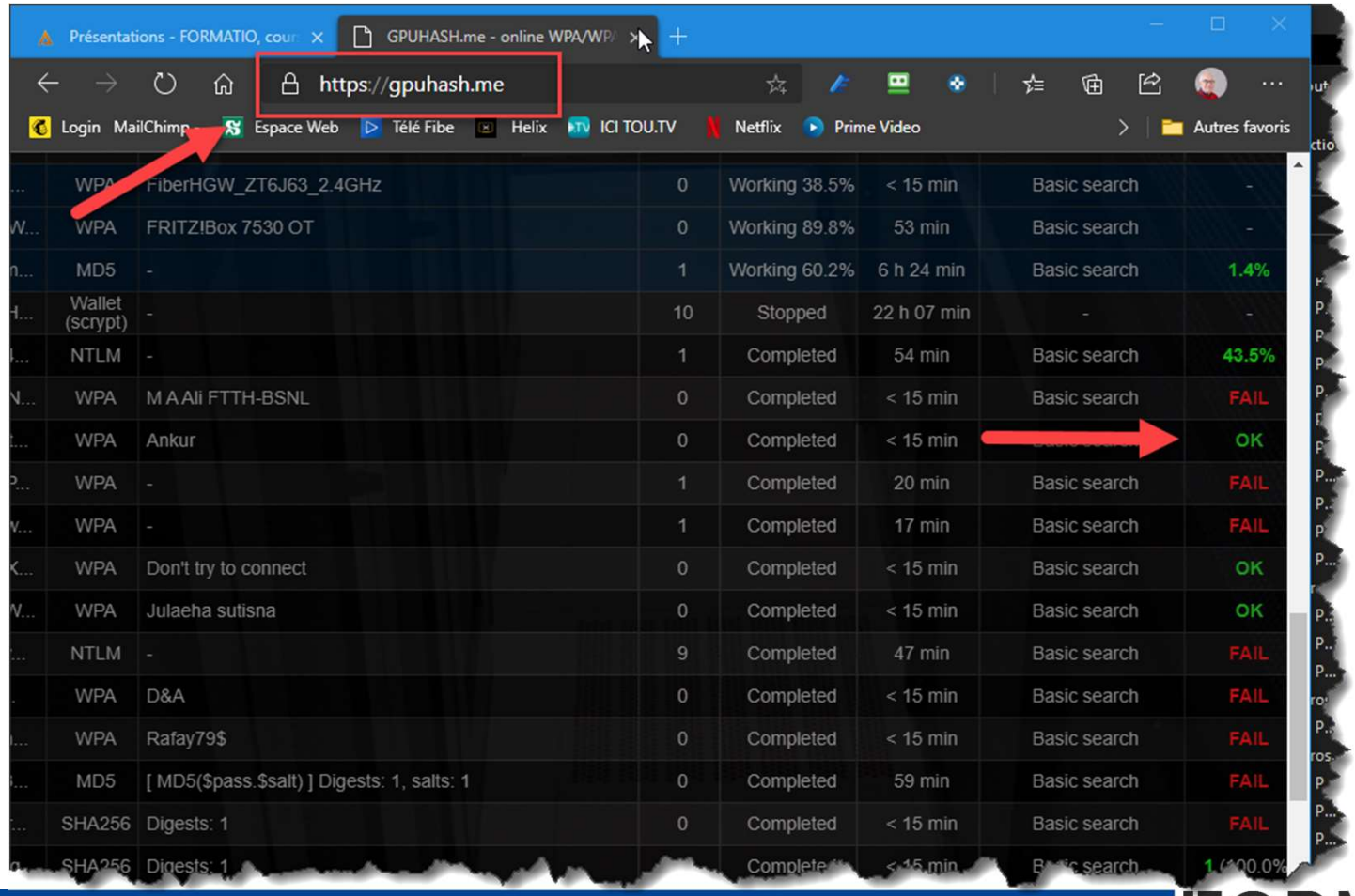
1. Utilisation d’image d’une entreprise connue
2. Caractères menaçant ou alarmiste
3. Promesses d’argent facile
4. Fautes d'orthographe ou de syntaxe
5. Adresses de courriel et URL suspects
6. Pièces jointes suspectes

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.



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

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.

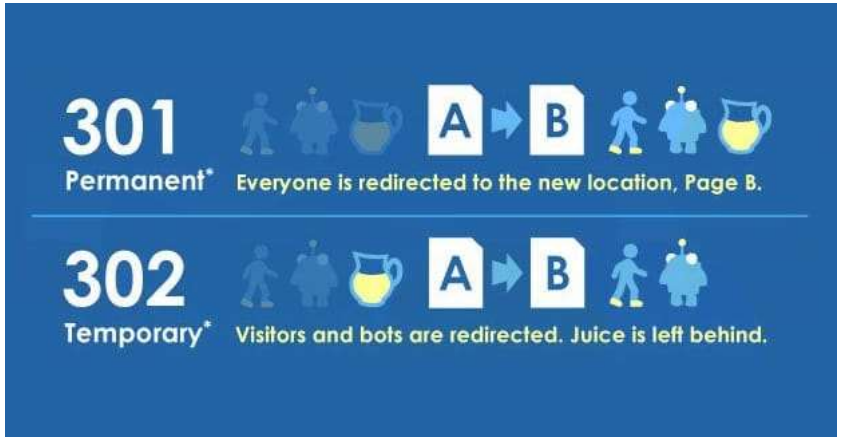
Redirection 301 ou 302

- 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



4 – Les pirates se faufilent 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 détourner 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.

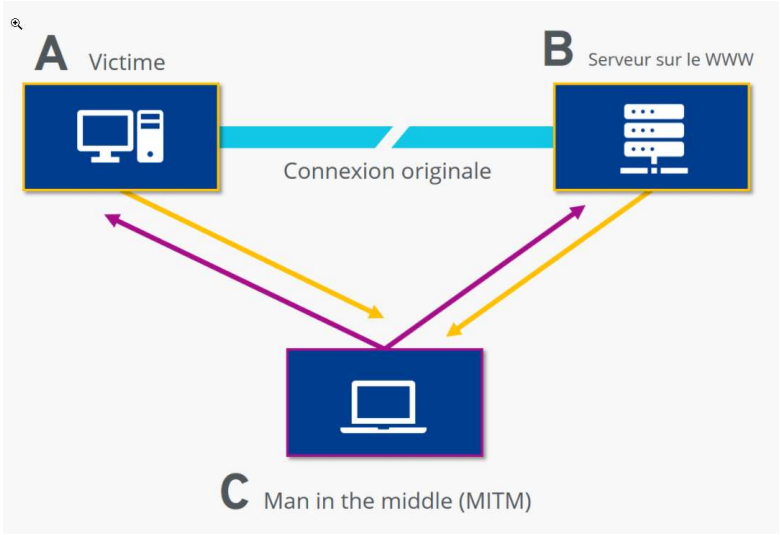
Les conseils d'Alain

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

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

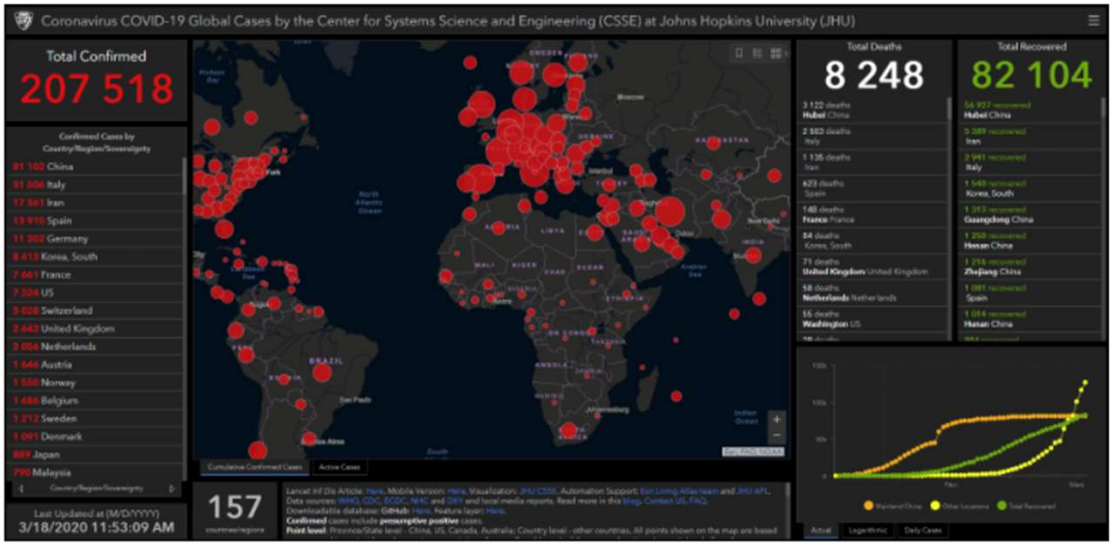
- **Les faux sites avec des URL légèrement modifiées.**
  - Comme **micrososft.com** ou **chse.com** ressemblent aux vraies adresses et aux sites que vous voulez visiter. Ils sont conçus pour voler vos données ou installer des logiciels malveillants.

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, accèdera 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

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 - Cryptage WEP remplacé par cryptage WPA.

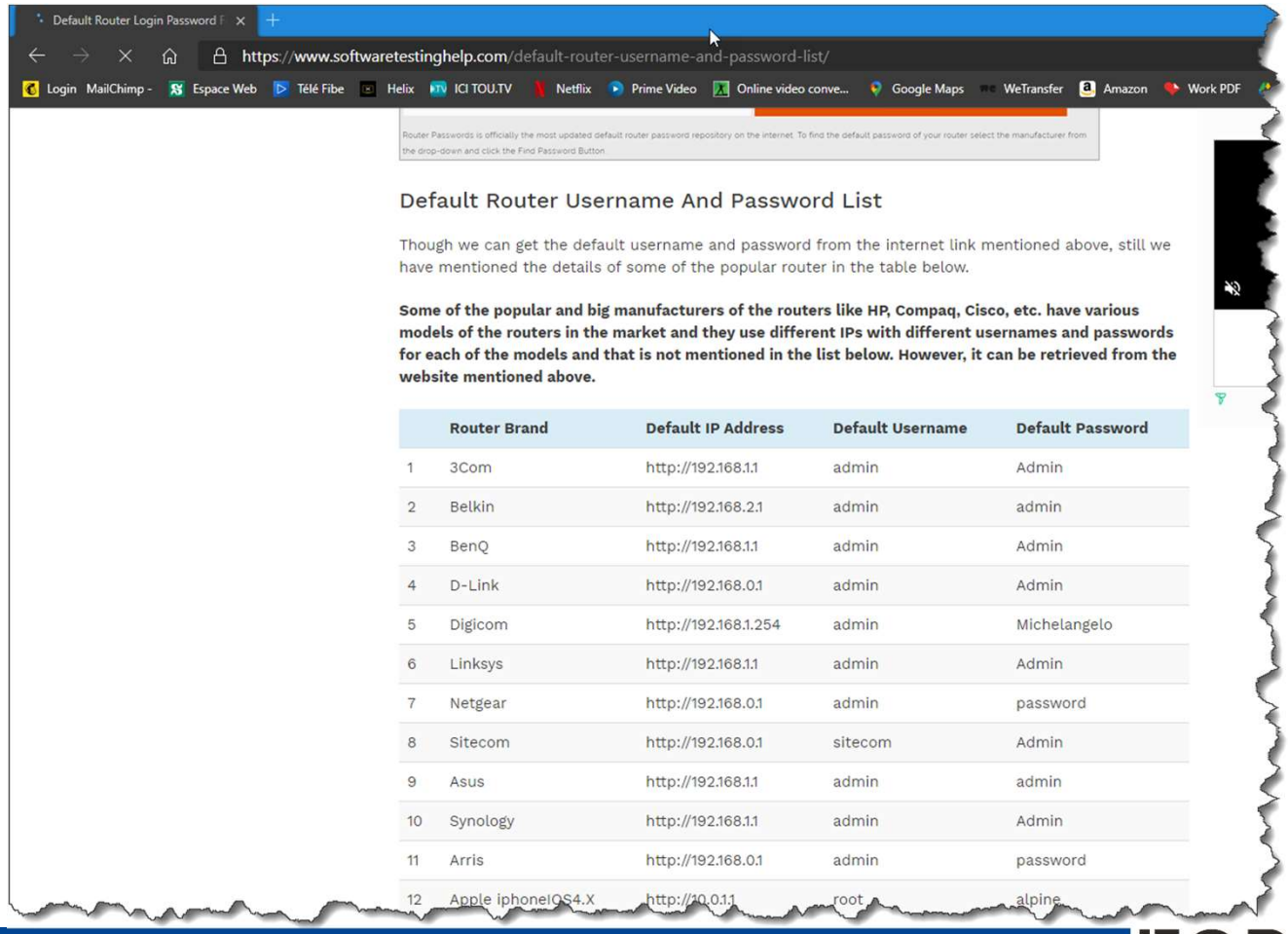
- Aujourd'hui, pour protéger nos données, notre ordinateur et notre modem Internet communiquent dans un langage codé, appelé WPA. Ce protocole permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité.

- 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 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 iphoneIOS4.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

FIN DE LA PREMIÈRE PARTIE