



CyberPeace
Institute

SENSIBILISATION À LA CYBERSÉCURITÉ

FORMATION À LA CYBERSÉCURITÉ ET
À LA SÉCURITÉ DE L'INFORMATION

cyber
peace
builders.

INTRODUCTION

Cette formation présente les cybermenaces auxquelles nous sommes confrontés sur Internet.

Objectifs de la formation:

- Connaître les cybermenaces actuelles
- Apprendre à détecter une cyberattaque et à y faire face
- Assimiler des astuces et les meilleures pratiques
- Tirer des enseignements à partir de cas concrets



METTRE L'HUMAIN EN AVANT

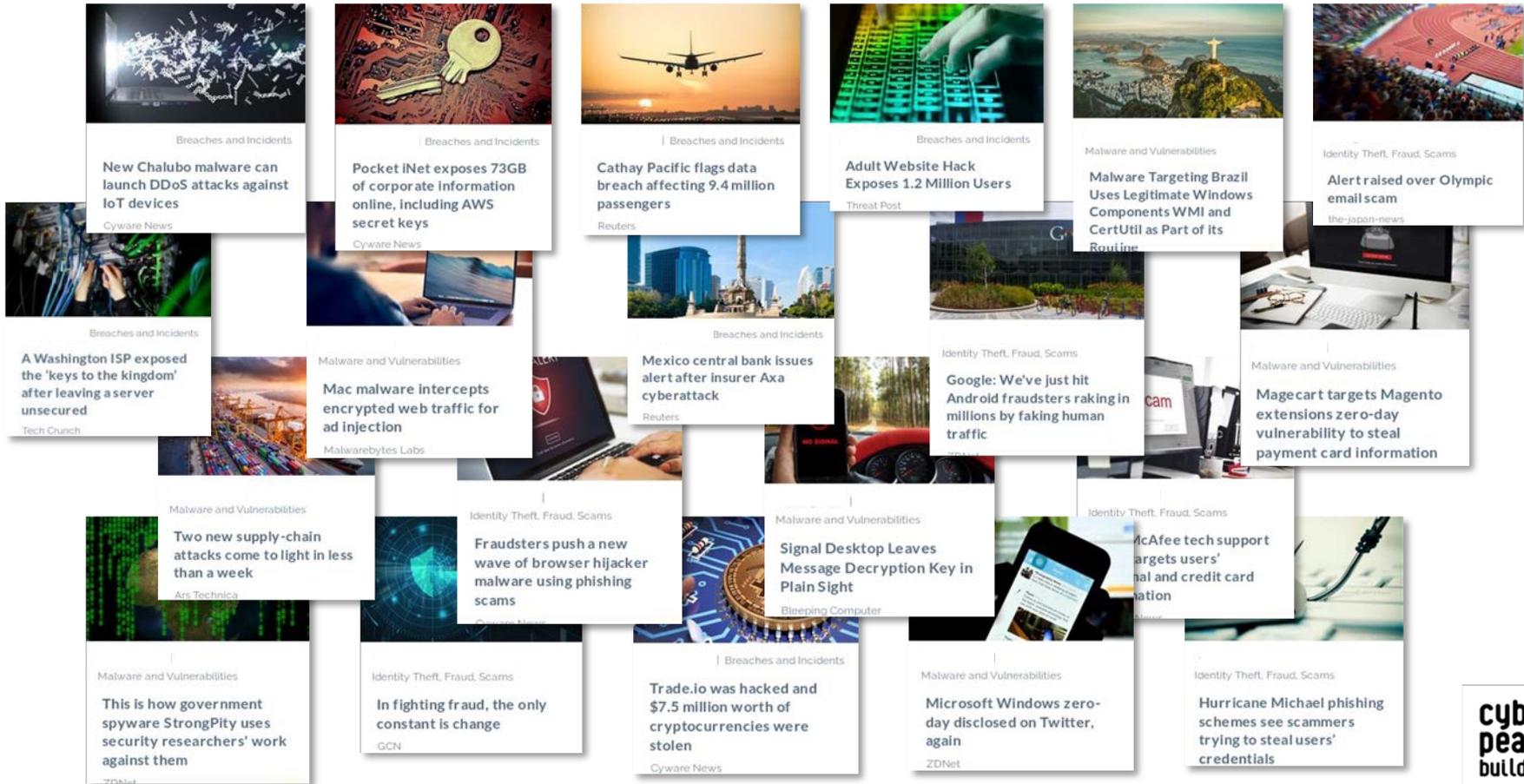


[HTTPS://WWW.YOUTUBE.COM/WATCH?V=UD-5LPULDNM](https://www.youtube.com/watch?v=UD-5LPULDNM)

LES CYBERMENACES

INTRODUCTION

LES CYBERMENACES FONT LA UNE AU QUOTIDIEN



Breaches and Incidents
New Chalubo malware can launch DDoS attacks against IoT devices
Cyware News

Breaches and Incidents
Pocket iNet exposes 73GB of corporate information online, including AWS secret keys
Cyware News

Breaches and Incidents
Cathay Pacific flags data breach affecting 9.4 million passengers
Reuters

Breaches and Incidents
Adult Website Hack Exposes 1.2 Million Users
Threat Post

Malware and Vulnerabilities
Malware Targeting Brazil Uses Legitimate Windows Components WMI and CertUtil as Part of its Routine
the-japan-news

Identity Theft, Fraud, Scams
Alert raised over Olympic email scam
the-japan-news

Breaches and Incidents
A Washington ISP exposed the 'keys to the kingdom' after leaving a server unsecured
Tech Crunch

Malware and Vulnerabilities
Mac malware intercepts encrypted web traffic for ad injection
Malwarebytes Labs

Breaches and Incidents
Mexico central bank issues alert after insurer Axa cyberattack
Reuters

Identity Theft, Fraud, Scams
Google: We've just hit Android fraudsters raking in millions by faking human traffic
cam

Malware and Vulnerabilities
Magecart targets Magento extensions zero-day vulnerability to steal payment card information

Malware and Vulnerabilities
Two new supply-chain attacks come to light in less than a week
Ars Technica

Identity Theft, Fraud, Scams
Fraudsters push a new wave of browser hijacker malware using phishing scams
Bleeping Computer

Malware and Vulnerabilities
Signal Desktop Leaves Message Decryption Key in Plain Sight
Bleeping Computer

Identity Theft, Fraud, Scams
McAfee tech support targets users' email and credit card information
ZDNet

Malware and Vulnerabilities
This is how government spyware StrongPity uses security researchers' work against them
ZDNet

Identity Theft, Fraud, Scams
In fighting fraud, the only constant is change
GCN

Breaches and Incidents
Trade.io was hacked and \$7.5 million worth of cryptocurrencies were stolen
Cyware News

Malware and Vulnerabilities
Microsoft Windows zero-day disclosed on Twitter, again
ZDNet

Identity Theft, Fraud, Scams
Hurricane Michael phishing schemes see scammers trying to steal users' credentials
ZDNet

LES ACTEURS MALVEILLANTS ET LEURS INTÉRÊTS



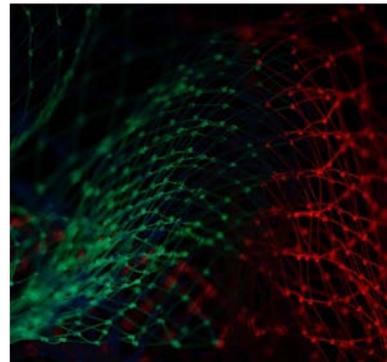
“Script Kiddies”

- Les organisations connues mondialement peuvent être vues comme un trophée
- Les attaques peuvent être menées par hasard voir par erreur
- Divertissement



Groupes criminels

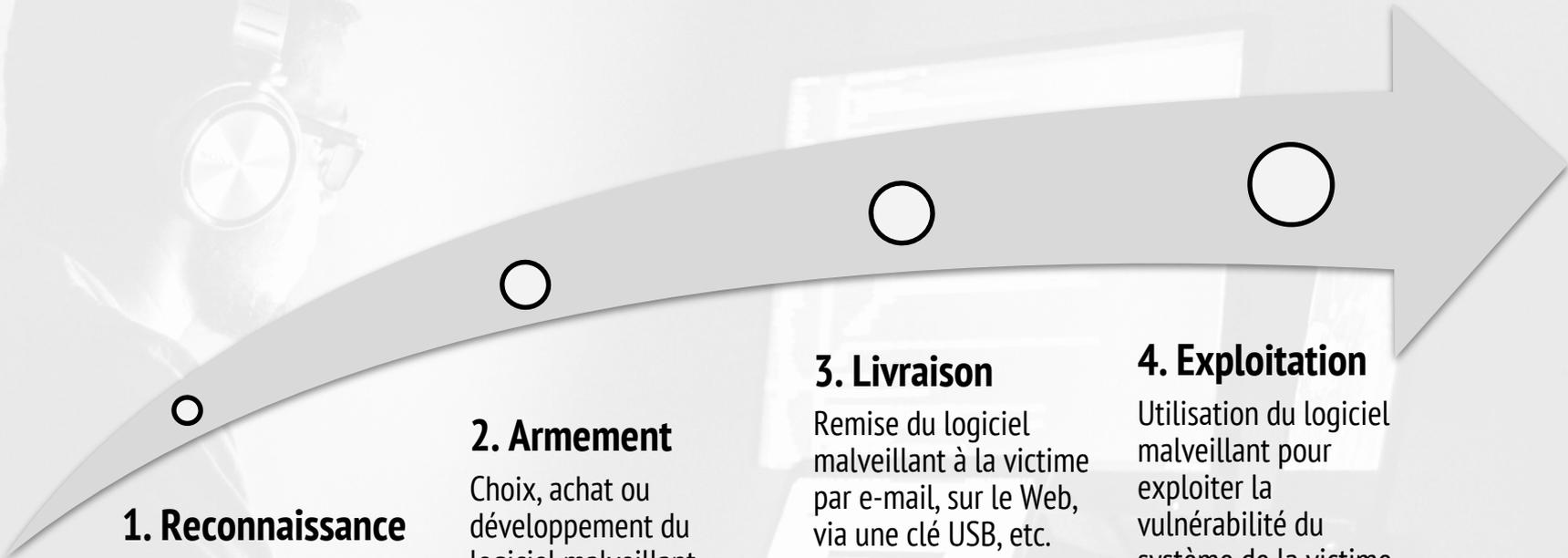
- Les organisations internationales, les organisations reconnues peuvent sembler riche
- Gain financier



États et groupes soutenus par des États

- Les organisations ou les individus détiennent des informations sensibles
- Les activités peuvent être considérées comme dérangeantes
- Espionnage, sabotage

LA “CYBER KILL CHAIN” SIMPLIFIÉE



1. Reconnaissance

Identification de la cible et de ses points faibles et planification de l'attaque, éventuellement par ingénierie sociale

2. Armement

Choix, achat ou développement du logiciel malveillant approprié

3. Livraison

Remise du logiciel malveillant à la victime par e-mail, sur le Web, via une clé USB, etc.

4. Exploitation

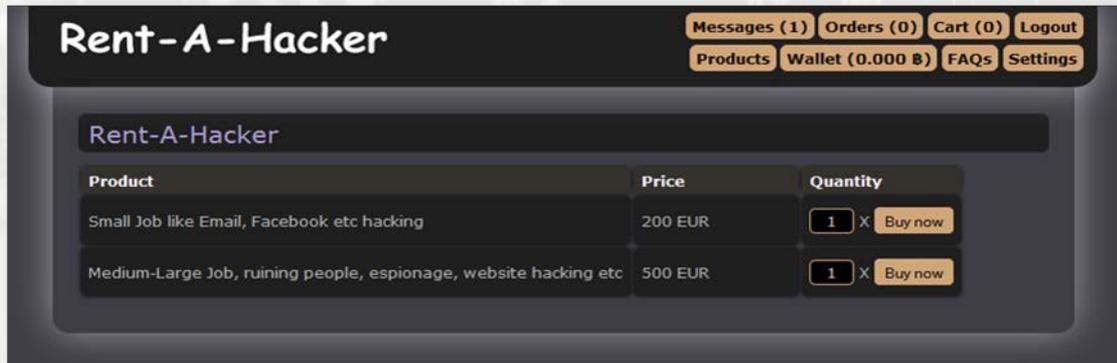
Utilisation du logiciel malveillant pour exploiter la vulnérabilité du système de la victime

LES CYBERMENACES

LA RECONNAISSANCE

EXEMPLE DE RECONNAISSANCE

- John Doe travaille pour une ONG à Bangkok et a accès à des données sensibles sur des détenus
- Evil Sandi travaille pour un gouvernement et aimerait mettre la main sur ces informations
- Solution : voler ces données en engageant un hacker sur le Dark Web



Rent-A-Hacker

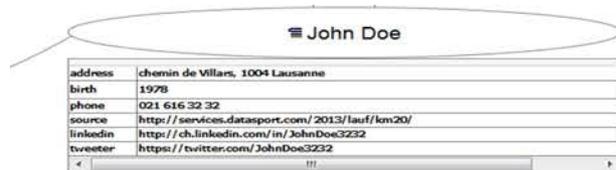
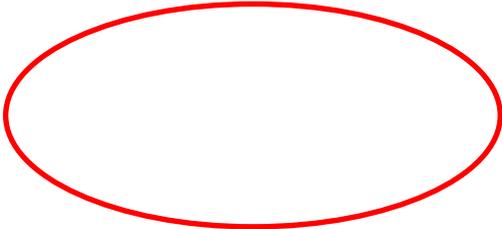
Messages (1) Orders (0) Cart (0) Logout
Products Wallet (0.000 B) FAQs Settings

Rent-A-Hacker

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR	1 X Buy now

CES SERVICES SONT FACILES À TROUVER SUR LE DARK WEB. IL SUFFIT DE FOURNIR AU HACKER L'IDENTITÉ DE LA CIBLE ET LE TOUR EST JOUÉ...

EXEMPLE DE RECONNAISSANCE

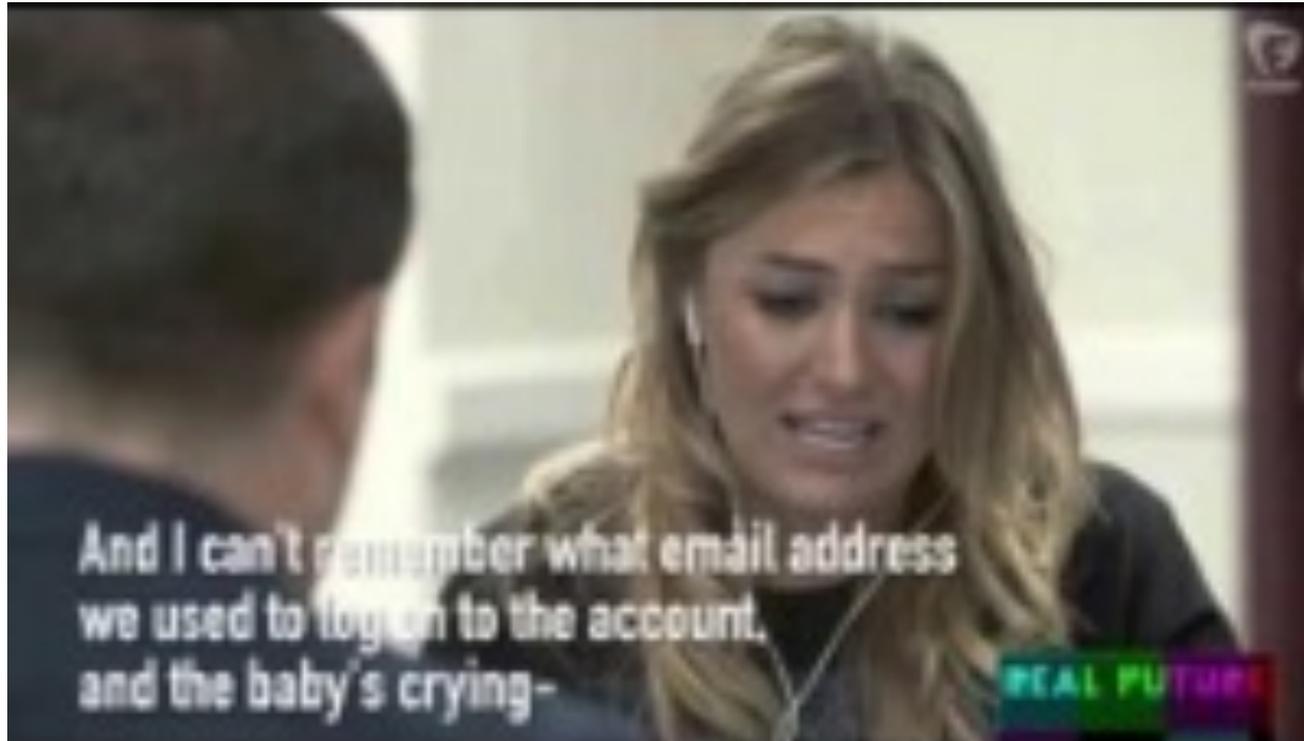


John Doe	
address	chemin de Villars, 1004 Lausanne
birth	1978
phone	021 616 32 32
source	http://services.datasport.com/2013/lauf/km20/
linkedin	http://ch.linkedin.com/in/JohnDoe3232
twitter	https://twitter.com/JohnDoe3232

**IL S'AGIT D'UN POINT D'ENTRÉES POUR
LE CYBER CRIMINEL**

SENSIBILISATION À LA SÉCURITÉ - L'ACCENT SUR L'ÉLÉMENT HUMAIN

11



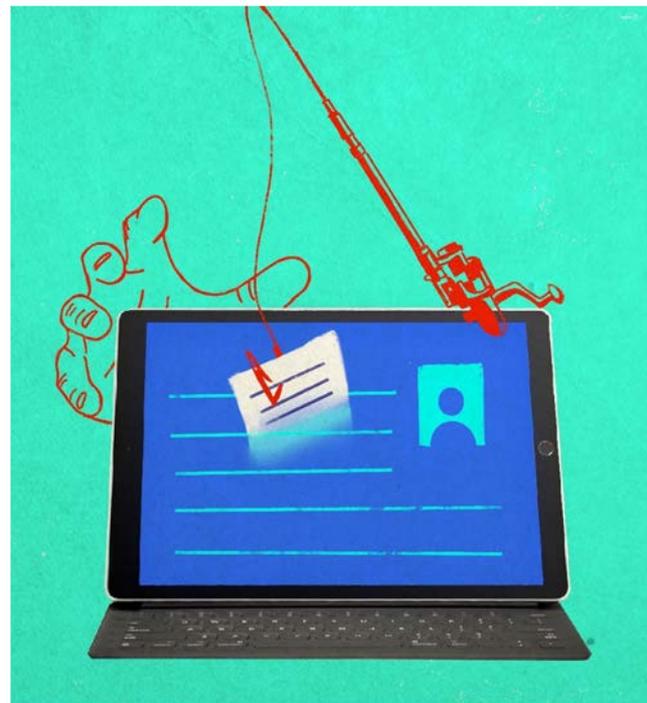
[HTTPS://WWW.YOUTUBE.COM/WATCH?V=LC7SCXVKQ00](https://www.youtube.com/watch?v=LC7SCXVKQ00)

LES CYBERMENACES

—
LA LIVRAISON ET LE PHISHING
(HAMEÇONNAGE)

LE FAMEUX «PHISHING» OU HAMEÇONNAGE

13

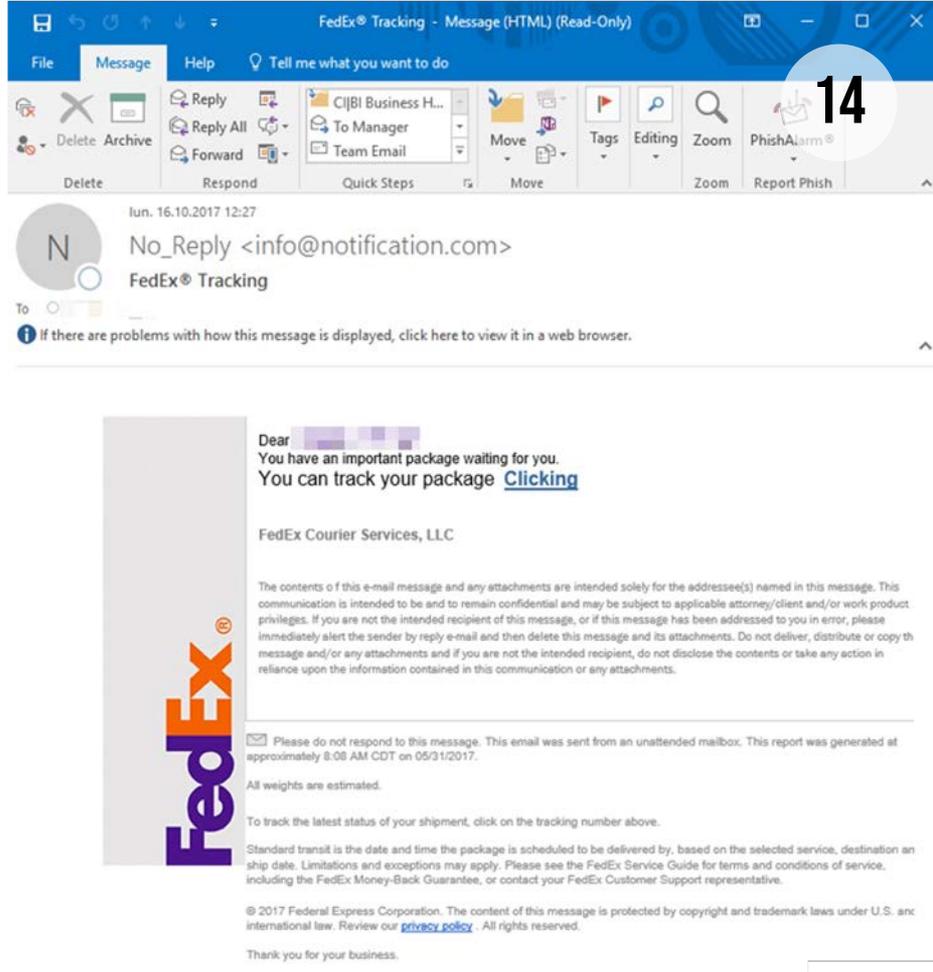


LA LIVRAISON

Les cyber-criminels peuvent se servir de différents vecteurs pour livrer un logiciel malveillant :

- E-mails, appels téléphoniques, clés USB, fax, lettres, etc.

L'e-mail reste le vecteur le plus couramment utilisé



The screenshot shows an email client interface with a blue header. The email is from "No_Reply <info@notification.com>" with the subject "FedEx® Tracking". The body of the email contains a phishing message:

Dear [redacted]
You have an important package waiting for you.
You can track your package [Clicking](#)

FedEx Courier Services, LLC

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney/client and/or work product privileges. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments.

Please do not respond to this message. This email was sent from an unattended mailbox. This report was generated at approximately 8:08 AM CDT on 05/31/2017.

All weights are estimated.

To track the latest status of your shipment, click on the tracking number above.

Standard transit is the date and time the package is scheduled to be delivered by, based on the selected service, destination and ship date. Limitations and exceptions may apply. Please see the FedEx Service Guide for terms and conditions of service, including the FedEx Money-Back Guarantee, or contact your FedEx Customer Support representative.

© 2017 Federal Express Corporation. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our [privacy policy](#). All rights reserved.

Thank you for your business.

The number 14 is circled in the top right corner of the screenshot.

ÉLÉMENTS À CONTRÔLER DANS LES E-MAILS (1/2)

L'expéditeur et le destinataire



Examiner l'adresse électronique de l'expéditeur plutôt que ses nom et prénom



S'il vous est demandé de fournir des informations sensibles par retour de courriel, bien vérifier l'adresse du destinataire



Prendre garde aux e-mails qui semblent provenir de grandes entreprises mais comportent une extension qui n'y correspond pas ou paraît étrange (@outlook.com, @gmail.com, @yahoo.fr, etc.)



ÉLÉMENTS À CONTRÔLER DANS LES E-MAILS (2/2)

Contenu du message



Demande d'informations personnelles et/ou confidentielles



Ton pressant ou menaçant



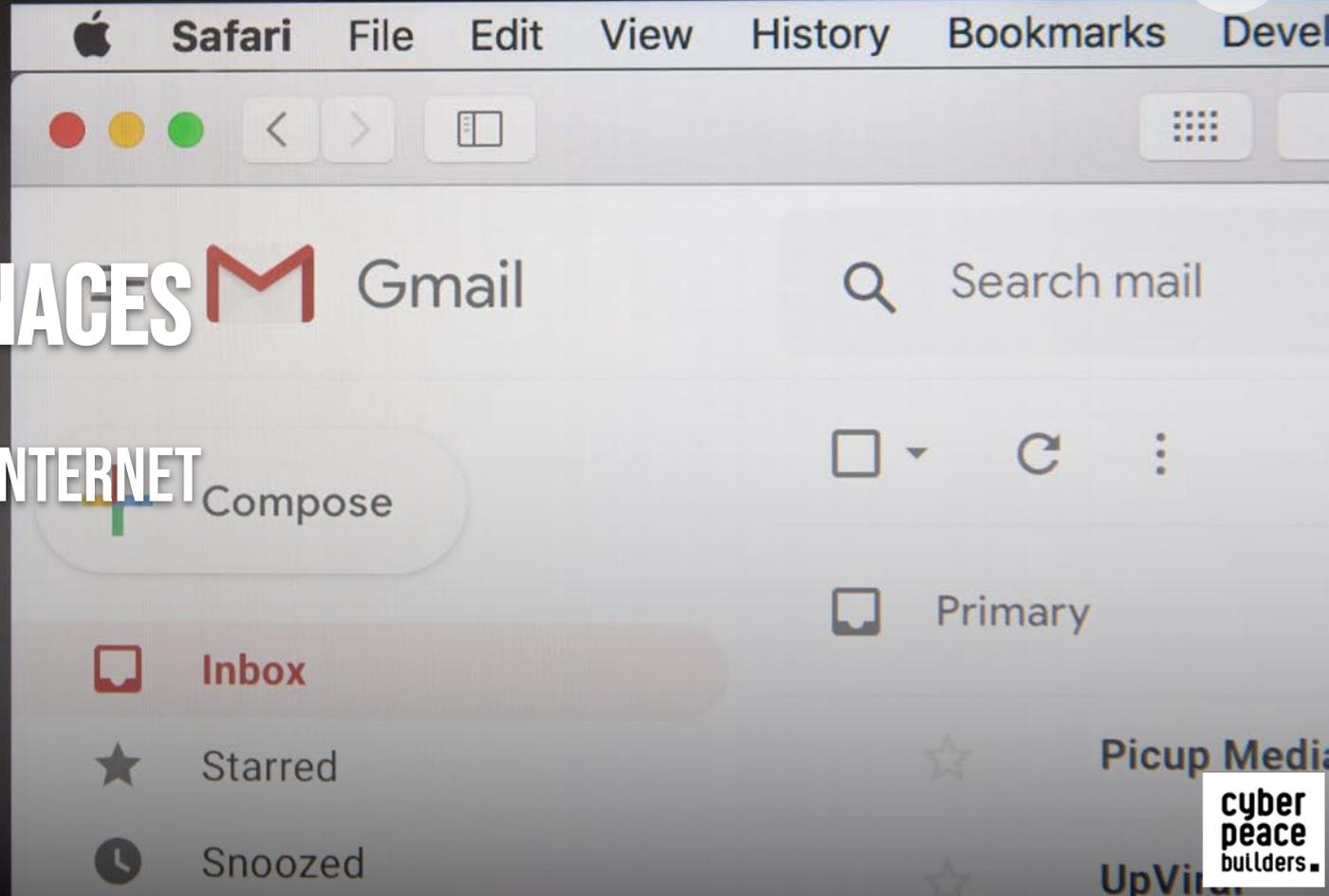
Liens étranges



Pièces jointes surprenantes (exe, js, iso, pdf, docx, xlsx, etc.)

LES CYBERMENACES

LES ADRESSES INTERNET (URL)



QUELS SONT LES DIFFÉRENTS ÉLÉMENTS D'UNE URL ?

URL (Uniform Resource Locator)

http ://www.exemple.com

Protocole

Sous-domaine

Nom

Extension

Nom de domaine

Examinez le protocole : la partie « https » indique que la connexion est sécurisée

Sécurisé ≠ authentique !

Étudiez attentivement le nom de domaine

<https://Facebook-login-FR-LocationGeneve.mauvaisdomaine.com>

ATTENTION AVANT DE CLIQUER...

19

Login alert for Firefox on Windows Inbox x

Facebook <security@facebookmail.com>

to Fabien ▾

🌐 English ▾ > French ▾ [Translate message](#)

 Login Alert

Hi Fabien,

We noticed an unusual login from a device or location you don't usually use. Was this you?

New Login

🕒 September 3, 2018 at 10:37 AM

📍 Near Maiduguri, Nigeria

🦊 Firefox on Windows

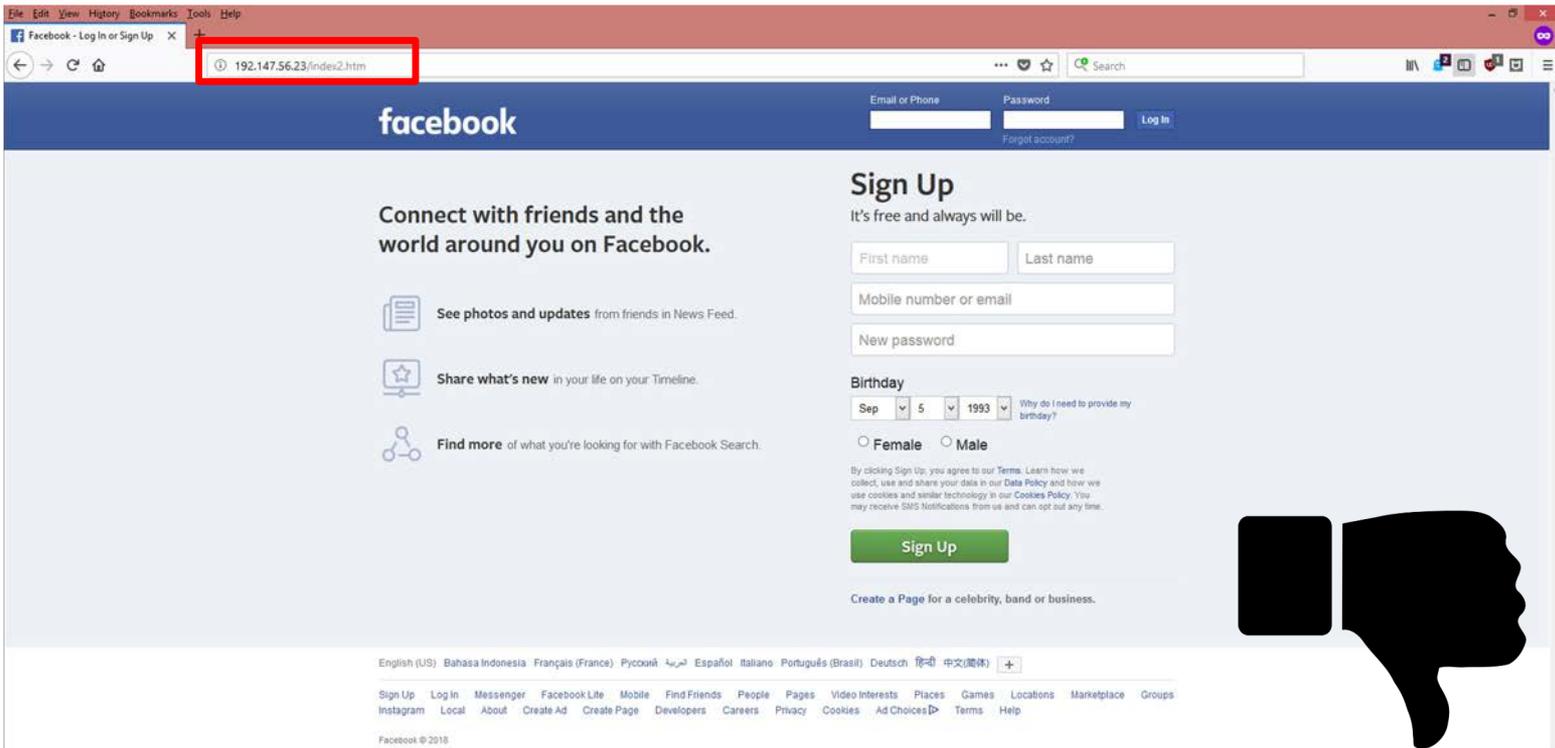
[Review Login](#)

[Manage Alerts](#)

This message was sent to [redacted]. If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).
Facebook Ireland Ltd., Attention: Community Operations, 4 Grand Canal Square, Dublin 2, Ireland

REMARQUEZ-VOUS QUELQUE CHOSE D'ÉTRANGE SUR CETTE PAGE ?

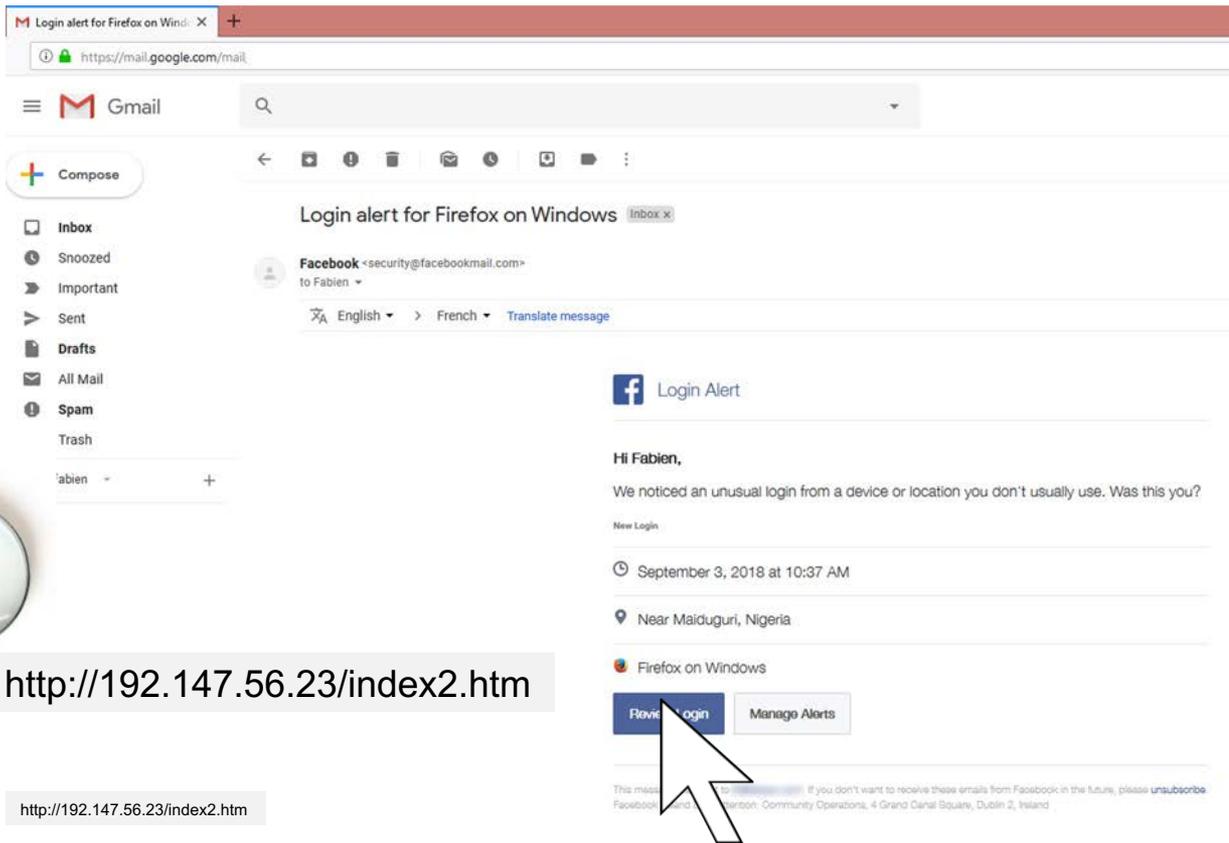
20



The image shows a screenshot of a web browser displaying the Facebook sign-up page. The browser's address bar contains the URL `192.147.56.23/index2.htm`, which is highlighted with a red rectangular box. The Facebook sign-up form is visible, including fields for "Email or Phone", "Password", "First name", "Last name", "Mobile number or email", "New password", "Birthday" (set to Sep 5, 1993), and "Female" / "Male" radio buttons. A green "Sign Up" button is at the bottom of the form. A large black thumbs-down icon is overlaid on the right side of the page.

CONNAÎTRE L'URL QUI SE CACHE DERRIÈRE UN LIEN

21



https://mail.google.com/mail

Gmail

Compose

Inbox

Snoozed

Important

Sent

Drafts

All Mail

Spam

Trash

abien +

Login alert for Firefox on Windows Inbox x

Facebook <security@facebookmail.com>
to Fabien ▾

English > French ▾ [Translate message](#)

fb Login Alert

Hi Fabien,

We noticed an unusual login from a device or location you don't usually use. Was this you?

New Login

🕒 September 3, 2018 at 10:37 AM

📍 Near Maiduguri, Nigeria

🔥 Firefox on Windows

[Review login](#) [Manage Alerts](#)

This message was sent from a verified sender. If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).
Facebook, Inc. 1601 Willow Road, Menlo Park, CA 94025, USA. © 2018 Facebook. Community Operators, 4 Grand Canal Square, Dublin 2, Ireland

<http://192.147.56.23/index2.htm>

<http://192.147.56.23/index2.htm>

J'AI CLIQUÉ SUR UN LIEN – QUE FAIRE ?

Ne paniquez pas, ça peut arriver à tout le monde 😊

Vous avez saisi votre identifiant et votre mot de passe professionnel ? Modifiez immédiatement votre mot de passe

Si vous utilisez le même mot de passe ou presque sur d'autres plateformes en ligne (à des fins professionnelles et/ou privées), modifiez là aussi votre mot de passe, car un hacker peut réutiliser vos données pour cibler vos autres comptes

En cas de besoin, contactez votre référent-e informatique local-e ou le Help Desk

LES CYBERMENACES

LES MOTS DE PASSE



PEACECYBER2022



COMMENT GÉRER VOS MOTS DE PASSE?

1. Adoptez des mots de passe longs et variés (12 caractères minimum)

- Évitez les mots de passe faciles à deviner (date de naissance, prénom, nom de ville)

2. Utilisez un mot de passe différent pour chaque service et gardez-le pour vous

- Un gestionnaire de mots de passe peut vous aider à gérer facilement tous vos mots de passe complexes

3. Activez la fonctionnalité d'authentification à deux facteurs quand c'est possible

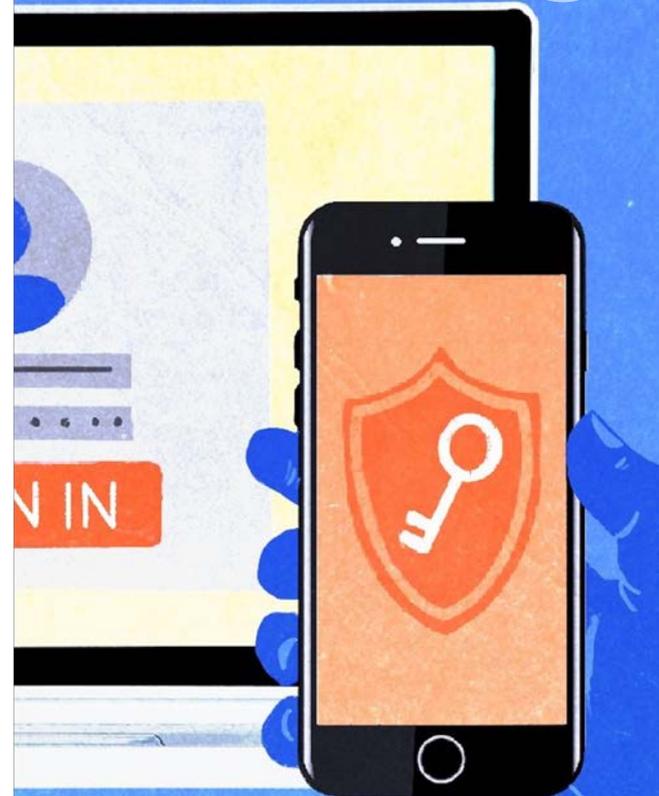
- Vérifiez si vos sites favoris l'acceptent : <https://twofactorauth.org/>

Les 10 mots de passe les plus courant

- | | |
|-------------|--------------|
| 1. 123456 | 6. 123456789 |
| 2. Password | 7. letmein |
| 3. 12345678 | 8. 1234567 |
| 4. qwerty | 9. football |
| 5. 12345 | 10. iloveyou |

AUTRES POINTS CONCERNANT LES MOTS DE PASSE

- **Portez une attention particulière au mot de passe qui protège votre messagerie électronique**
 - C'est généralement sur votre messagerie que sont envoyés les liens permettant de récupérer ou de redéfinir le mot de passe associé à un autre service
- **Ne laissez jamais une session ouverte sur votre ordinateur si vous devez quitter votre bureau**
 - Prenez l'habitude de vous déconnecter, d'éteindre l'ordinateur ou de le verrouiller (simplement en appuyant sur les touches  Win+L)



LES CYBERMENACES

LES TÉLÉPHONES MOBILES ET LES DÉPLACEMENTS

QUEL WI-FI PUBLIC CHOISIR À L'AÉROPORT ?

28





RÉSEAUX WI-FI PUBLICS

1. Évitez les Wi-Fi publics (aéroports, restaurants, hôtels)

- Vous ne savez pas qui gère ces réseaux

2. Préférez la connexion 4G de votre smartphone

- Ce réseau est plus sûr et donc recommandé pour se connecter à un site Web qui nécessite de saisir des données sensibles ou qui en stocke

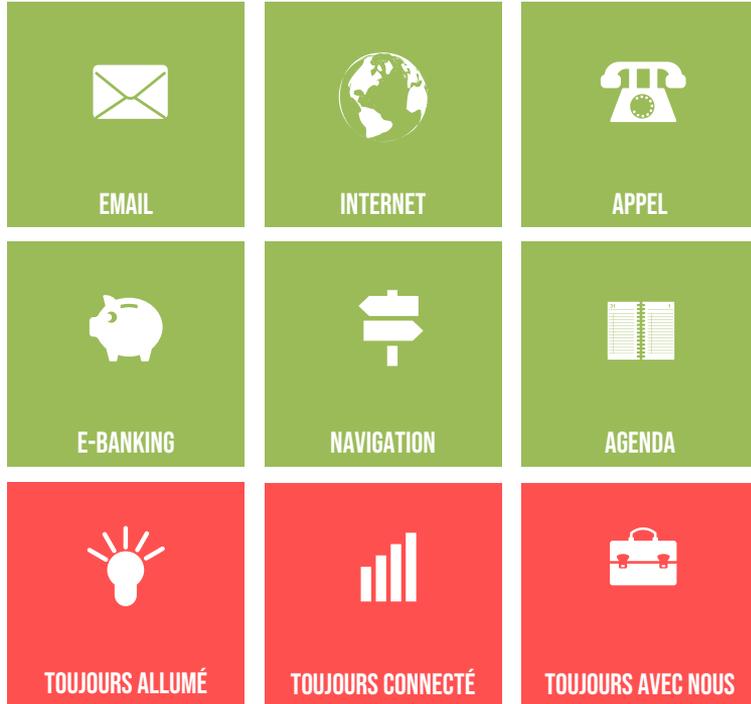
3. Utilisez un VPN, un outil de sécurité pour ordinateurs portables, tablettes et téléphones

- Le VPN protège votre connexion sur les réseaux Wi-Fi publics

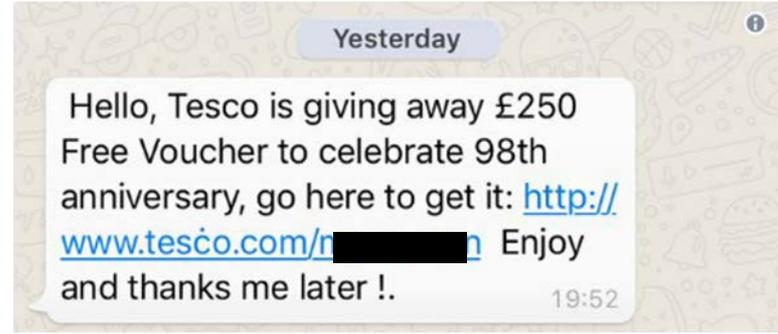
LE SAVIEZ-VOUS?

TOUTES LES COMMUNICATIONS EFFECTUÉES VIA UN RÉSEAU WI-FI PUBLIC PEUVENT ÊTRE INTERCEPTÉES À VOTRE INSU. IL EN VA DE MÊME DANS LES HÔTELS AVEC LA CONNEXION PAR CÂBLE

UTILISATION D'UN SMARTPHONE?



**Téléphone mobile ou ordinateurs :
les mêmes menaces**

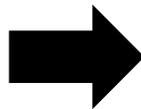


LES CYBERMENACES

LA SÉCURITÉ PHYSIQUE DES
INFORMATIONS

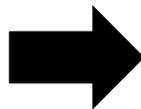
QUE PEUT-IL ARRIVER ?

Espionnage par-dessus votre épaule



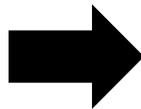
Vérifiez qui se trouve derrière vous

Clé USB malveillantes



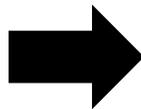
Ne branchez pas n'importe quelle clé USB

Impression



Imprimez de manière sécurisée

Perte d'un appareil



Cryptez vos contenus

EST-CE UNE BONNE IDÉE ?

33

Email
Password:

freddie23

Banking
Password:

money23

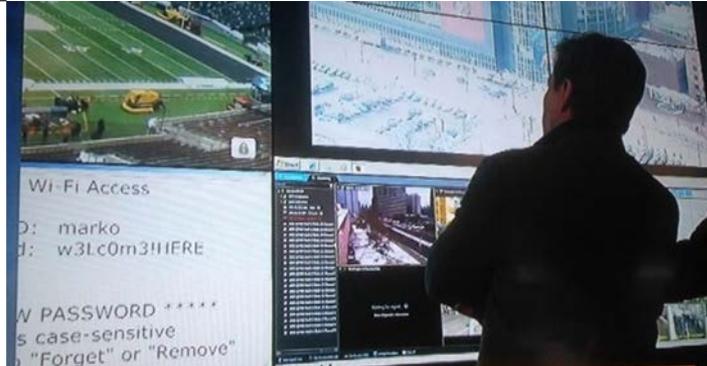
COMMENT DIRE...



Super Bowl
XLVIII



World Cup,
Brazil



UK weather
emergency

CONCLUSION

LA SÉCURITÉ DE L'INFORMATION EST
NOTRE RESPONSABILITÉ À TOUS

RESTEZ VIGILANT-E-S...

36



[HTTPS://WWW.YOUTUBE.COM/WATCH?V=UBNF9QNEQLA](https://www.youtube.com/watch?v=UBNF9QNEQLA)



MERCI

assistance@cyberpeaceinstitute.org
<https://cyberpeaceinstitute.org>

f CyberpeaceInstitute

t @CyberpeaceInst

in The CyberPeace Institute

