



Êtes-vous cybersécuritaire?

Marc-Antoine Bernier



Déroulement

OpenTR 2019

1. Présentation mon équipe et moi
2. Pourquoi la cybersécurité?
3. Les mots de passe
4. L'hameçonnage
5. Conclusion





Qui suis-je?

Expériences

- 3 ans en sécurité / 2 ans comme développeur
- 2 ans chez Desjardins

Certification et Diplôme

- Baccalauréat en Génie Informatique (UdeS)
- OSCP (Offensive Security Certified Professional)

Contact

- <https://ca.linkedin.com/in/marc-antoine-bernier>
- @marcan2020





Mon équipe



NAME

ETTIC - Experts Technologiques en Test Intrusion et Criminalistique

DESCRIPTION

Équipe de cybersécurité offensive

--red-team Simulation d'attaque

--training Formation développement sécuritaire

--vigie Observation du périmètre externe

--pentest Test d'intrusion

Pourquoi la
cybersécurité?





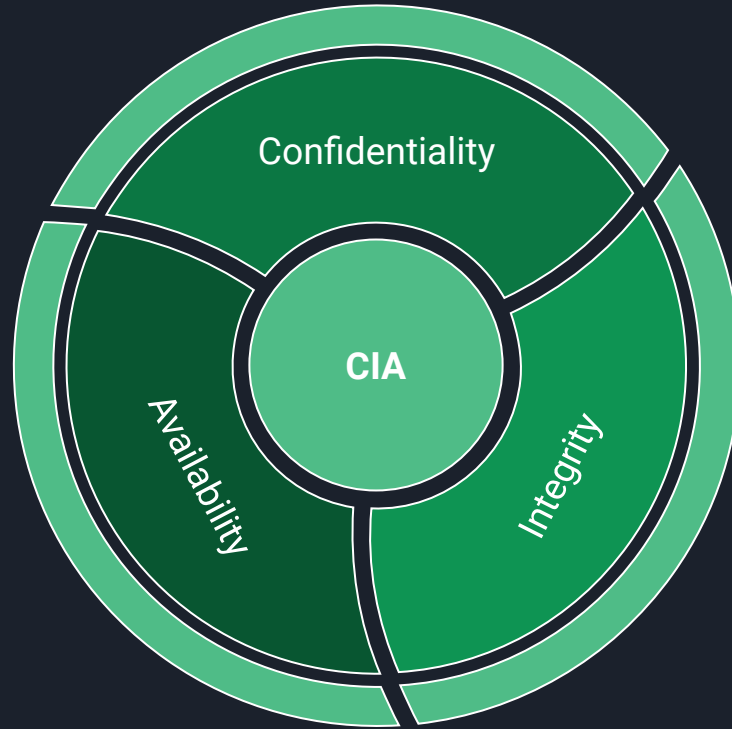
Pourquoi la cybersécurité?

Principale cause: Transformation numérique

Les raisons pour investir en cybersécurité:

- Protection des renseignements personnels des clients et des employés.
- Prévention de la fraude et du vol.
- Éviter les interruptions de service.
- Éviter des pertes financières.
- Conserver notre réputation et notre l'image de marque intact.
- etc.

Sécurité de l'information



Qui nous attaque et
pourquoi?



Attaquants

Motivation



Statistiques

Les incidents de cybersécurité provoqués par les cybercriminels ont été faits dans l'intention

de voler de l'argent ou de demander une rançon

Entreprises touchées par un incident de cybersécurité

38 %

d'accéder à des zones d'accès non autorisées

26 %

de voler des renseignements personnels ou financiers

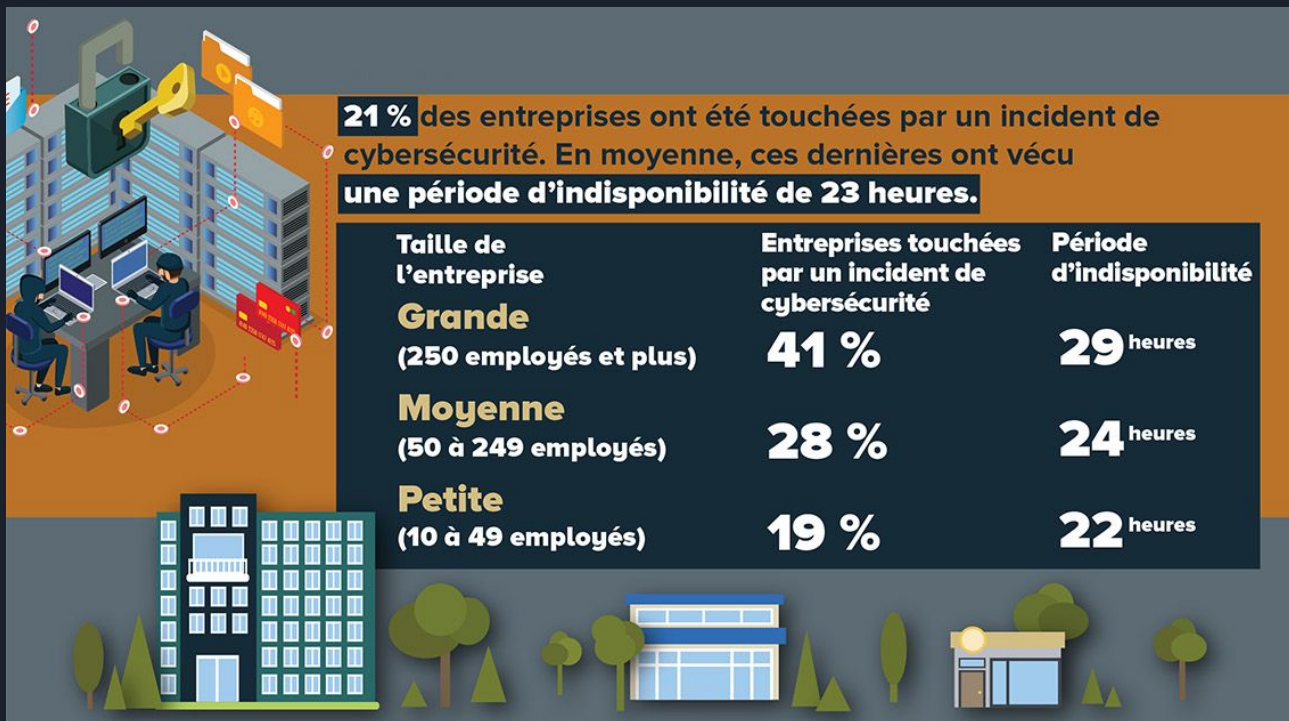
23 %

de perturber ou de dénaturer l'entreprise ou sa présence sur le Web

22 %



Statistiques



Les mots de passe



Qui a un pin code sur
son cellulaire?



Combien de mots de
passe utilisez-vous?



Qui utilise une voûte de
mots de passe?



Qui utilise des
authentifications à deux
facteurs?





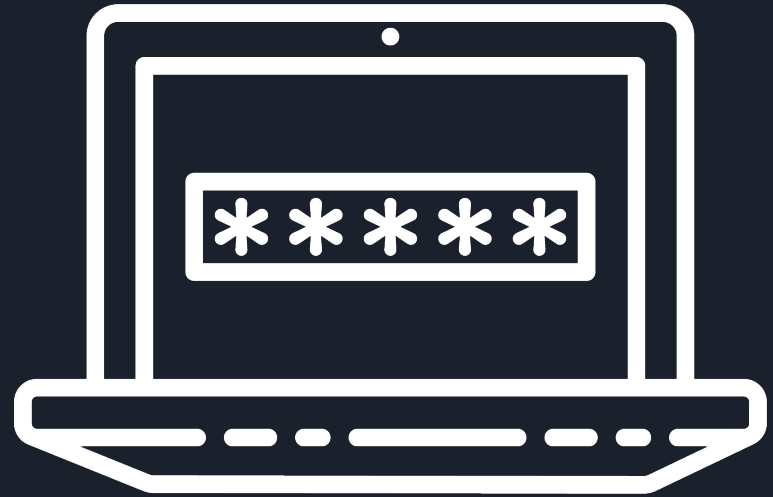
Fort ou Faible?

- P@55w0rD1!
- qwertyuiopasdfghjklzxcvbnm
- Zaq12wsxcde3!
- CareyPrice1987
- WKZAe3,JFU67zY;3
- Un avion qui chante des ananas
- Spongebobsquarepants
- I got a participation ribbon



Bonnes pratiques

1. Mes mots de passe doivent être:
 - Forts
 - Différents sur chaque site
2. Utiliser une voûte de mots de passe
3. Utiliser l'authentification à deux facteurs
4. Faire attention aux questions secrètes



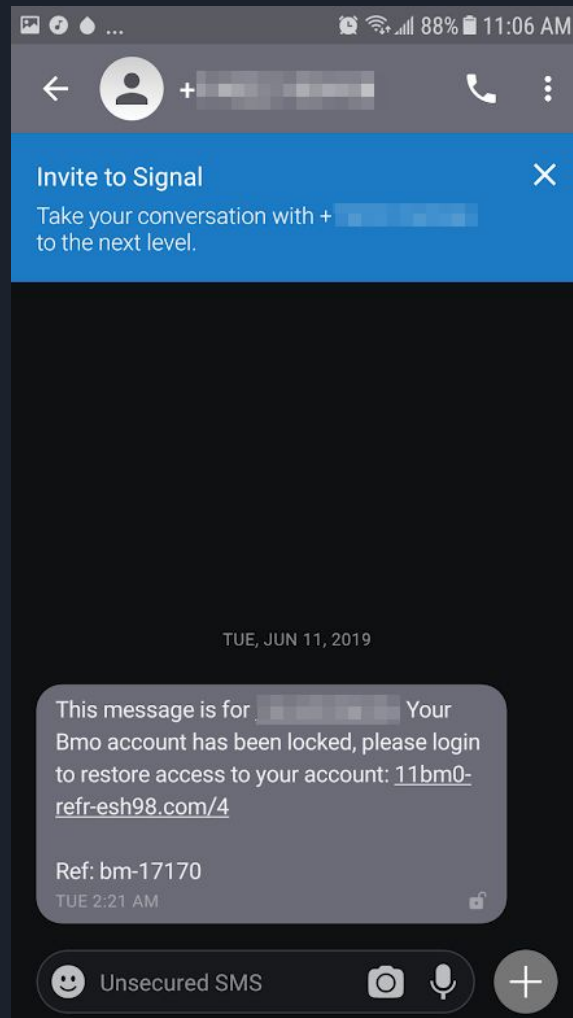
L'hameçonnage



Légitime ou pas?



Exercise #1




Exercise #2

User Account Control

×

Do you want to allow this app to make changes to your device?

 User Account Control Settings

Verified publisher: Microsoft Windows

[Show more details](#)

To continue, enter an admin user name and password.

Shawn Brink

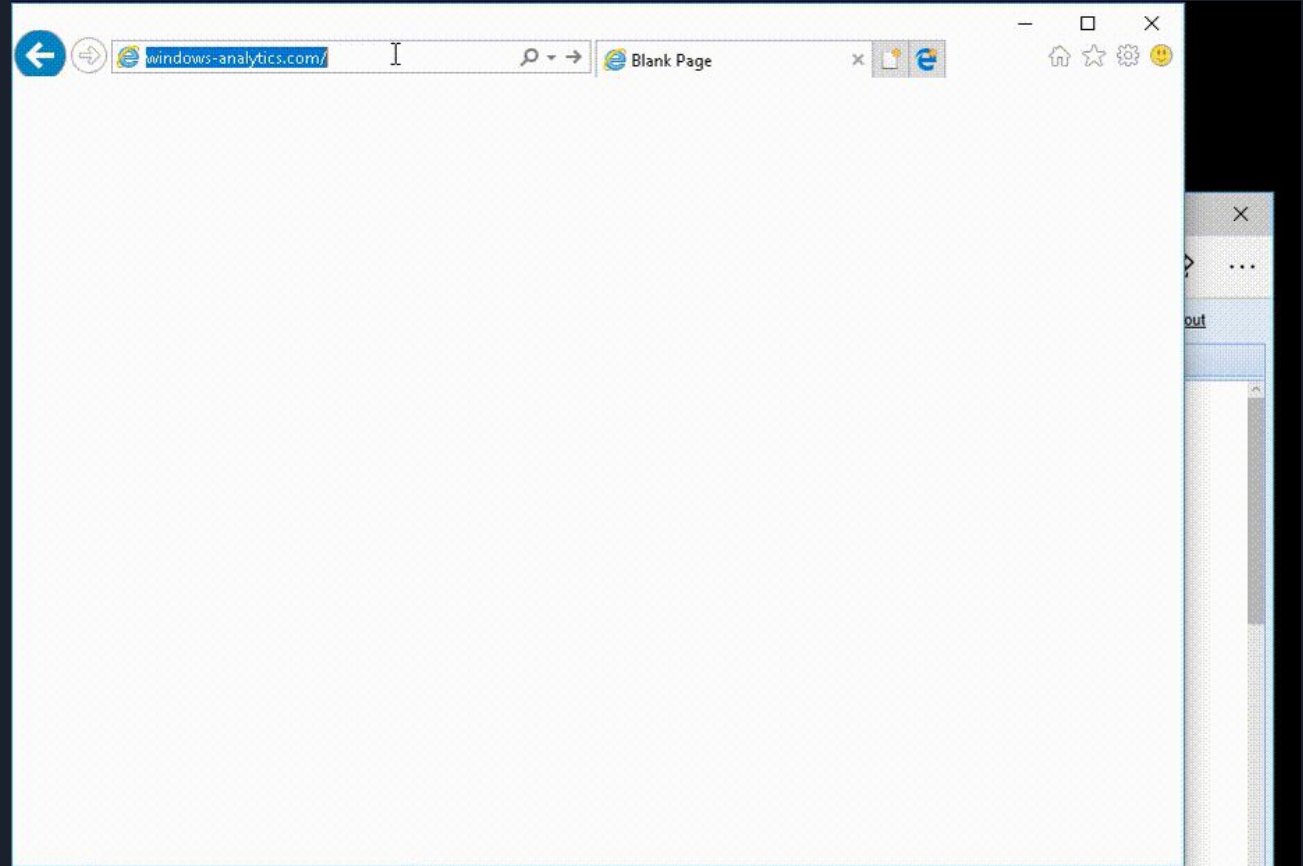
@outlook.com

Password

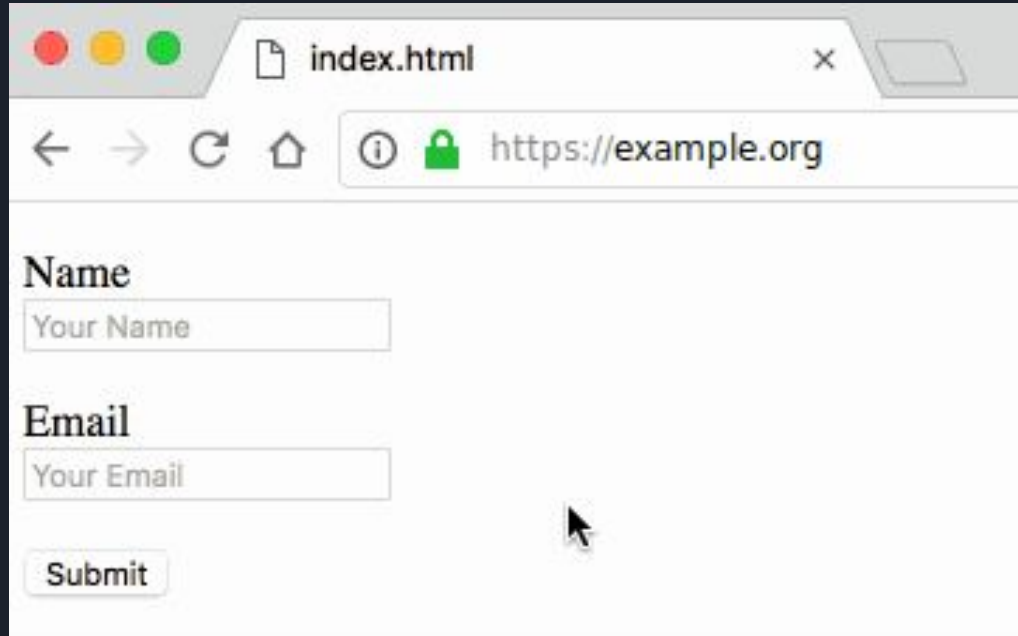
Yes

No

Explication



Exercise #3



A screenshot of a web browser window. The title bar shows a tab labeled "index.html". The address bar displays "https://example.org" with a green padlock icon. The page content includes a form with two text input fields and a submit button. The first field is labeled "Name" and contains the placeholder text "Your Name". The second field is labeled "Email" and contains the placeholder text "Your Email". Below these fields is a button labeled "Submit". A mouse cursor is visible near the bottom right of the form area.

index.html

https://example.org

Name

Your Name

Email

Your Email

Submit

Explication

▼ Form Data [view source](#) [view URL encoded](#)

name: John Doe
email: john@doe.com
phone: 501231234
organization: SecretCompany
address: SecretAddress
postal: 12345
city: SecretCity
country: FI

The screenshot shows a web browser window with the address bar displaying `https://example.org`. The page contains a form with fields for Name, Email, and a Submit button. Below the form, the Network tab is open, showing a list of requests. The request for `index.html` is selected. The right-hand pane displays the details for this request, including the Request URL, Request Headers, and Form Data. The Form Data section is expanded, showing the same data as the left-hand pane.

Network Tab Details:

- Request URL:** file:///Users/antti/password-autocomplete-test/index.html
- Request Headers:**
 - Content-Type: application/x-www-form-urlencoded
 - Origin: null
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36
- Form Data:**
 - name:** John Doe
 - email:** john@doe.com
 - phone:** 501231234
 - organization:** SecretCompany
 - address:** SecretAddress
 - postal:** 12345
 - city:** SecretCity
 - country:** FI

Exercise #4



SNELL, CHURCH & BAILEY LLP

Barrister & Solicitors

NOTARIES PUBLIC

10940 W SAN HOUSTON PKWY, # 200

HOUSTON, TX 77064

Tel: +1 (281) 616 5772

Fax: +1 (281) 581 9105

Website: www.snellchurchbailey.com

REF: EDMLP/41007/290419

Date: 06-10-2019

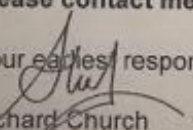
Dear [REDACTED]

My name is Richard Church; I am a partner at Snell, Church & Bailey LLP.

It may surprise you to receive this letter from me, since there has been no previous correspondence between us. There is an unclaimed "permanent life insurance policy" held by our deceased Canadian client. I decided to contact you during my visit to Toronto Ontario, Canada, for three days seminar.

Please contact me privately via: (email: [REDACTED]@gmail.com

Your earliest response to this matter would be highly appreciated.


Richard Church
Attorney

Exercise #5



Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE


You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: 

Exercise #6



DOCUMENT IS ENCRYPTED

TO DECRYPT DOCUMENT, PLEASE PERFORM THE FOLLOWING STEPS:

- 1 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.
- 2 Once you have enabled editing, please click "Enable content" on the yellow bar above.

WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS, Android.
- You are trying to view this document using an online viewer.



Center for Food
Safety and Applied Nutrition

Food poisoning control



Center for Food Safety and Applied Nutrition (CFSAN) <fda@CFSAN.gov>

Friday, February 16, 2018 at 3:39 PM

[Show Details](#)



[Download All](#)

[Preview All](#)



THE CENTER FOR FOOD SAFETY
AND APPLIED NUTRITION (CFSAN)

Hallo. We have recently detected a number of safety shortcomings in your fast food restaurants, including your own. You were particularly found to fall short on several key foodborne illness prevention practices. There were 4 reported food poisoning cases in your state over the past month, including two cases of severe poisoning.

It was further detected that food poisoning was caused by cross-contamination from handling raw beef or undercooked hamburgers. It was brought to our attention that at least three of four patients dined at your restaurant network branches shortly before poisoning and suspect that food was contaminated.

You can find attached the list of inspections and checks scheduled to take place at your restaurant.

U.S. Food and Drug Administration
Center for Food Safety and Applied Nutrition (CFSAN)
Outreach and Information Center
5001 Campus Drive, HFS-009, College Park, MD 20740-3835



- Fraude de **plus d'un milliard** de dollars \$\$\$
- **15 millions** de numéros de cartes de crédit*
- **3 600** entreprises*

*Aux États-Unis **seulement**



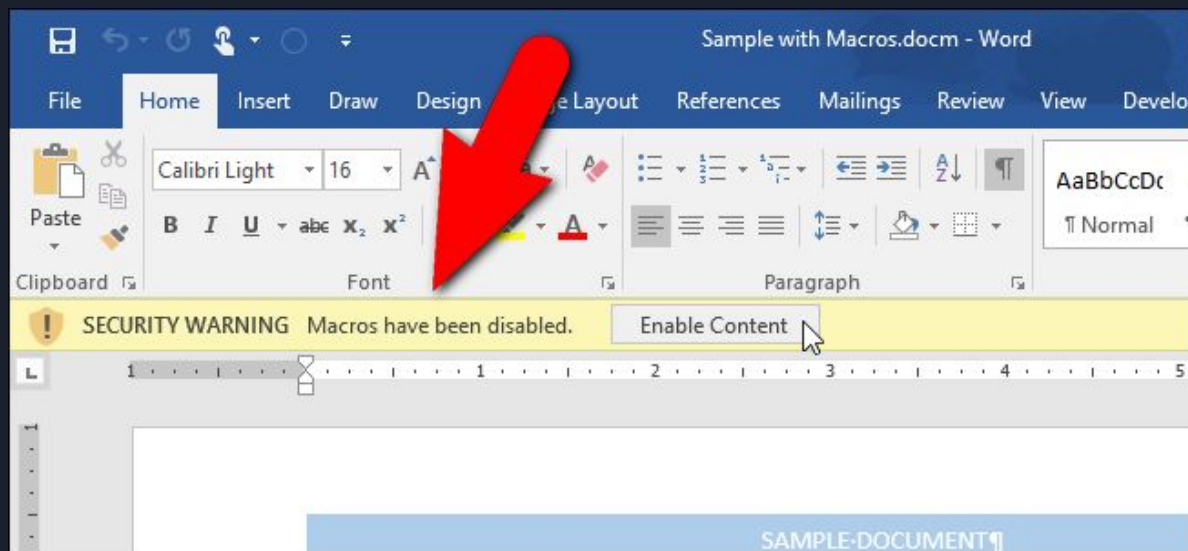
<https://www.wired.com/story/fn7-wild-inner-workings-billion-dollar-hacking-group/>

Bonnes pratiques

- Faites attention aux caractéristiques suivantes:
 1. Trop beau pour être vrai
 2. Sentiment d'urgence
 3. Hyperliens
 4. Pièces jointes
 5. Expéditeur inhabituel
- Ne pas ouvrir de documents avec des extensions inconnues (ex. bat, cfg, etc.)
- Ne jamais désactiver son antivirus
- Ne pas accepter ou activer des fonctionnalités dangereuses (bien lire les messages)



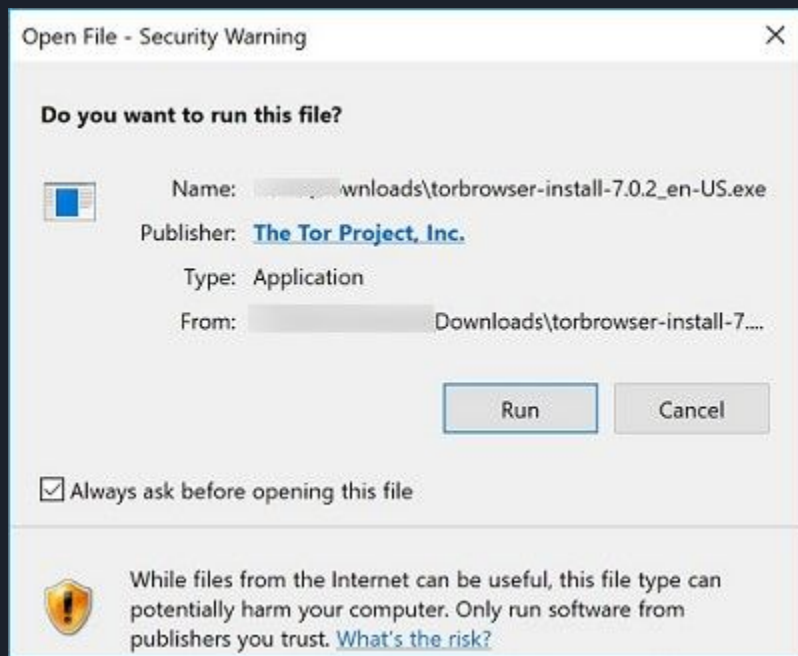
Bonnes pratiques (suite)



Bonnes pratiques (suite)



Bonnes pratiques (suite)





Conclusion

Nous avons la responsabilité de protéger nos entreprises.

On doit donc:

- Sécuriser nos mots de passe.
- Faire des *backups* de nos données.
- Mettre à jour nos appareils, nos ordinateurs et nos applications.
- Rester vigilant pour les messages d'hameçonnage et de harponnage.



Questions?





We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply [restart your membership](#) to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

—Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix membership. We share your email address with our service providers.

<https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017>



Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: [0p2uYq5RIho](#)

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.



[Get the UPS My Choice app for Facebook](#)



[Download the UPS mobile app](#)



<https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/>



Liens utiles

- <https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces>
- <https://www.desjardins.com/proteger-entreprise-contre-cyberattaques/>
- <https://cyber.gc.ca/fr/orientation/cinq-moyens-pratiques-de-renforcer-votre-cybersecurite>
- <https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-fra.htm>
- <http://www.phishing.org/what-is-phishing>