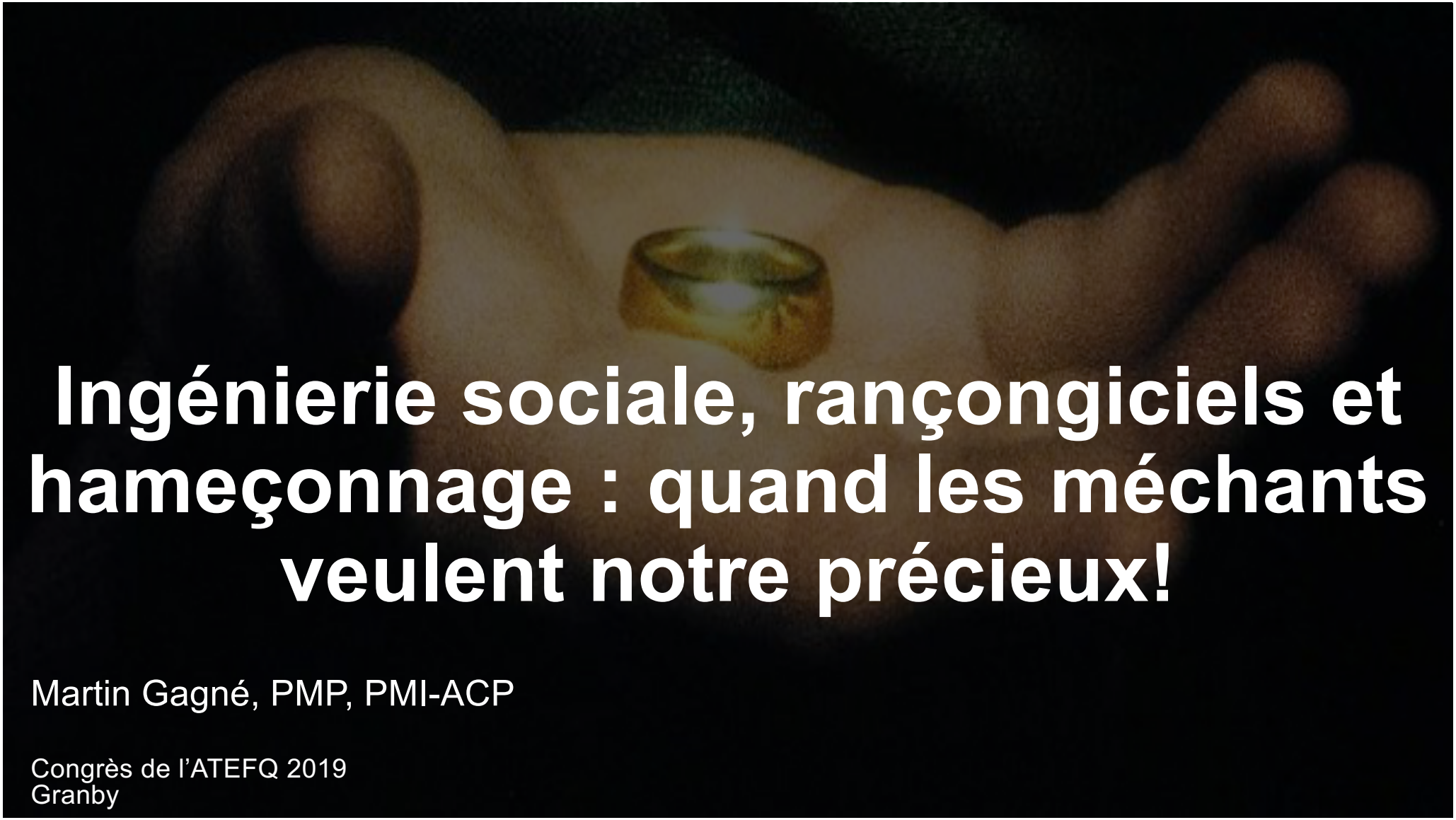


Ingénierie sociale, rançongiciels et hameçonnage : quand les méchants veulent notre précieux!

Martin Gagné, PMP, PMI-ACP

Congrès de l'ATEFQ 2019
Granby

Votre conférencier

Martin Gagné, PMP, PMI-ACP

Directeur, Développement Logiciel
Sherweb

Âge : 42

Formation :

- Bacc - Informatique de gestion - UdeS (2000)
- MBA - Gestion des entreprises - UdeS (2019)

Certification : PMP, PMI-ACP

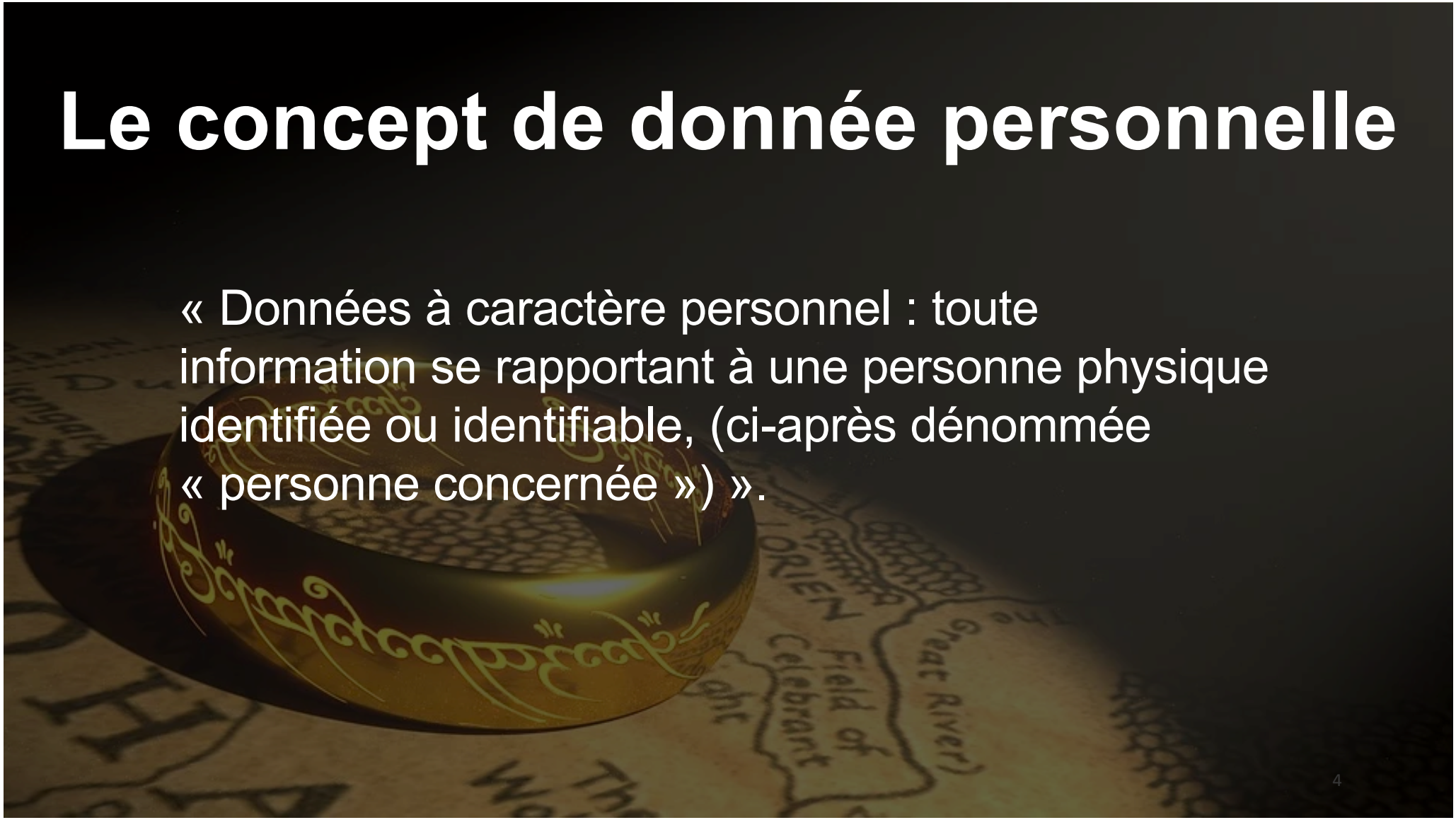
Sport préféré : Golf

Passion : le cinéma, l'informatique


Le précieux

Le concept de donnée personnelle

« Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable, (ci-après dénommée « personne concernée ») ».



Ce qui a de la valeur

- Les données personnelles
- Les informations financières d'une entreprise
- Les numéros de carte de crédit
- Les informations de connexion des usagers (login/password)
- Les préférences et les goûts d'un groupe de consommateur
- Les intentions de vote
- etc…

La valeur des données personnelles

La donnée à l'échelle individuelle ne vaut rien ! Sa valeur marchande provient uniquement de l'agrégation de masse.

Des prix de données personnelles en dollars américains

Fullz **:** 50-150 $ (très variable selon la cote de crédit)

Courriel et mot de passe Gmail : 3 $

Accès à un site web bancaire : 100 $

Numéro de carte de crédit avec code CVV : 60 $

Permis de conduire : 400-500 $ pour un permis d'un État américain (moins cher pour les autres pays)

Passeport canadien : 2000 à 5000 $, aussi peu que 15 $ pour un scan

Carte d'assurance maladie du Québec : 200 $

Nouvelle identité complète (incl. documents, etc.) : 46 000 $

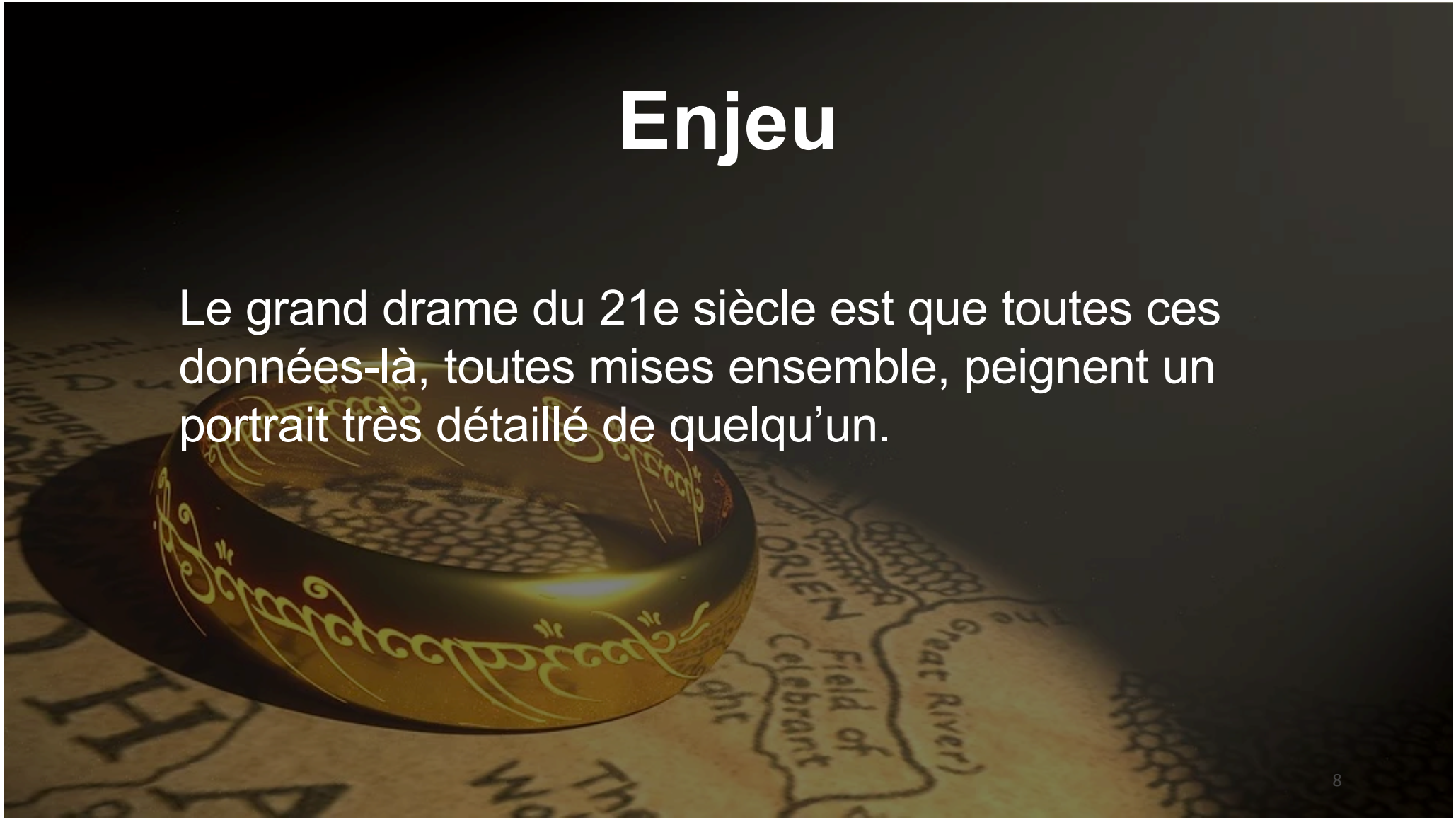
** Les prix fluctuent selon les marchés, les vendeurs, la demande et d'autres facteurs. Ces chiffres ne sont que des estimations.*

Le GAFAM

Les “GAFAM” : Google, Amazon, Facebook, Apple et Microsoft

Enjeu

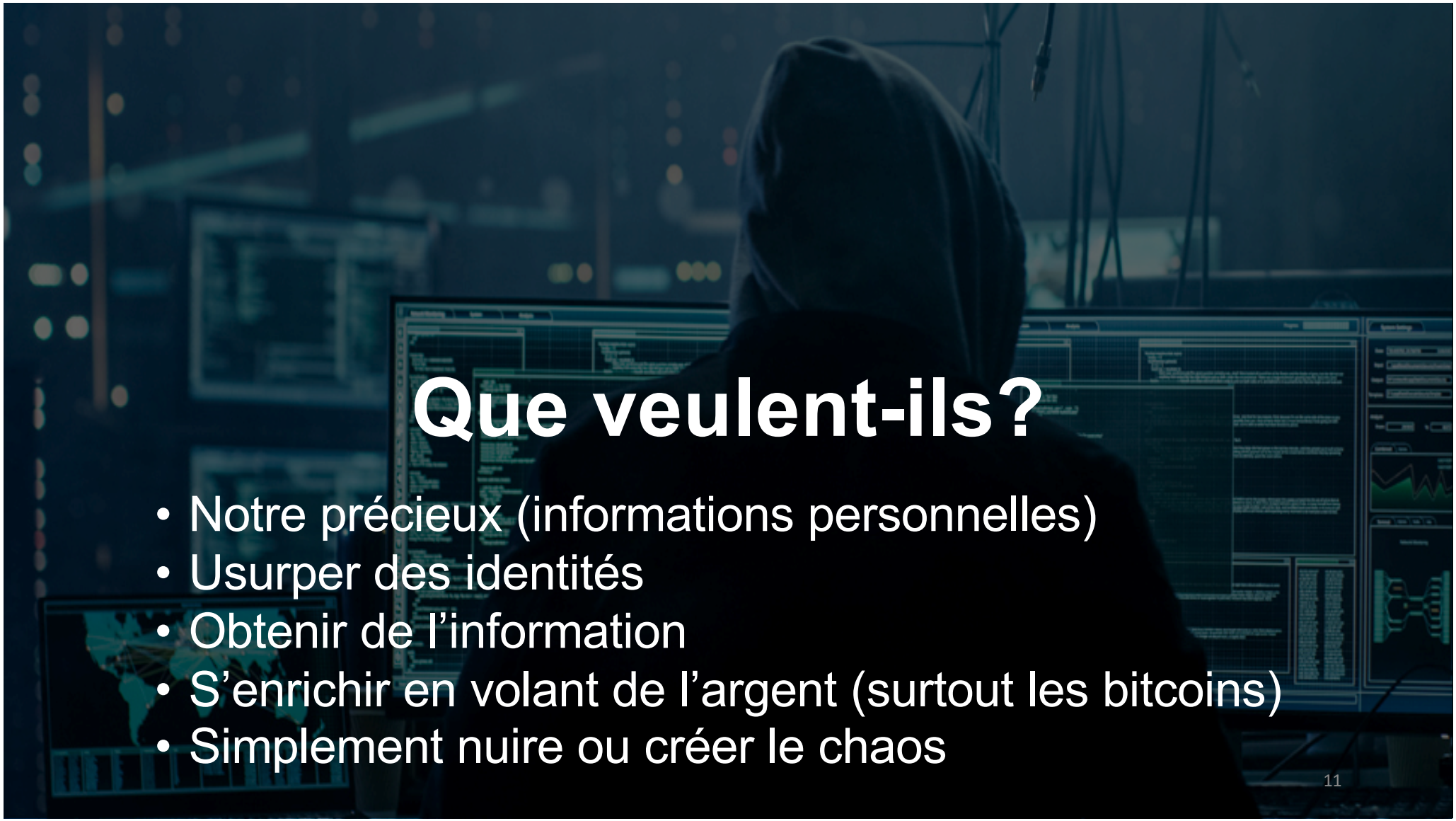
Le grand drame du 21e siècle est que toutes ces données-là, toutes mises ensemble, peignent un portrait très détaillé de quelqu'un.




Les méchants

Qui sont-ils?

- Individus mal intentionnés
- Organisations criminelles
- Employés frustrés
- Compétiteurs malhonnêtes



Que veulent-ils?

- Notre précieux (informations personnelles)
- Usurper des identités
- Obtenir de l'information
- S'enrichir en volant de l'argent (surtout les bitcoins)
- Simplement nuire ou créer le chaos

Leurs caractéristiques

- Forts techniquement
- Très créatifs
- Patients
- Persévérants
- Intelligents
- Peu d'habiletés sociales


Des exemples

John Draper

Alias

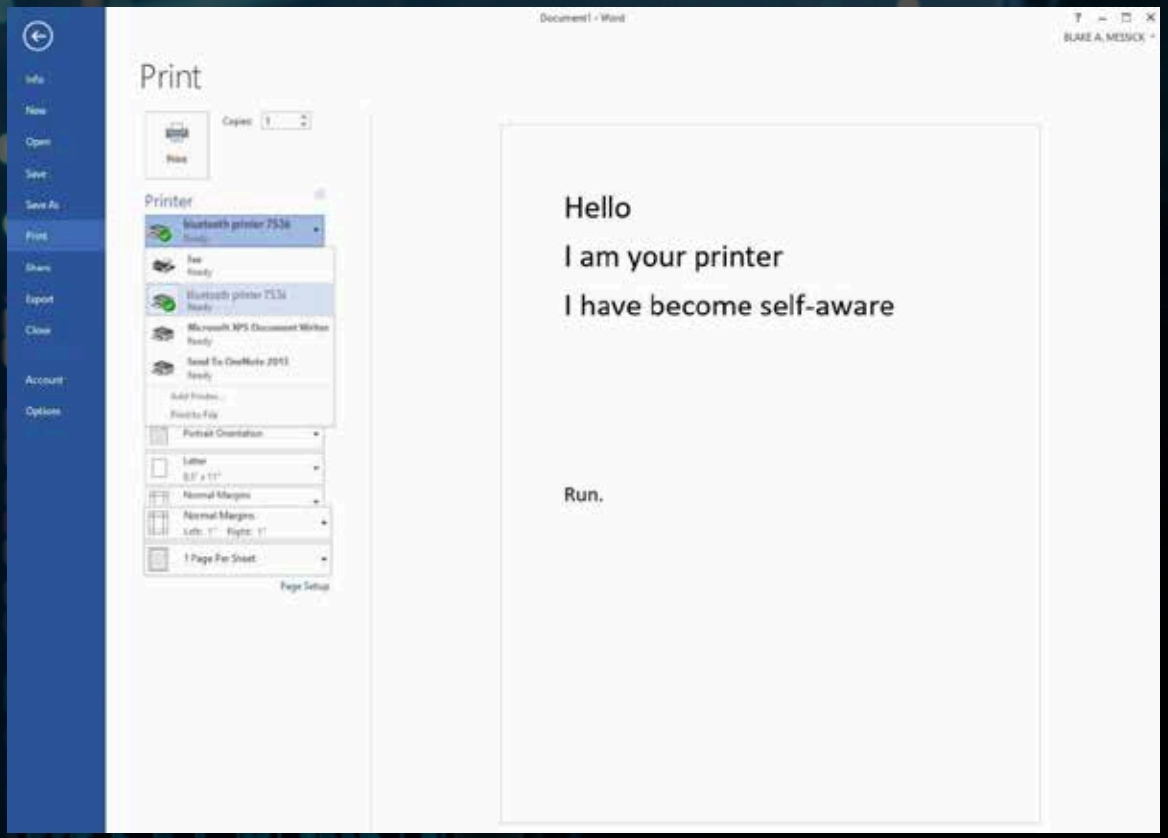
“Captain Crunch”

Michael Calce

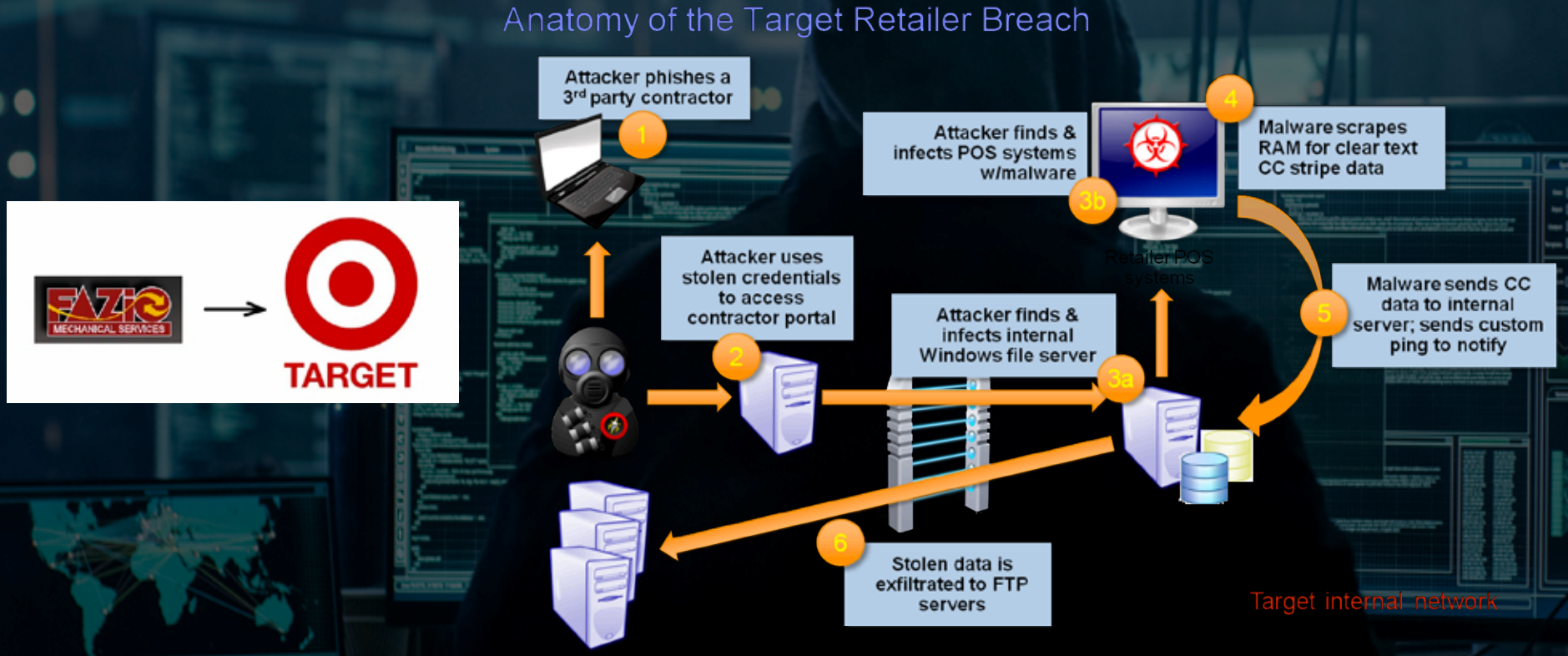
Alias

“MafiaBoy”

IL « PIRATE » L'IMPRIMANTE WIFI DU VOISIN ET FAIT LE BUZZ SUR LES RÉSEAUX SOCIAUX

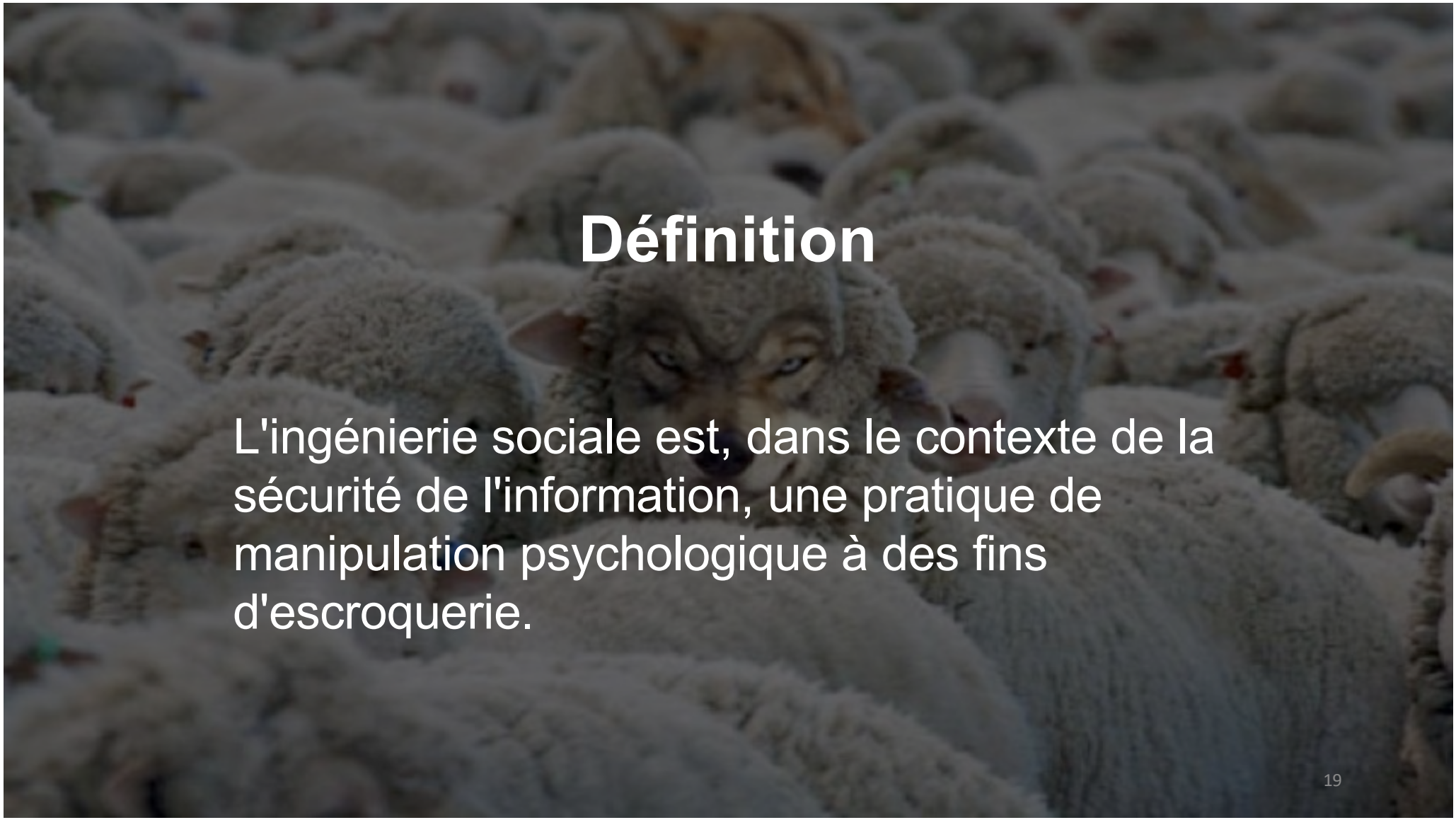


LES MAGASINS TARGET PIRATÉS À TRAVERS UN FOURNISSEUR DE SERVICE EN CLIMATISATION CHAUFFAGE (HVAC)



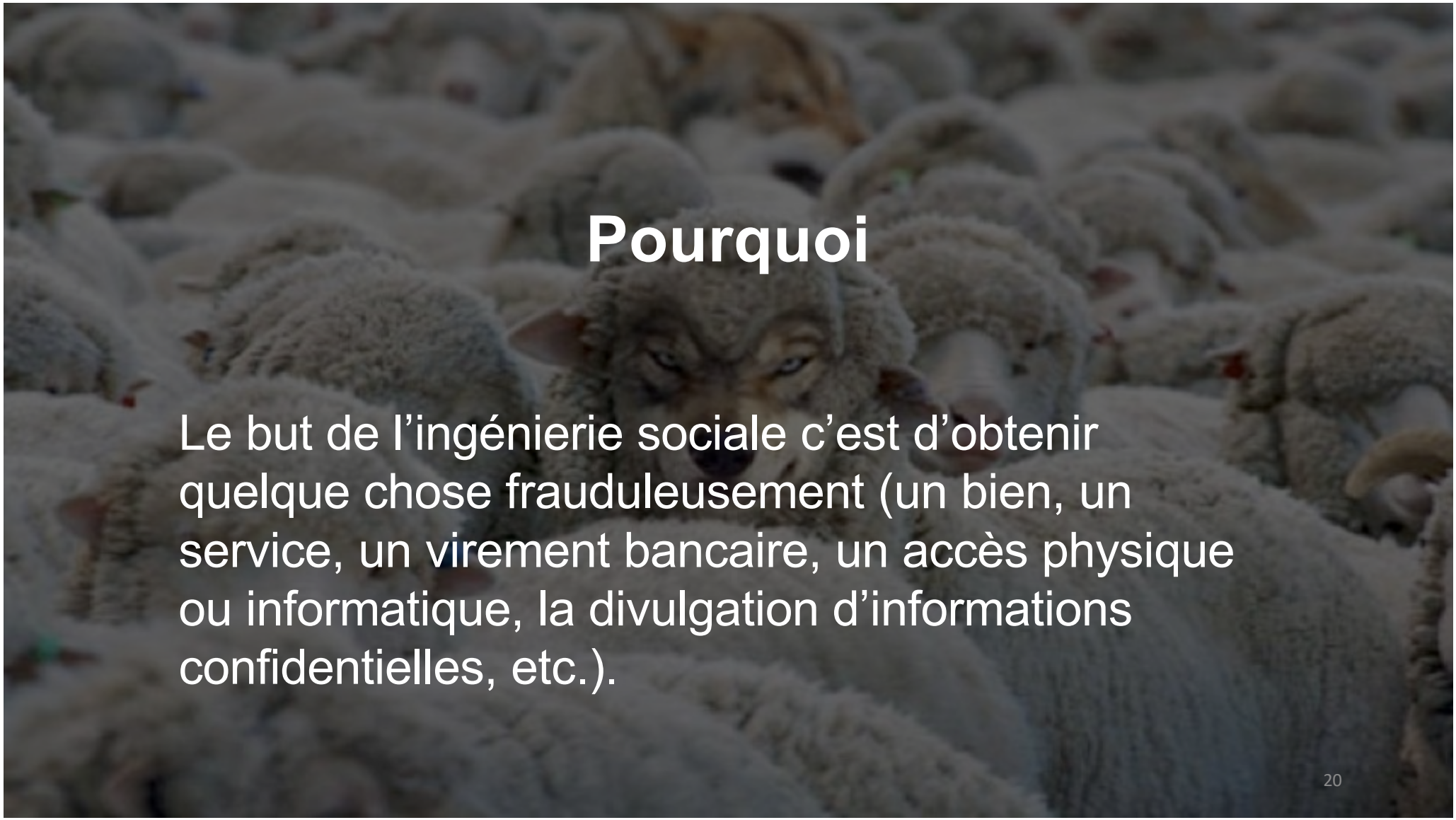
https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/


L’ingénierie sociale



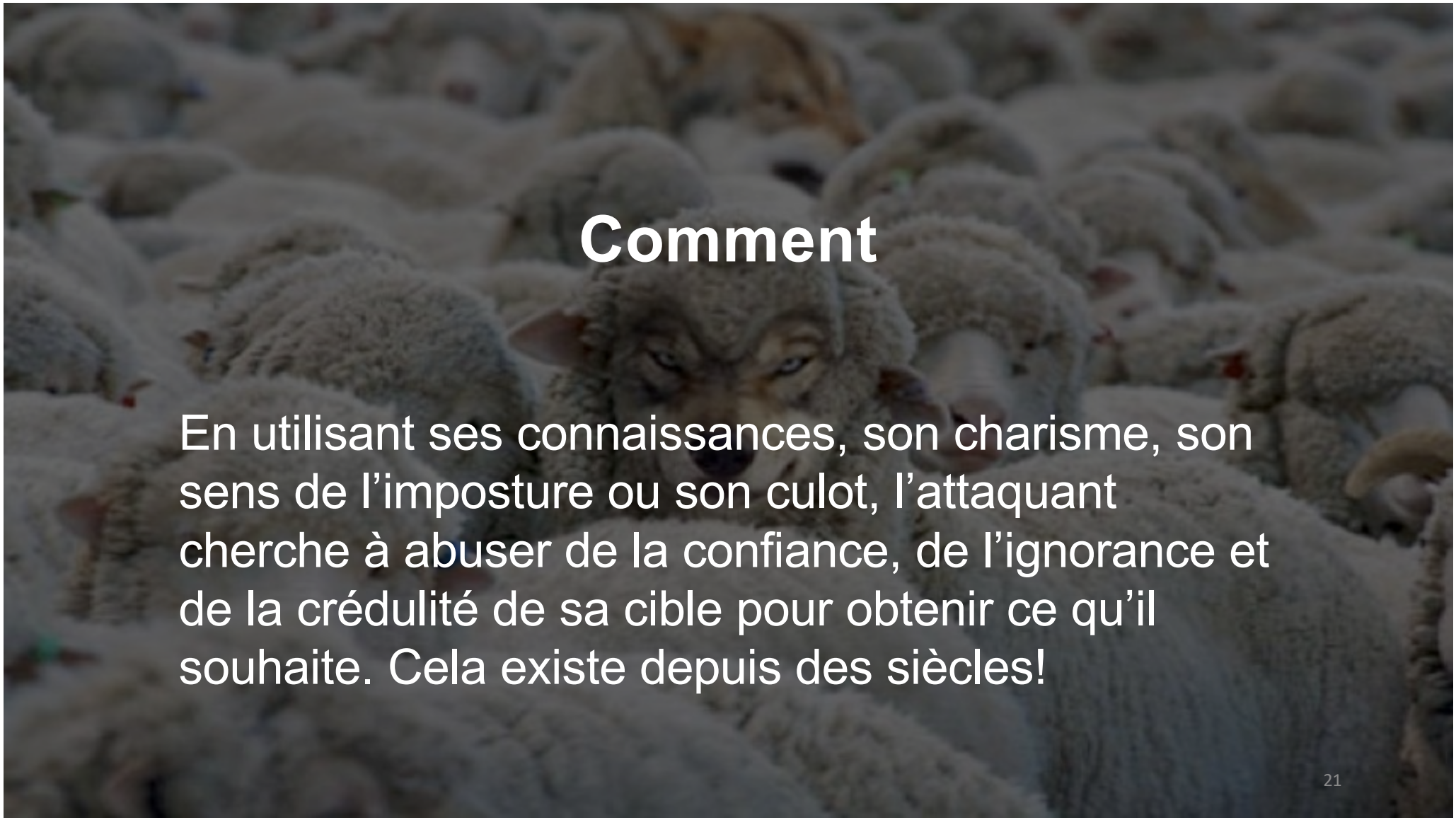
Définition

L'ingénierie sociale est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie.



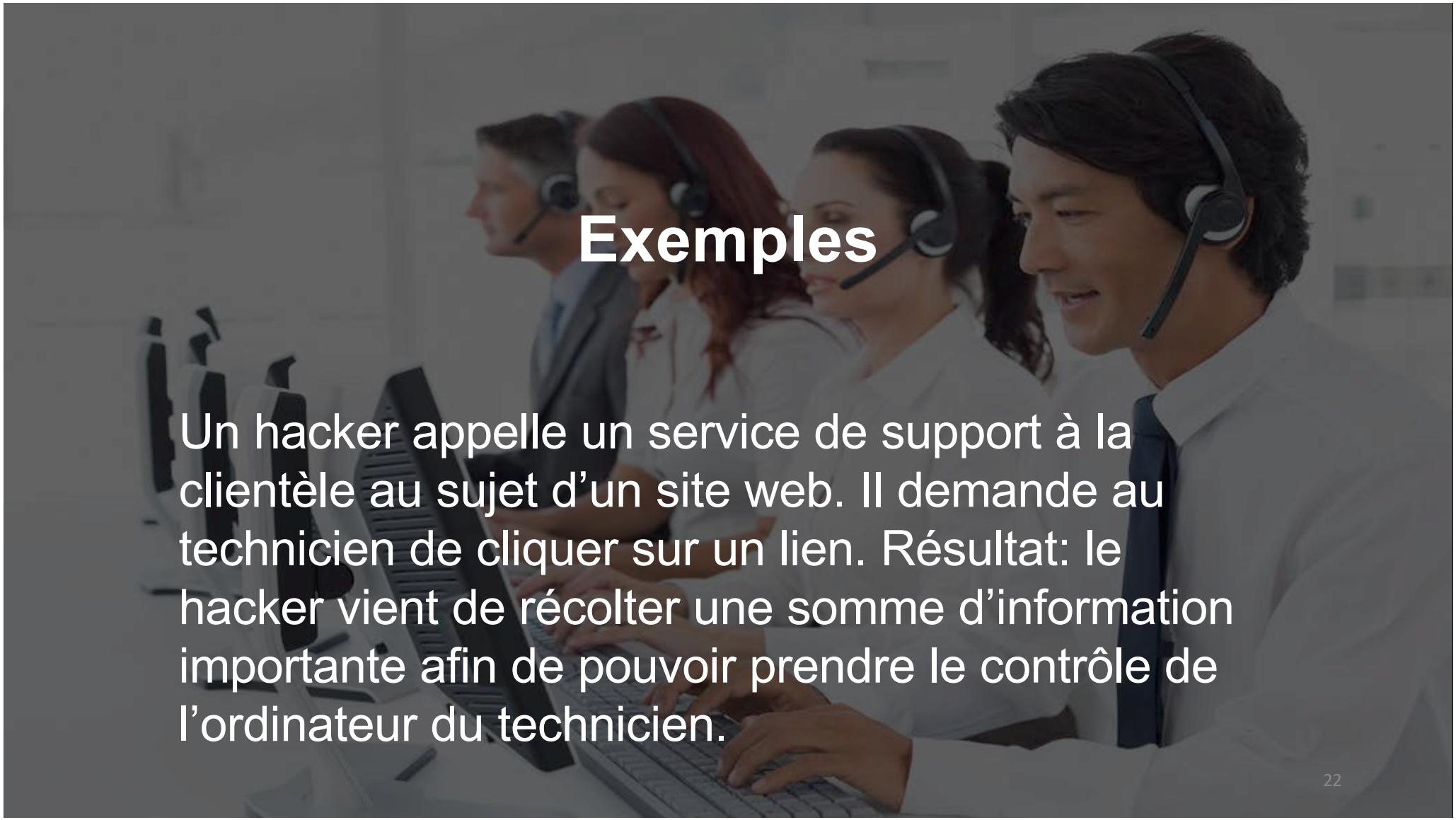
Pourquoi

Le but de l'ingénierie sociale c'est d'obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).



Comment

En utilisant ses connaissances, son charisme, son sens de l'imposture ou son culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité de sa cible pour obtenir ce qu'il souhaite. Cela existe depuis des siècles!



Exemples

Un hacker appelle un service de support à la clientèle au sujet d'un site web. Il demande au technicien de cliquer sur un lien. Résultat: le hacker vient de récolter une somme d'information importante afin de pouvoir prendre le contrôle de l'ordinateur du technicien.

Exemples

Vous êtes en voyage d'affaires. Vous prenez un moment de répit au bar de votre hôtel. Une personne discute avec vous de tout et de rien. En un rien de temps, la personne connaît le nom de vos enfants, leurs âges, le nom de votre conjoint(e), pour qui vous travaillez et votre métier. La personne peut commencer à tenter de deviner des mots de passe.


© Sony Pictures

Protection

- Attention à qui vous parlez en déplacement.
- Valider les identités des visiteurs à votre travail.
- Attention aux arnaques au téléphone (valider les entreprises).
- Ayez des procédures de sécurité au niveau des données
- Soyez alertes et suspicieux, c'est le meilleur moyen pour votre protection!

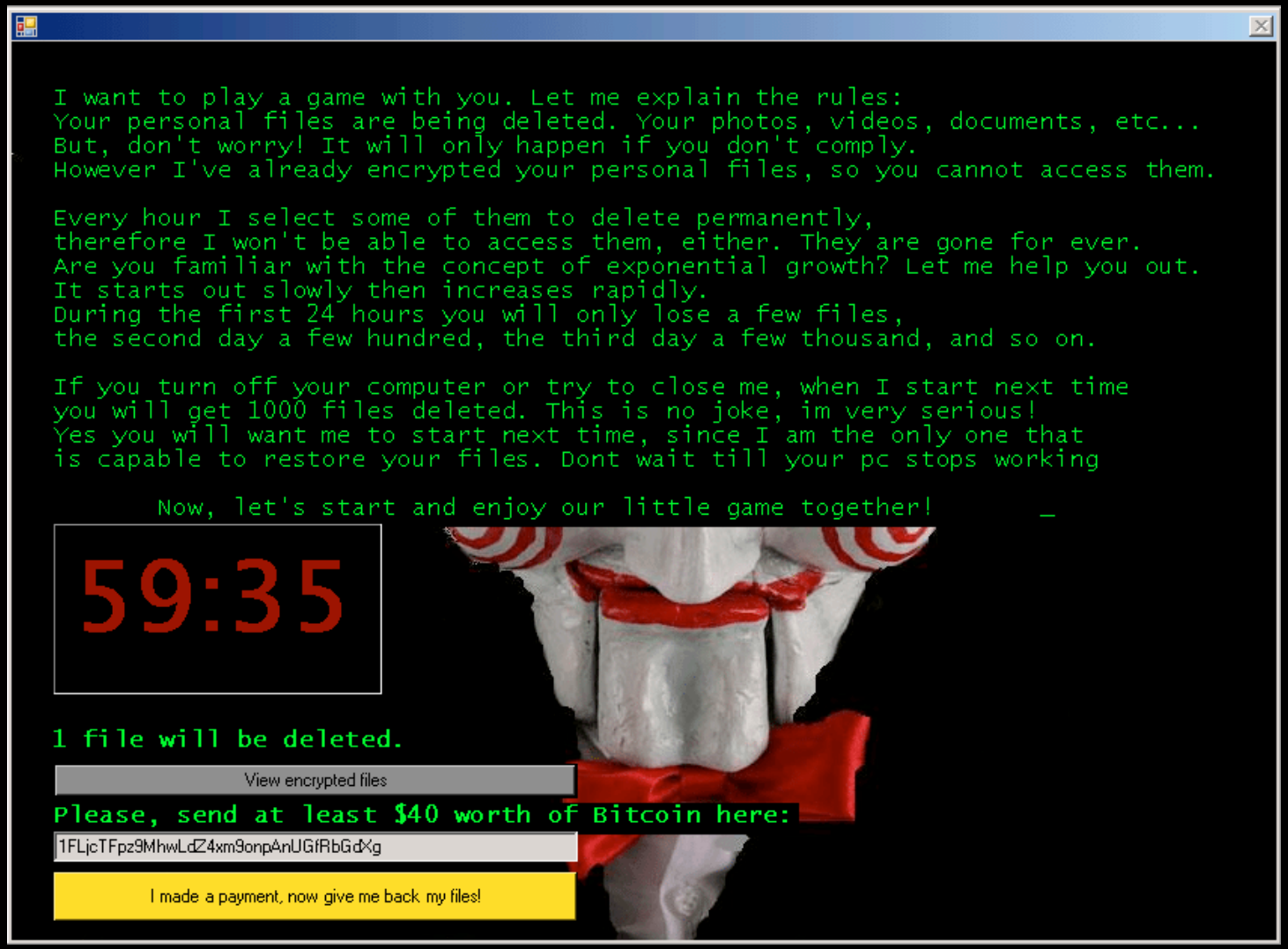

Les rançongiciels

Définition

Un rançongiciel (ransomware en anglais) est un logiciel informatique malveillant, prenant en otage les données. Le rançongiciel chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.

Exemples

Vous recevez une pièce jointe d’un client. Vous l’ouvrez. Une fenêtre d’un logiciel s’affiche et vous demande de l’argent contre vos données. Vous venez de découvrir que vos fichiers sont maintenant encryptés et un compte à rebours est amorcé.


I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.
Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either. They are gone for ever.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hours you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.
If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted. This is no joke, im very serious!
Yes you will want me to start next time, since I am the only one that
is capable to restore your files. Dont wait till your pc stops working
Now, let's start and enjoy our little game together!
59:35
1 file will be deleted.
View encrypted files
Please, send at least $40 worth of Bitcoin here:
1FLjcTFpz9MhwLdZ4xm9onpAnUGfRbGdXg
I made a payment, now give me back my files!

YOUR COMPUTER HAS BEEN LOCKED!

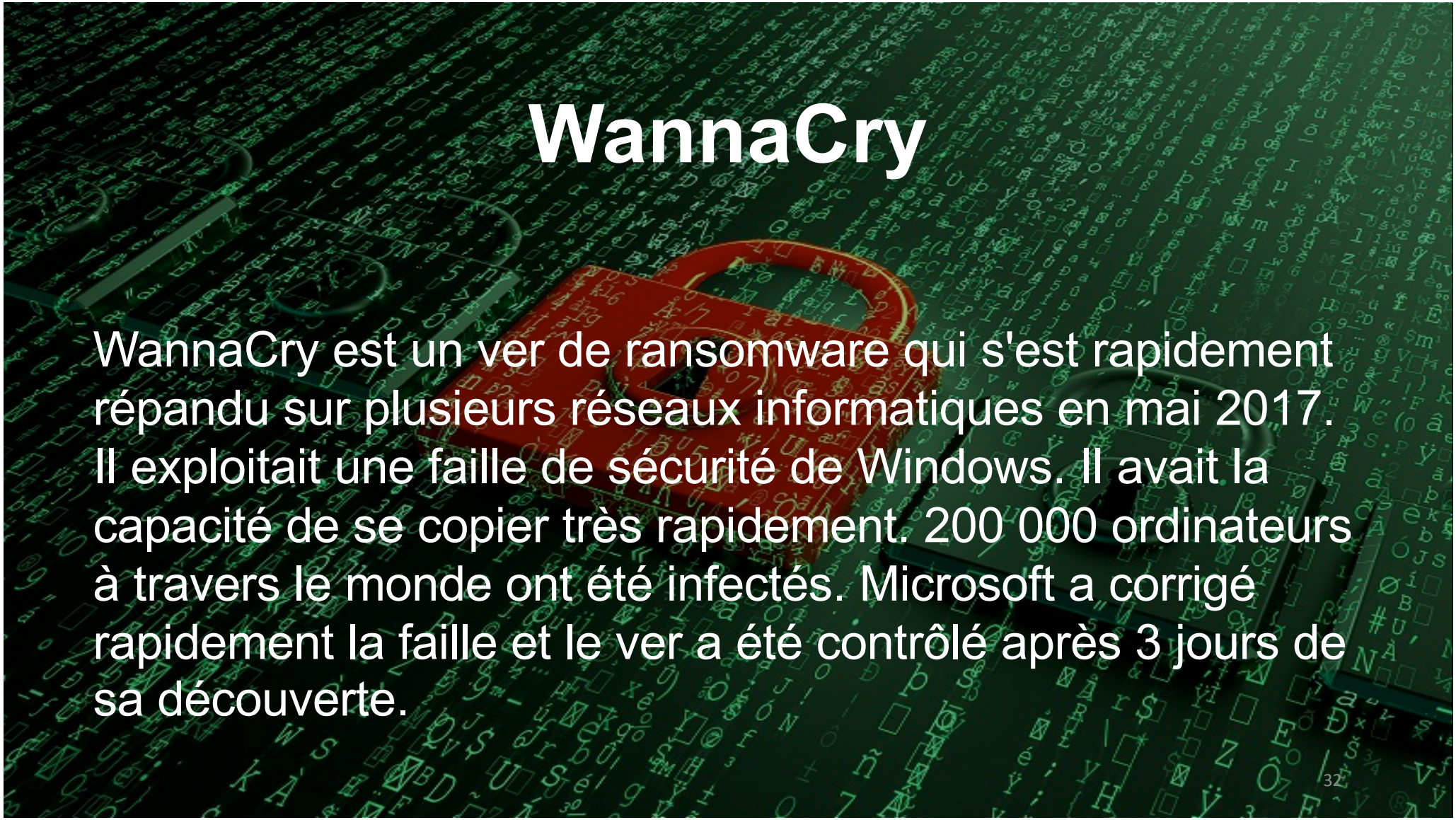
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

OK



WannaCry

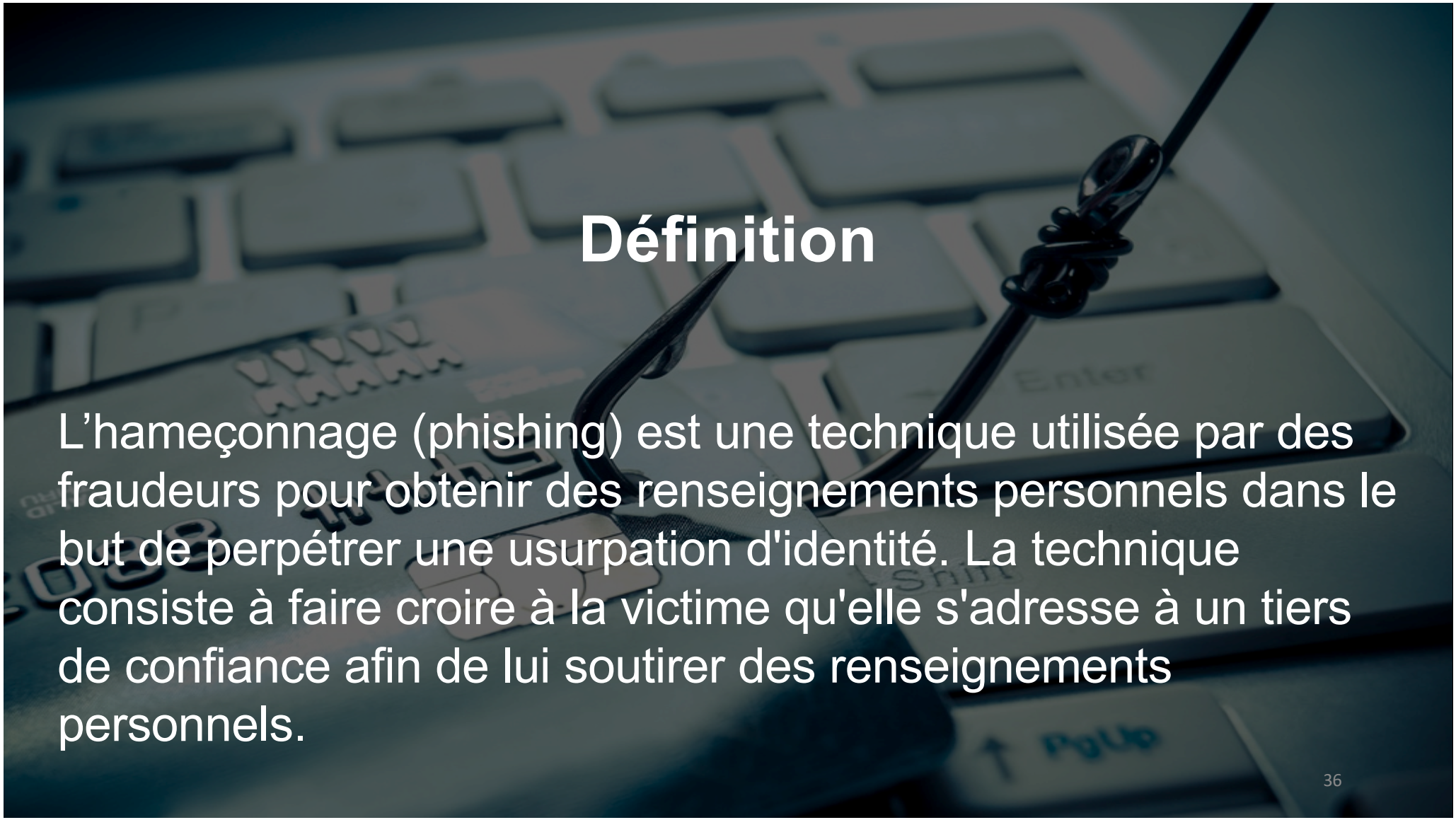
WannaCry est un ver de ransomware qui s'est rapidement répandu sur plusieurs réseaux informatiques en mai 2017. Il exploitait une faille de sécurité de Windows. Il avait la capacité de se copier très rapidement. 200 000 ordinateurs à travers le monde ont été infectés. Microsoft a corrigé rapidement la faille et le ver a été contrôlé après 3 jours de sa découverte.


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

Protection

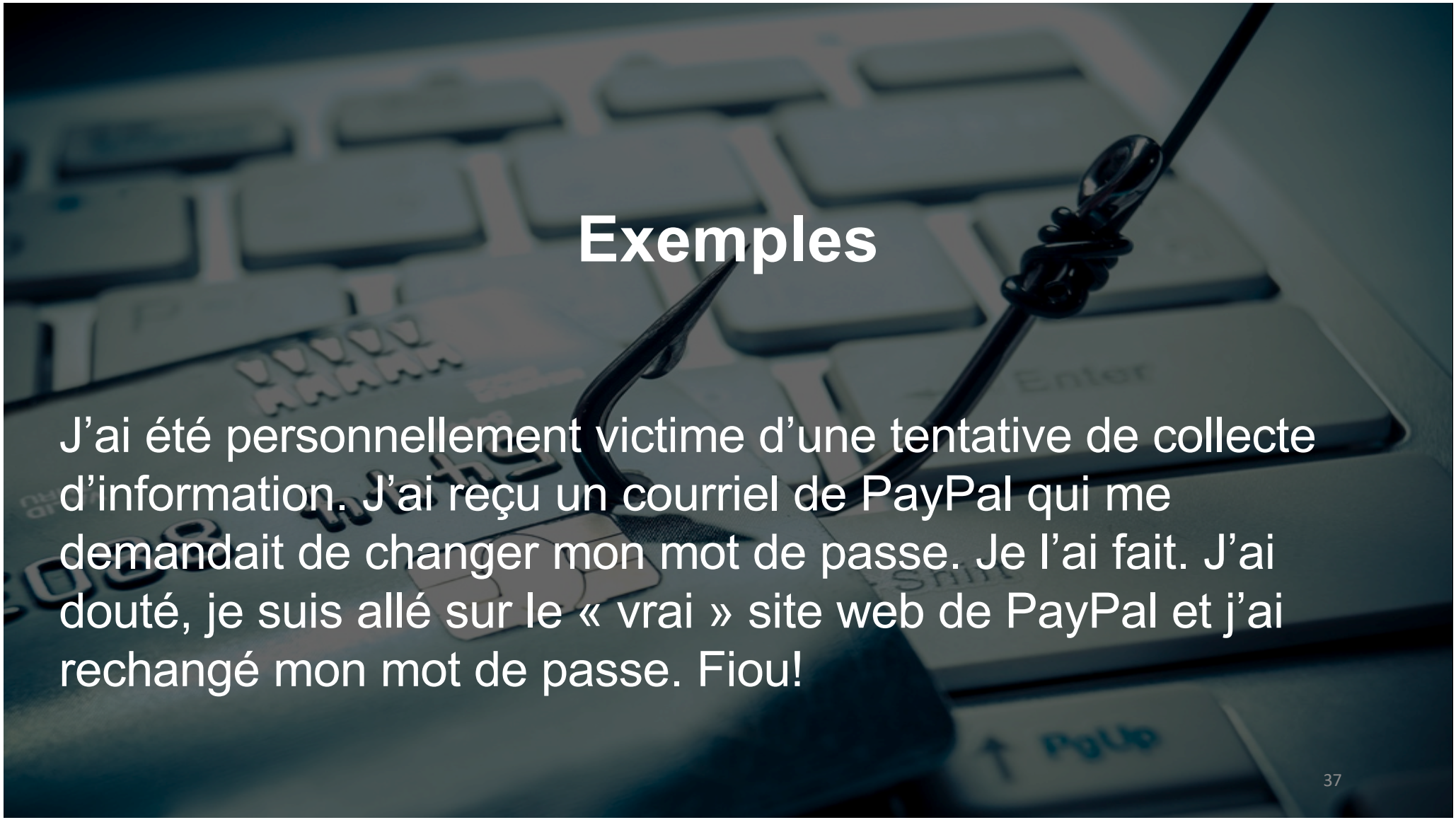
- N’ouvrez pas les pièces jointes d’une personne que vous ne connaissez pas.
- Ayez un anti-virus toujours à jour.
- Ayez des systèmes d’exploitation à jour.
- Ne soyez pas « administrateur » de votre ordinateur.
- Le plus important : FAITES VOS COPIES DE SÉCURITÉ **SOUVENT!**


L’hameçonnage



Définition

L’hameçonnage (phishing) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels.

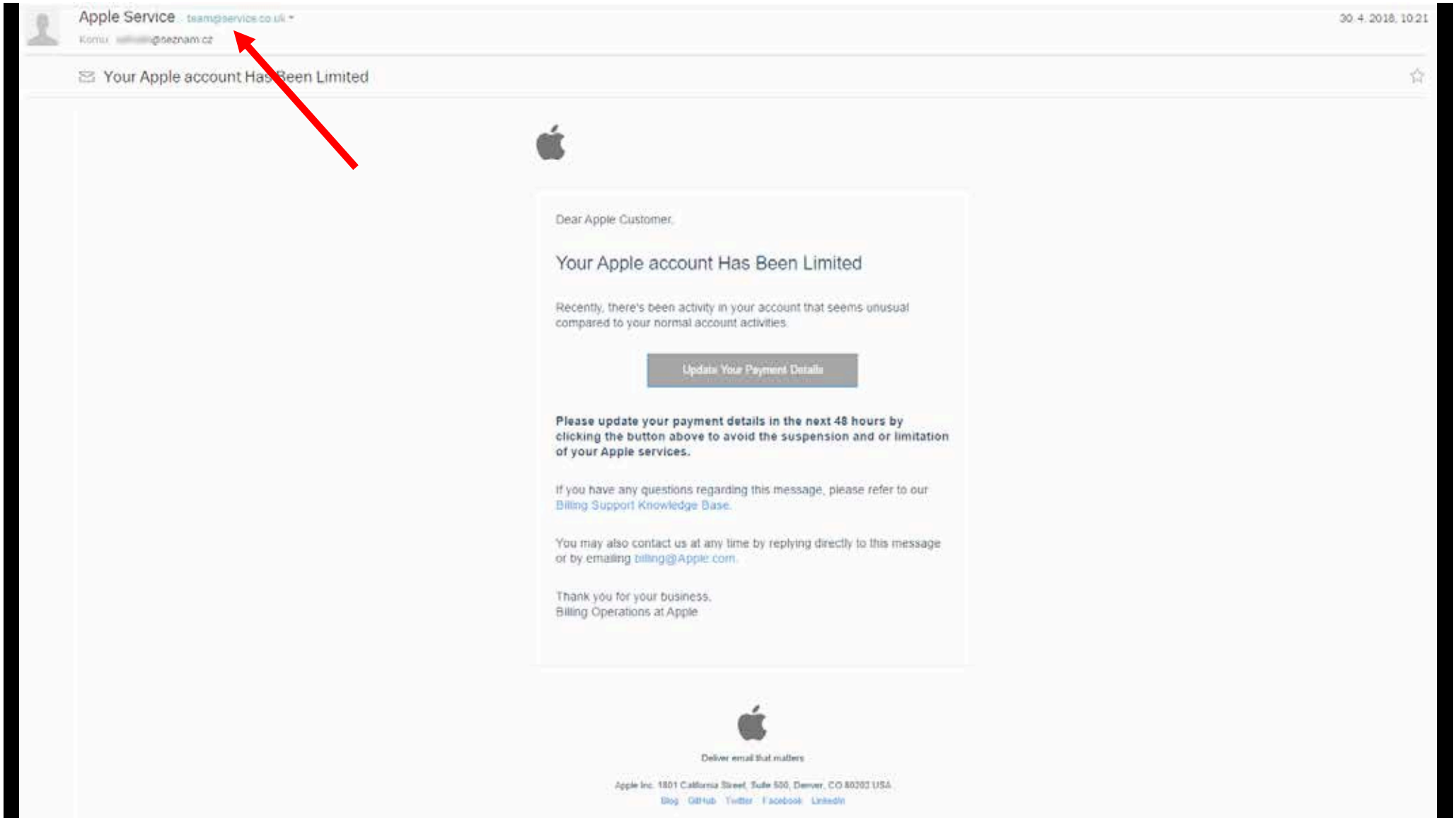


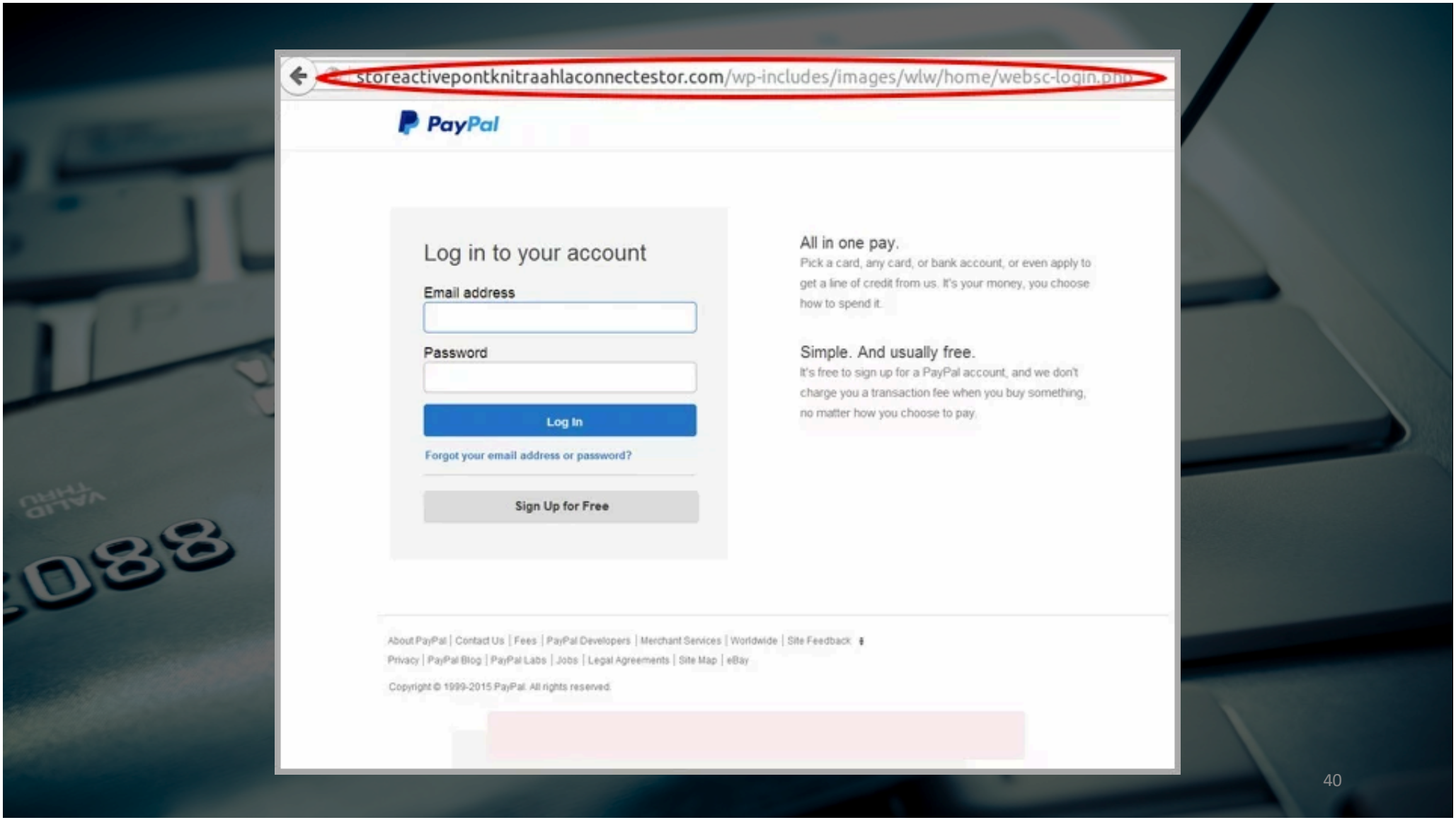
Exemples

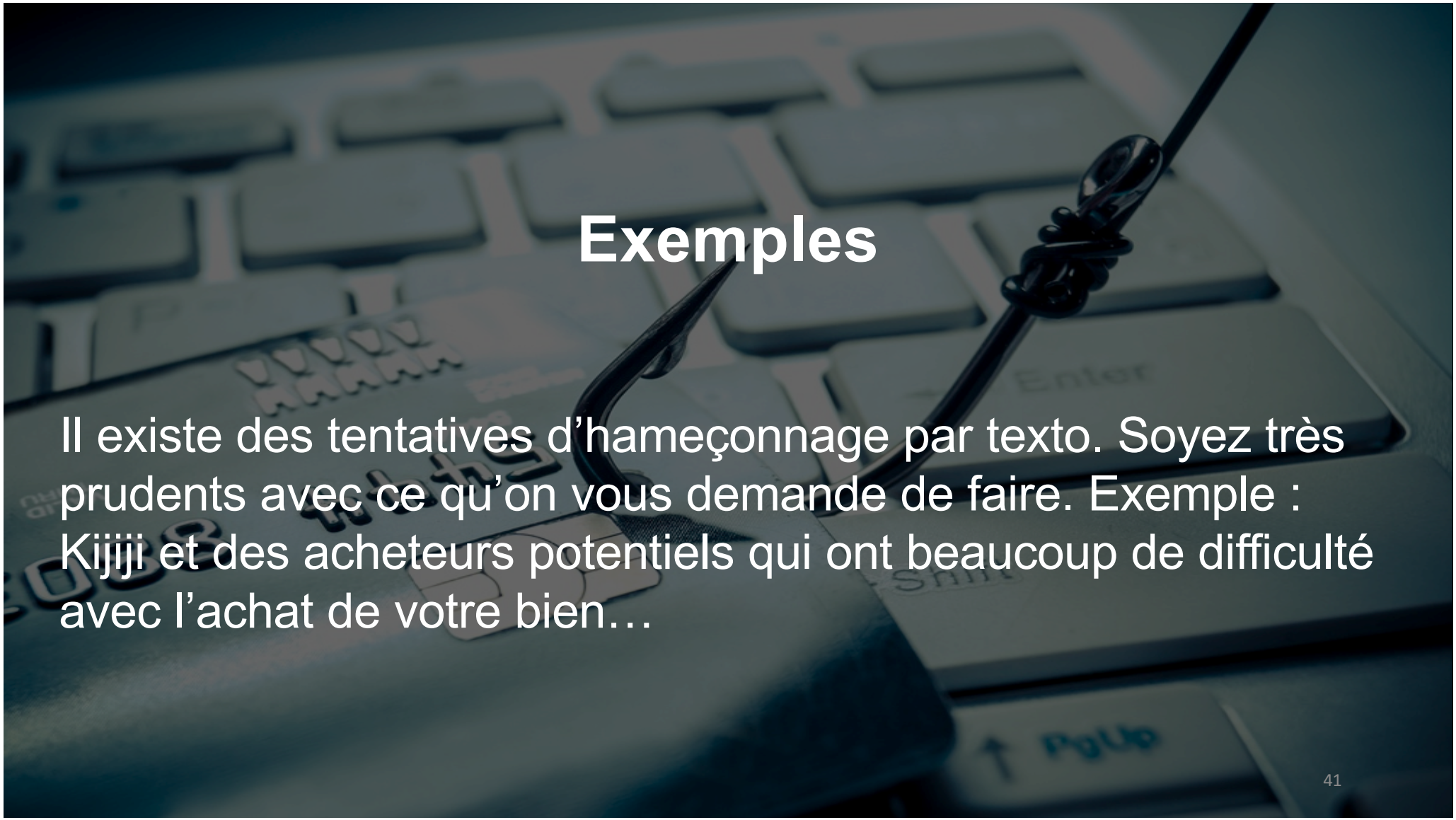
J’ai été personnellement victime d’une tentative de collecte d’information. J’ai reçu un courriel de PayPal qui me demandait de changer mon mot de passe. Je l’ai fait. J’ai douté, je suis allé sur le « vrai » site web de PayPal et j’ai rechangé mon mot de passe. Fiou!

Exemples

Les courriels sont toujours en lien avec les sites les plus populaires. Ce sont des messages envoyés automatiquement via des serveurs anonymes. La vraie arnaque : c'est de vous faire douter!

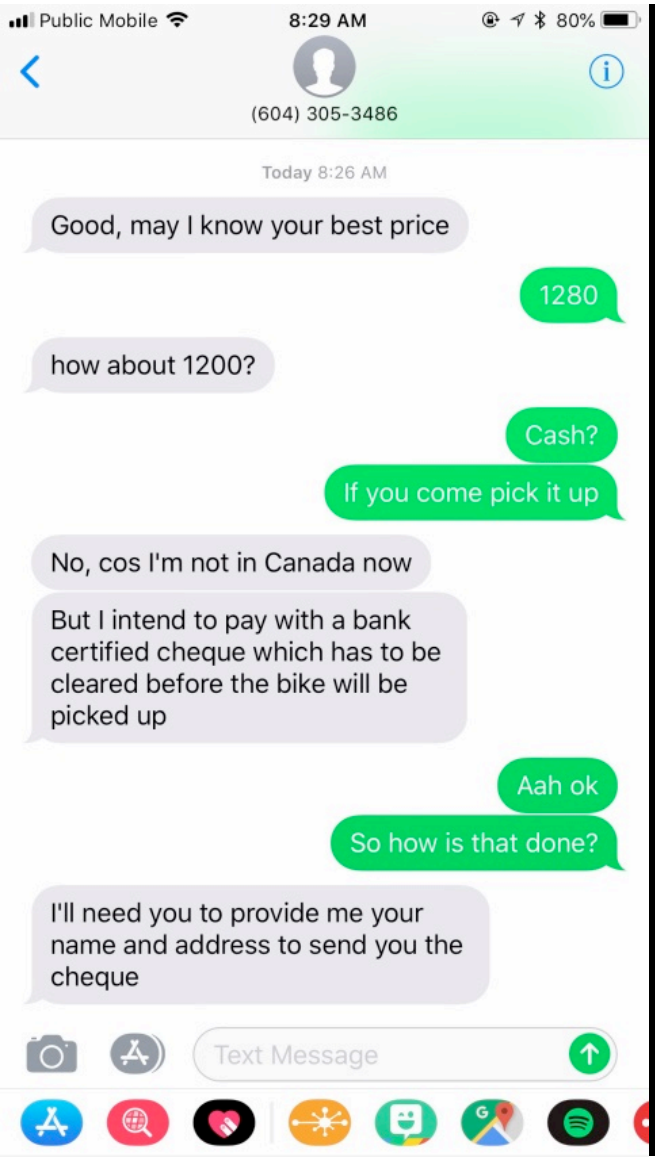

Apple Service team@service.co.uk
30. 4. 2018, 10:21
Your Apple account Has Been Limited
Dear Apple Customer,
Your Apple account Has Been Limited
Recently, there's been activity in your account that seems unusual compared to your normal account activities.
Update Your Payment Details
Please update your payment details in the next 48 hours by clicking the button above to avoid the suspension and or limitation of your Apple services.
If you have any questions regarding this message, please refer to our Billing Support Knowledge Base.
You may also contact us at any time by replying directly to this message or by emailing billing@Apple.com.
Thank you for your business.
Billing Operations at Apple
Deliver email that matters
Apple Inc. 1801 California Street, Suite 500, Denver, CO 80202 USA
Blog GitHub Twitter Facebook LinkedIn

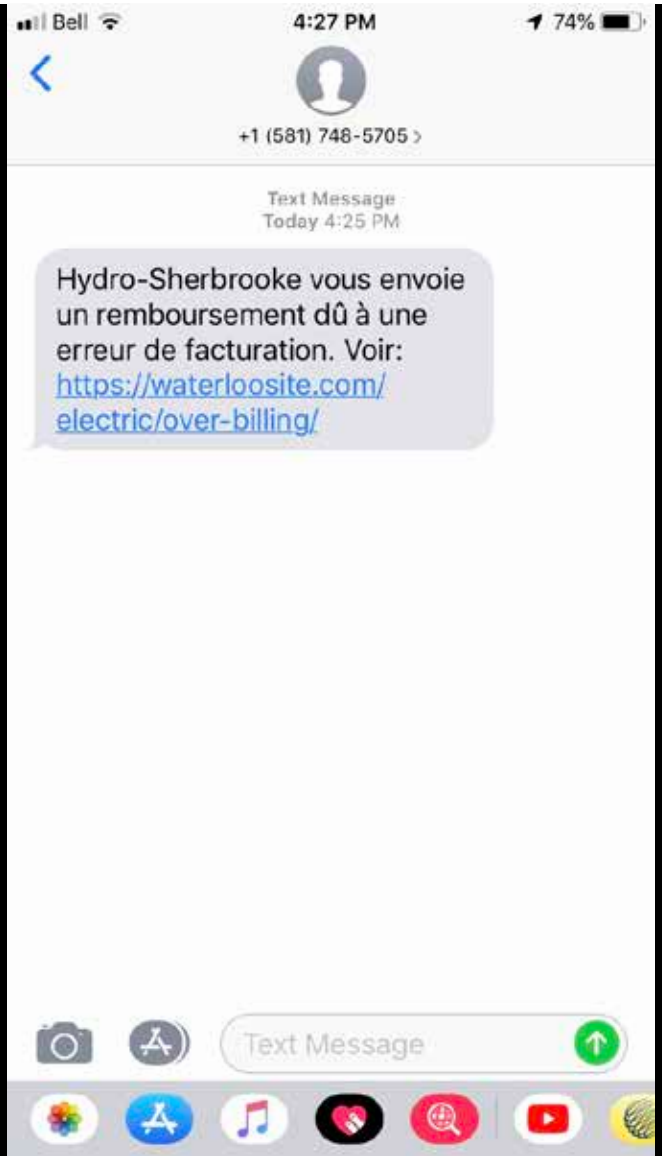

storeactivepontknitraahlaconnectestor.com/wp-includes/images/wlw/home/websc-login.php
PayPal
Log in to your account
Email address
Password
Log In
Forgot your email address or password?
Sign Up for Free
All in one pay.
Pick a card, any card, or bank account, or even apply to get a line of credit from us. It's your money, you choose how to spend it.
Simple. And usually free.
It's free to sign up for a PayPal account, and we don't charge you a transaction fee when you buy something, no matter how you choose to pay.
About PayPal | Contact Us | Fees | PayPal Developers | Merchant Services | Worldwide | Site Feedback
Privacy | PayPal Blog | PayPal Labs | Jobs | Legal Agreements | Site Map | eBay
Copyright © 1999-2015 PayPal. All rights reserved.



Exemples

Il existe des tentatives d'hameçonnage par texto. Soyez très prudents avec ce qu'on vous demande de faire. Exemple : Kijiji et des acheteurs potentiels qui ont beaucoup de difficulté avec l'achat de votre bien…





[redacted] your Apple ID is due to expire today. To prevent termination confirm your details at http://appleidlogin.co.uk - Apple Support.

Text Message
Today 11:33 AM

RBC Alert!
Your client card starting with '4519' has been disabled.
Please secure your account below.
http://rbc.com.ssl-sec-mls-119.com/r/

Protection

- Aucune banque ne vous contactera pour changer un mot de passe!
- Aucun site web comme PayPal ne vous contactera sauf pour vous passer un message.
- Rester prudent avec les transactions de vente en ligne.
- Examinez les liens en passant votre souris dessus. Vous allez voir la « vraie » adresse qui se cache derrière le lien.
- Surtout : ne cliquez pas sur les liens du message. Allez directement en ligne sur le « vrai » site pour vous connecter.


Conclusion

Protection

- Soyez au courant des tendances du web.
- Utilisez vos appareils avec prudence, surtout pour des transactions.
- Soyez certain de l'identité de votre interlocuteur.
- Installez des logiciels de fournisseurs que vous connaissez.
- Ayez des procédures de sécurité en lien avec vos données.
- Le plus important : FAITES VOS COPIES DE SÉCURITÉ **SOUVENT!**

Si jamais vous êtes victime

Centre antifraude du Canada

http://www.antifraudcentre-centreantifraude.ca/index-fra.htm

Le 20 juin dernier Desjardins dévoilait que 2,7 millions de ses membres étaient touchés par un vol de données personnelles. C'est 60 % des particuliers clients de l'institution financière québécoise qui risquent maintenant de se faire voler leur identité.

Desjardins annonçait le 1er novembre **les 4,2 millions de membres particuliers de Desjardins sont touchés par la fuite de renseignements personnels communiquée le 20 juin dernier**.


Merci!