

TECHNIQUES DE PHISHING

ET COMMENT S'EN PROTÉGER

Morgan Hotonnier

*<f> pour mettre en plein écran,
<espace> pour continuer*

PHISHQUOI?

- Aussi appelée "hammeçonnage" en français
- Technique cherchant à vous **manipuler** pour
 - révéler des informations sensibles
 - installer a malware
 - envoyer de l'argent
 - une combinaison des points ci-dessus et plus encore

TYPES DE PHISHING

- Phishing "de masse"
- **Spear phishing** : Harponnage
- **Whaling** : Chasse à la baleine



SPEAR PHISHING

*Bonjour <votre nom>, vous avez reçu une
facture de <votre FAI>*

A black and white photograph of a person wearing a dark hoodie with a logo on the chest. They are holding a long, thin spearfishing harpoon gun with both hands, pointing it upwards. The background is dark and out of focus.

QU'EST CE QUE SPEAR PHISHING

- Phishing de meilleur qualité
- Personnalisé pour un groupe d'individus
- Peut utiliser des données personnelles récoltées auparavant (hack, réseaux sociaux...)

SPEAR PHISHING - EXEMPLE

Telia **FAKTURA**

Sven Svensson

Faktura för Telia Säker lagring Extra

OCR-nr:	1877-277506
Datum:	2016-05-24
Belopp:	459 kronor
Förfallodag:	31 maj 2016

[Visa Faktura](#) [Betala Faktura](#)

Din integriteit hos Telia

För att kunna erbjuda dig den allra bästa servicen, de bästa tjänsterna och för att kunna hjälpa dig om du har frågor så behöver vi spara olika uppgifter om dig. Vårt främsta fokus är alltid att skydda våra kunders integritet. Därför sparar vi aldrig uppgifterna längre än vi behöver. Viss information slängs direkt, annan sparas olika lång tid beroende på vad uppgifterna ska användas till och vad lagen säger. All information hanteras under mycket strikta regler. Inom olika områden anlitar vi leverantörer för att kunna leverera våra tjänster, vilket innebär att även de behöver viss information om våra kunder.

© Telia 556430-0142 Box 50077, 973 22 Luleå Säte: Stockholm

A dramatic photograph of a whale breaching, with its massive body arched out of dark blue water. The whale's skin is textured and mottled with white. The background is a bright, overcast sky.

WHALING

Il faut virer 2000 euro de toute urgence sur ce compte étranger? C'est confidentiel, surtout n'en parle à personne

QU'EST CE QUE LE WHALING

- Spearphishing++
- Cible de "gros poissons" (personnes riches ou avec des accès privilégiés)
 - CEO, CFO, etc
- Recherche au préalable sur les victimes, utilisation du jargon d'entreprise
- Fameuse "fraude au président"

EXEMPLE DE WHALING

● Mary CEO

To: Joe.CFO@example.com

18 February 2016 at 11:00 AM

Hi Joe

Hi Joe

Are you in the office? Kindly let me know because i need you to send out an important payment for me today.

Thank you,

Mary CEO

Sent from my iPhone

PAS SEULEMENT DES EMAILS!

- Vishing
- Smishing
- Réseaux sociaux

VISHING

*"Bonjour, je fais partie du service technique
de Microsoft, votre PC est infecté par un
virus"*

LE VISHING, C'EST QUOI?

- Phishing par téléphone
 - Demande plus d'investissement de l'attaquant...
 - Mais bien plus efficace :)
- Des centres d'appel entiers dédiés à ce type d'arnaque
- Ne vous fiez pas à l'identification de l'appelant sur votre téléphone



Vishers are posing as IRS Agents



Threatening parties with police arrest, deportation, license revocation, etc.

IRS reports from January 2016 show that since October 2013:



896,000

people have been **solicited**

by **scammers** claiming
to be IRS officials



5,000
VICTIMS HAVE COLLECTIVELY
PAID OVER \$26.5 MILLION

AS A RESULT

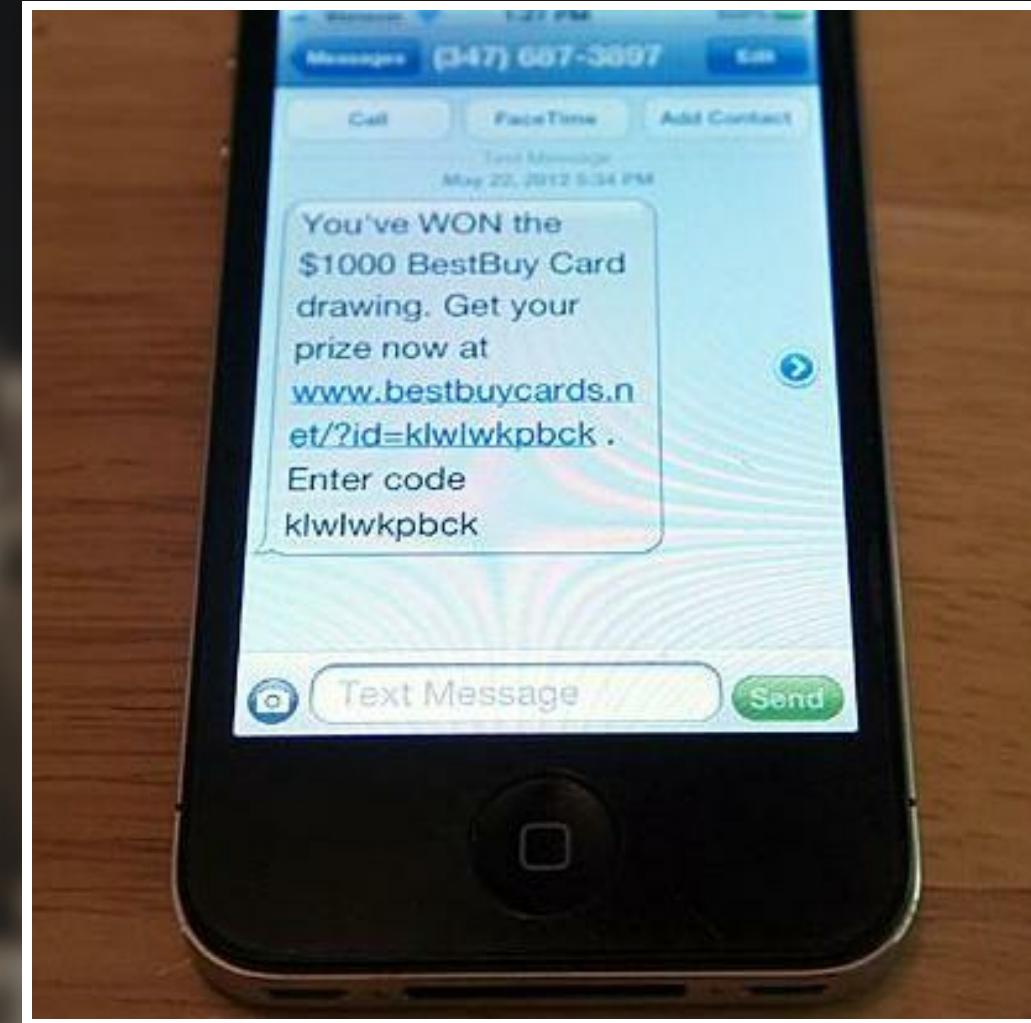
SMISHING

"Vous avez reçu un MMS, cliquez [ici](#) pour le consulter"

SMISHING : EXEMPLE



Quand c'est trop beau pour être vrai...



...ce n'est probablement pas vrai.



PHISHING & RÉSEAUX SOCIAUX

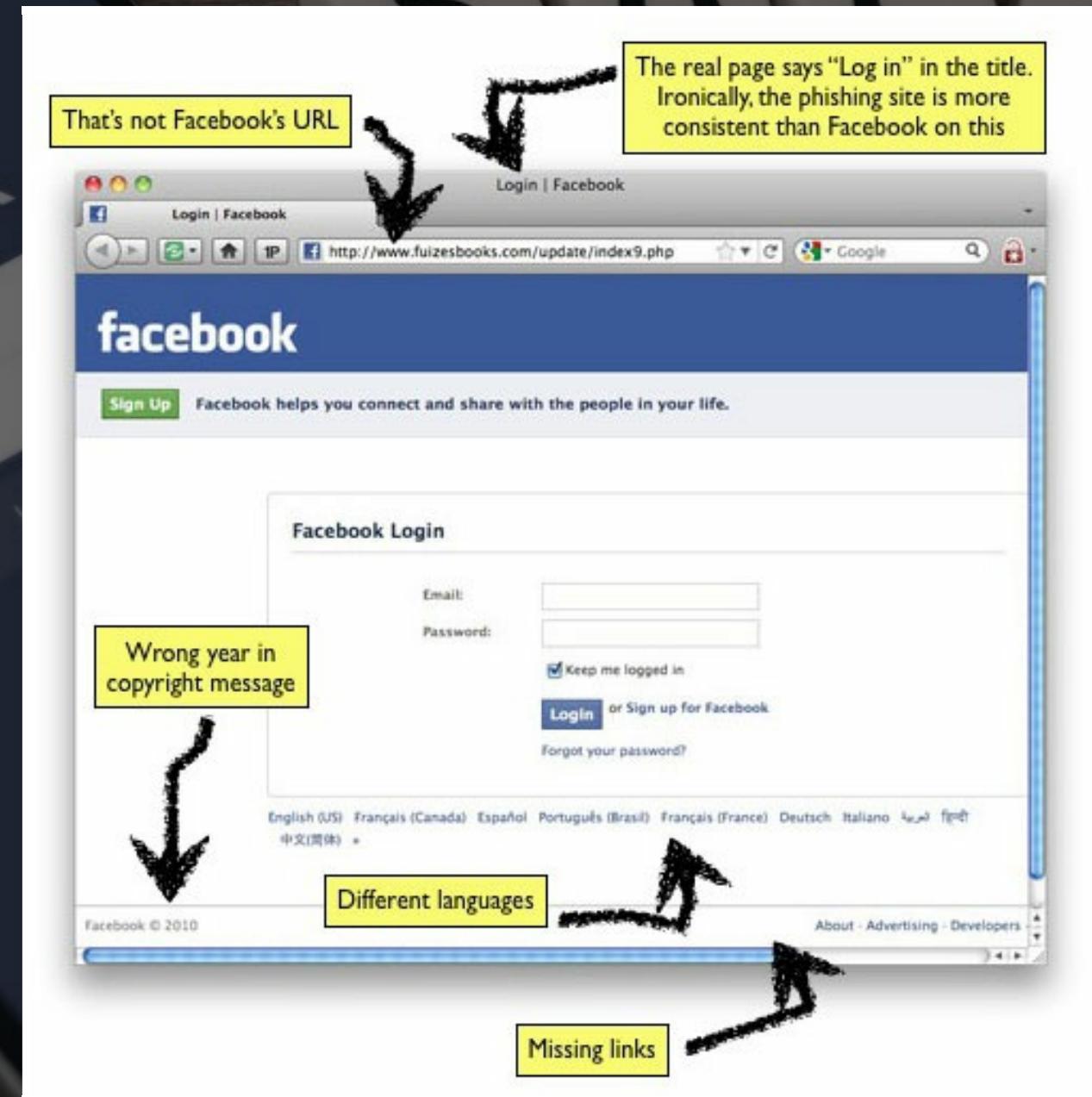
Comme toujours, on se base sur des faiblesses universelles

- Curiosité
- Peur (de voir son compte cloturé par exemple)
- Sexe

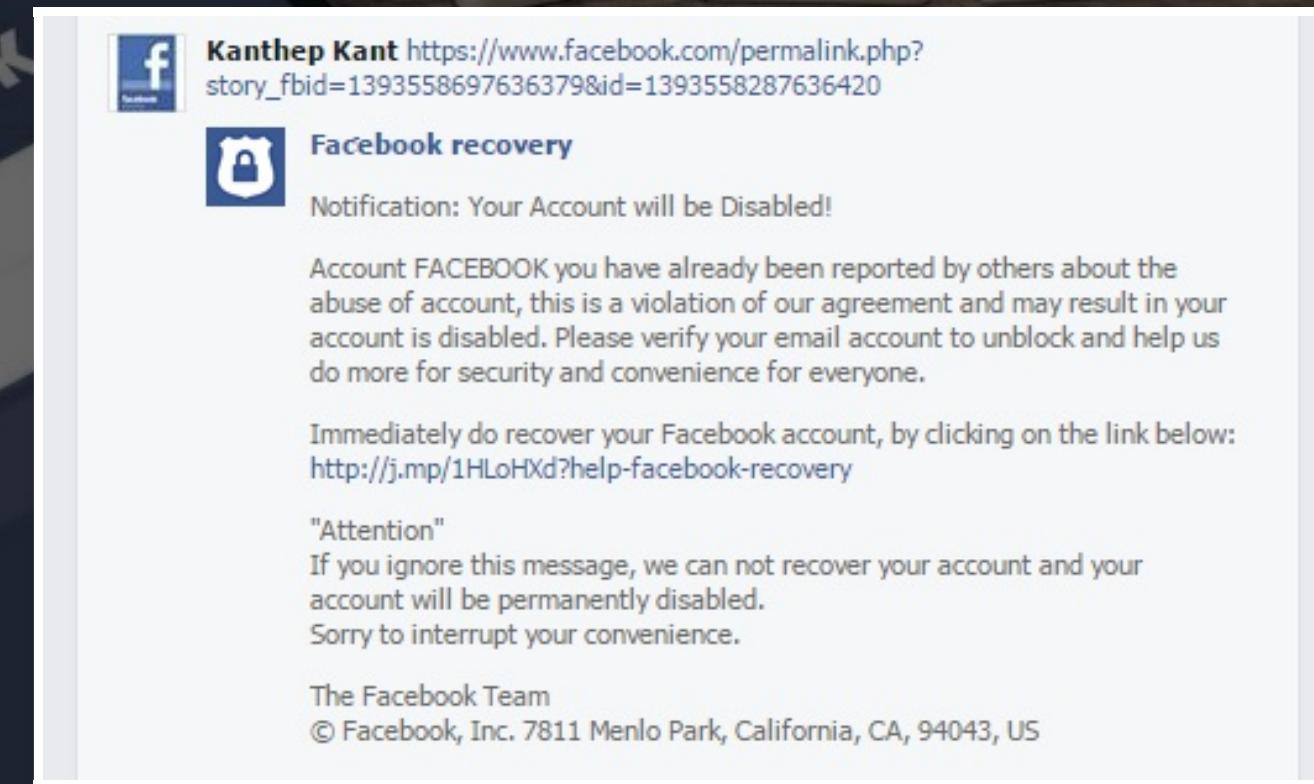
La curiosité est un vilain défaut



Ah zut je dois me reconnecter...attend, pourquoi?

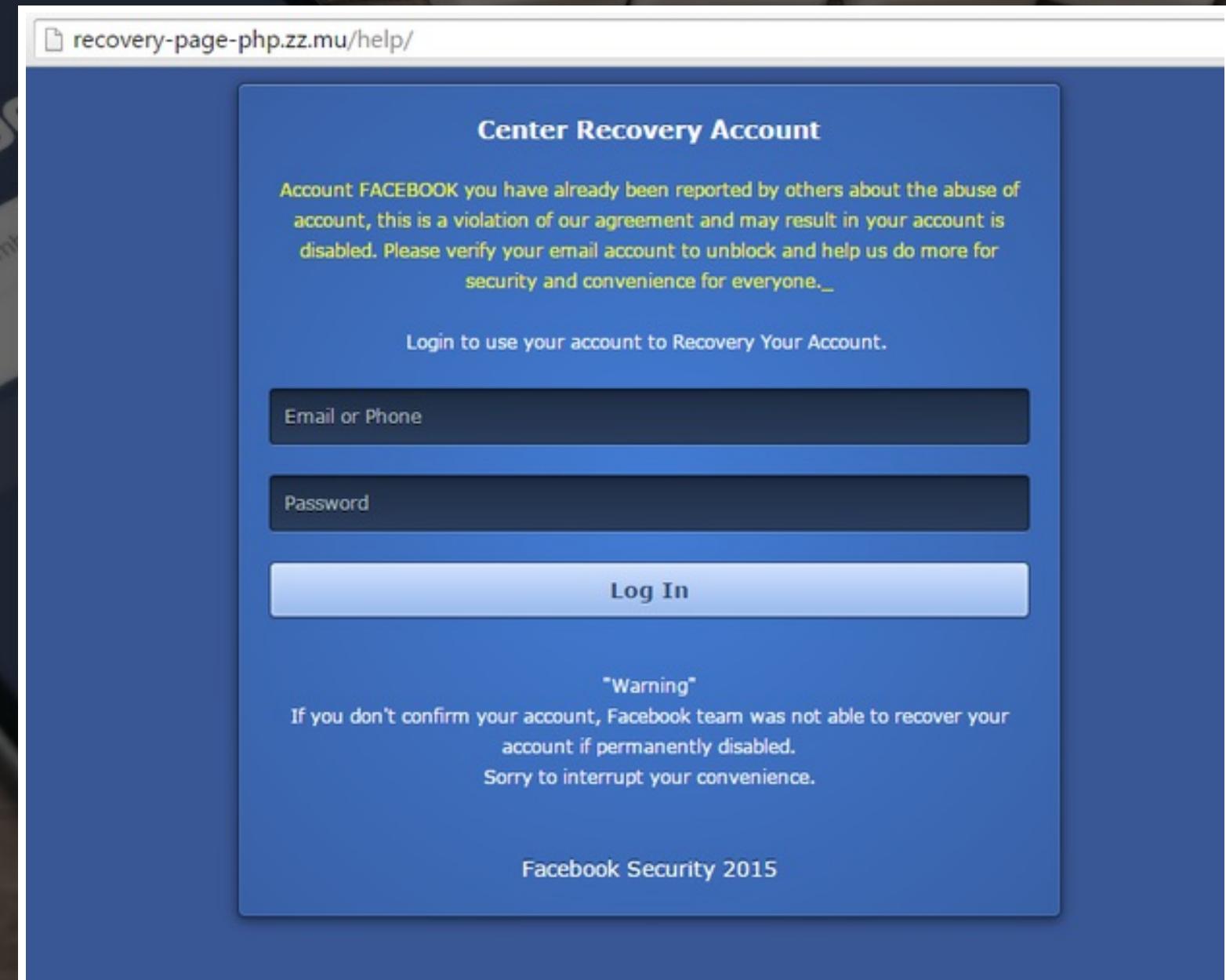


Si tu n'obtempère pas, ton compte sera définitivement fermé!



On ne rigole pas avec la police Facebook!

Il a vraiment cliqué? ...bon, Jacque a dit, donne moi ton mot de passe!



Il l'a fait?!

...Jacque a dit: donne moi ton numéro de carte!



Payment

f Enter your credit card

Payment page you were laid off, please upgrade your credit card again to return the payment in Facebook.

Full Name

Card Number XXXX XXXX XXXX XXXX

Card Type Select

Expiration Date MM / YY

Security Code (CVV) XXX [?]

Billing Address

City/Town

Province/Region

Zip/Postal Code

Country Select

Add **Reset**

Facebook will save your Credit Card data information for future purchases. You can always remove or manage this information in your account settings.

 Norton
SECURED
powered by VeriSign

“Cachez moi ce sein que je ne saurais voir.”

http://www.facebook.com/home.php?#!/search/?q=this is without a doubt the most hilarious video ever. LOL!&gl=1&lo=en_US

Latest Headlines

Lamar Johnson this is without a doubt the most hilarious video ever. LOL!

Naughty Camera Prank! [HQ]
apps.facebook.com
Length: 3:17

3 minutes ago

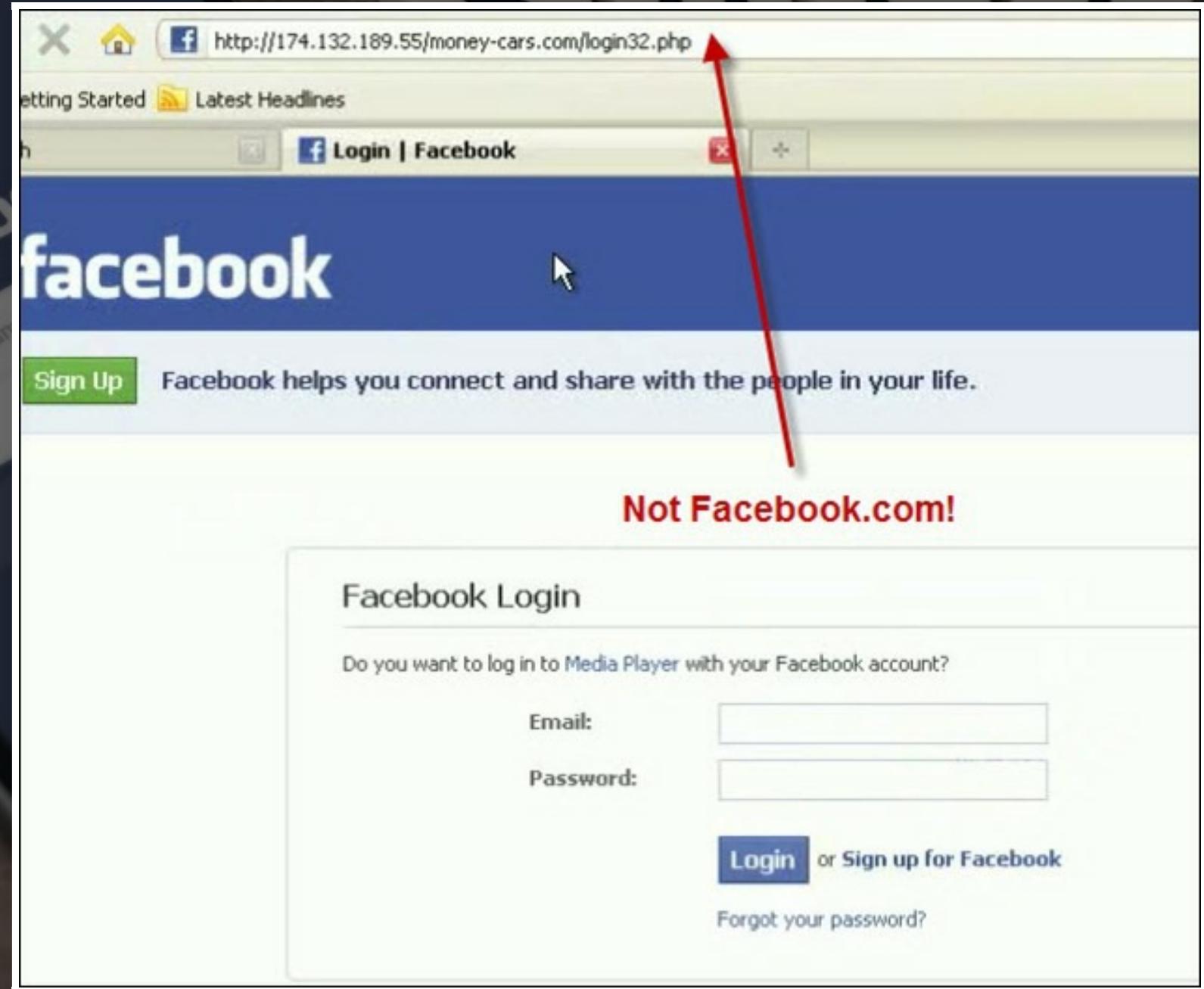
Thadeus Ngiela this is without a doubt the most hilarious video ever. LOL!

Naughty Camera Prank! [HQ]
apps.facebook.com
Length: 3:17

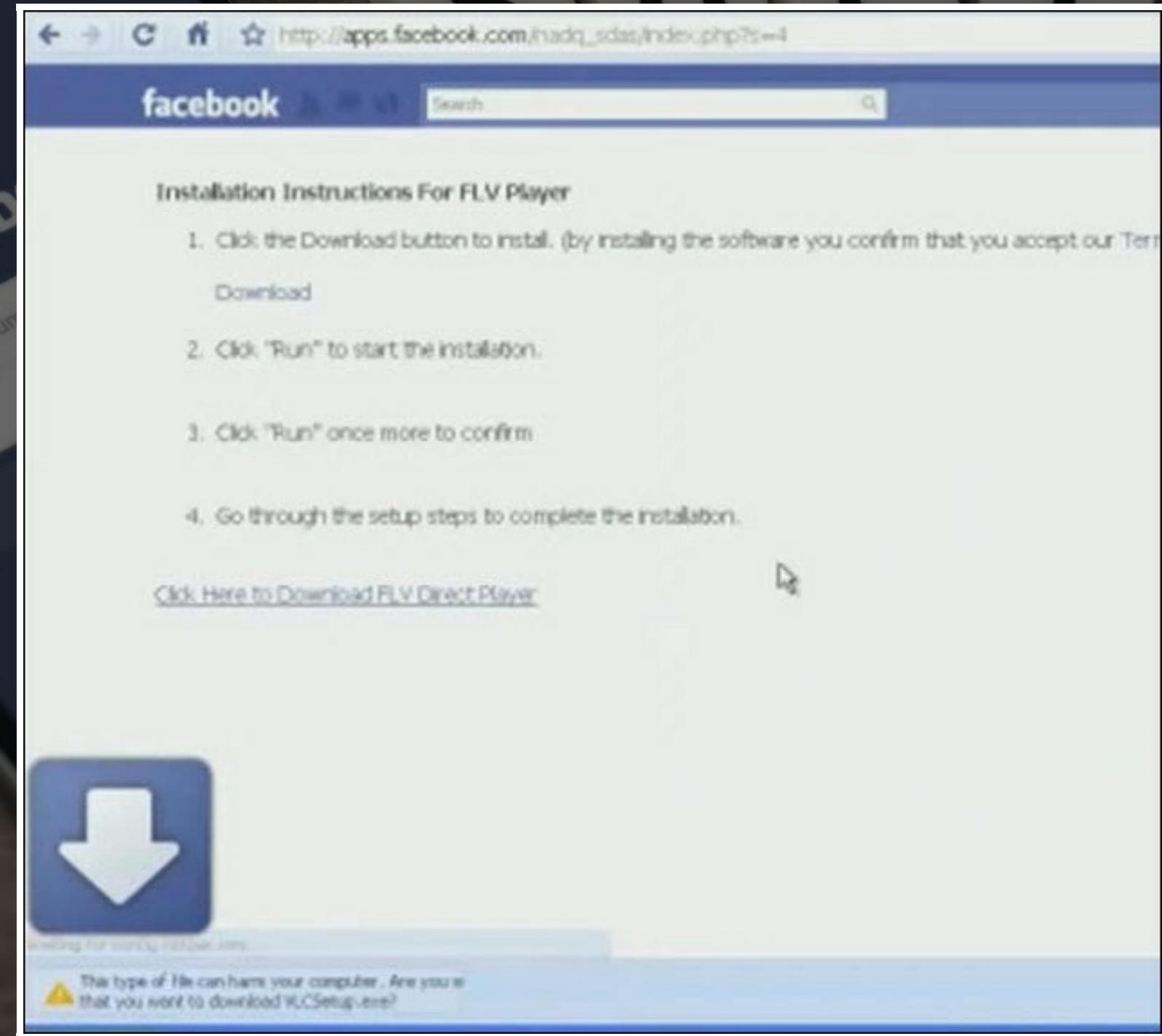
4 minutes ago

5 minutes ago

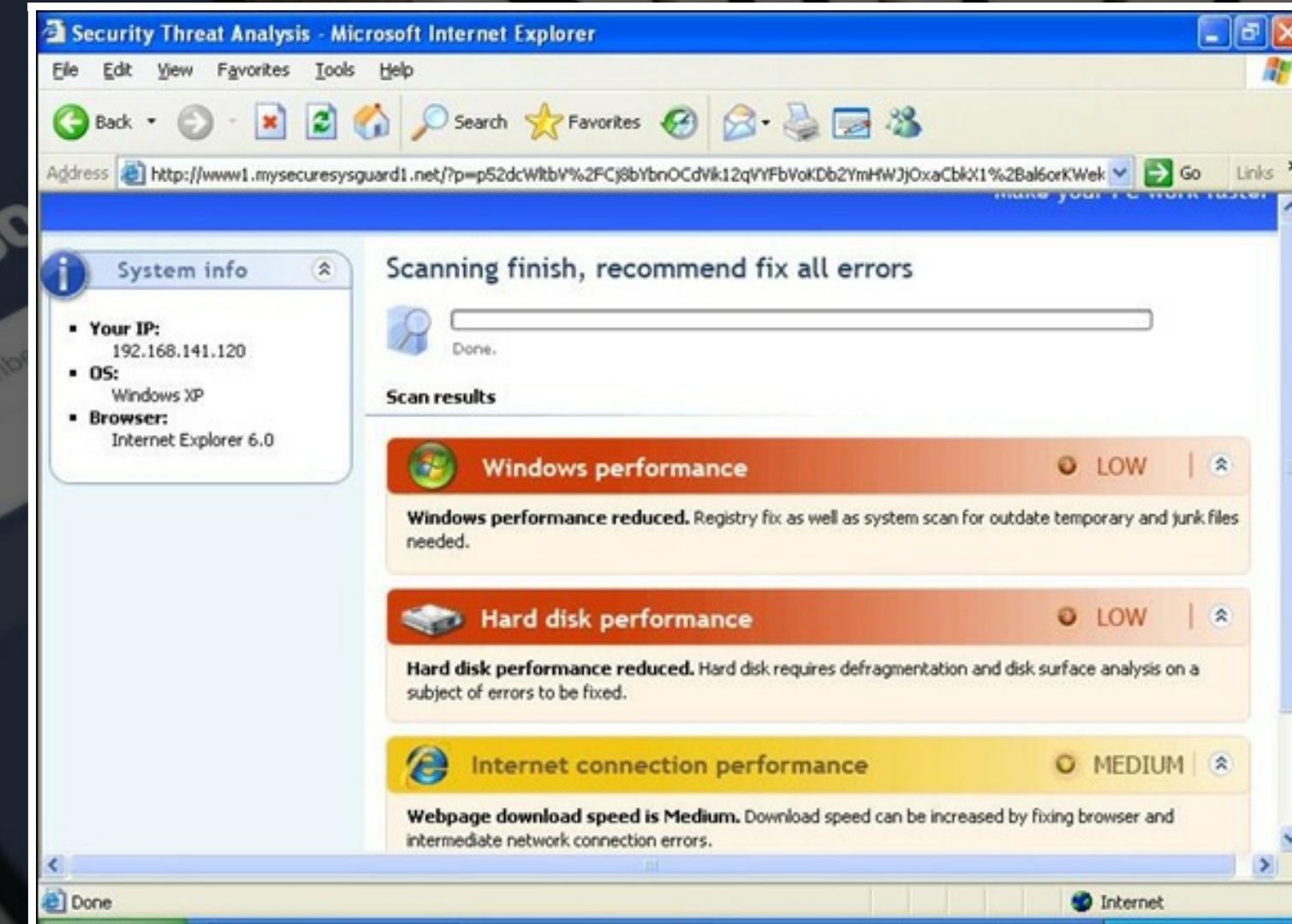
Tu connais la routine, envoie ton mot de passe



Ah oui, il faut aussi que tu télécharges ce faux plugin vidéo



Oh, tu as un virus! #SansBlague

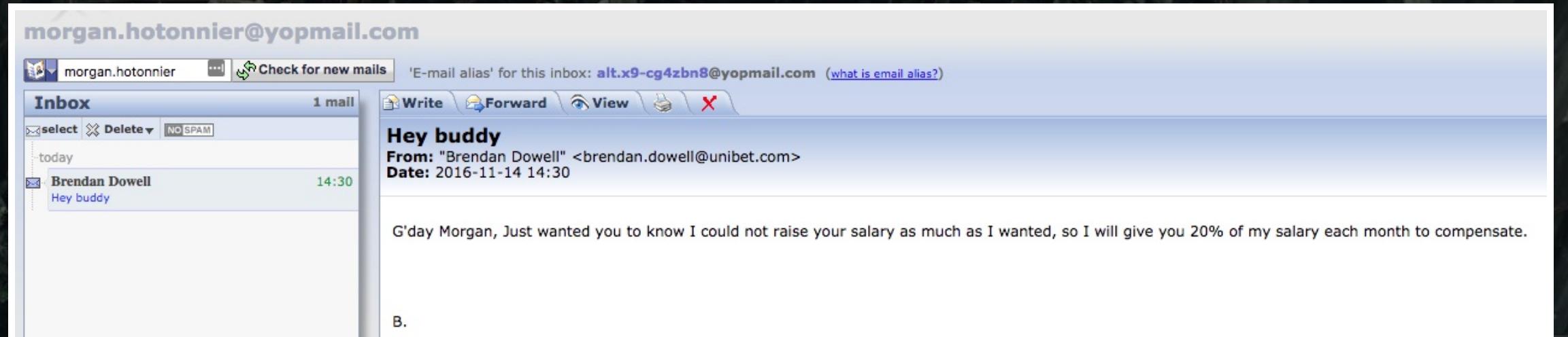


Achète mon antivirus et tous tes soucis disparaîtront!

SPOOFING (USURPATION)

Technique de phishing simple et efficace

Usurper une adresse email est un jeu d'enfant





Trafiguer un lien est très simple également

Par exemple, allons sur google.com

Fake Your Caller ID

Show any number as your own on any phone, and change your voice to sound like a man or a woman.

L'IDENTIFICATION DE L'APPELANT?
MÊME COMBAT



A black and white photograph of a knight in full armor. He is wearing a helmet with a visor, chainmail, and leather gauntlets. He is holding a long-sword with both hands. The lighting is dramatic, highlighting the metallic surfaces of the armor against a dark background.

COMMENT SE PROTÉGER ?

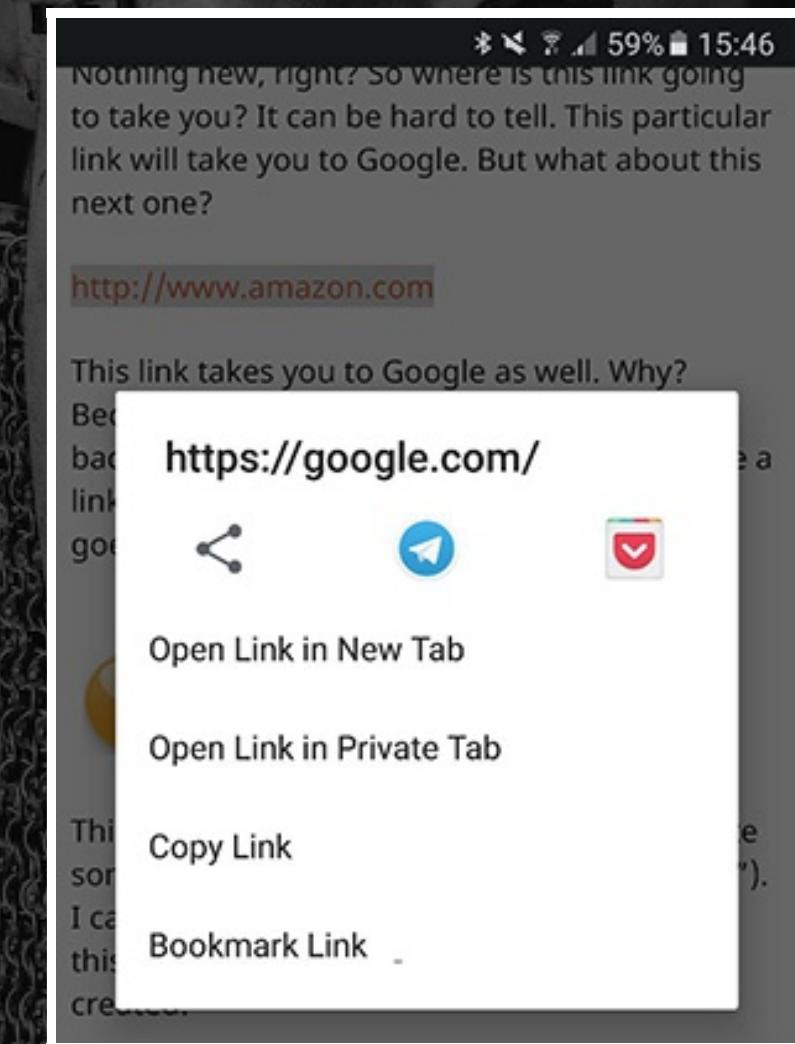
RESTEZ VIGILENT

Ne jamais prendre pour argent comptant ce qui est affiché

- Identification de l'appelant
- URL
 - Sauf dans la barre d'adresse du navigateur
 - Ou dans l'infobulle en survolant un lien
- Expéditeur d'un email
 - Pour les geeks: allez fouiller dans les entêtes

LIENS & SMARTPHONE

- Un appui long permet d'afficher la destination réelle



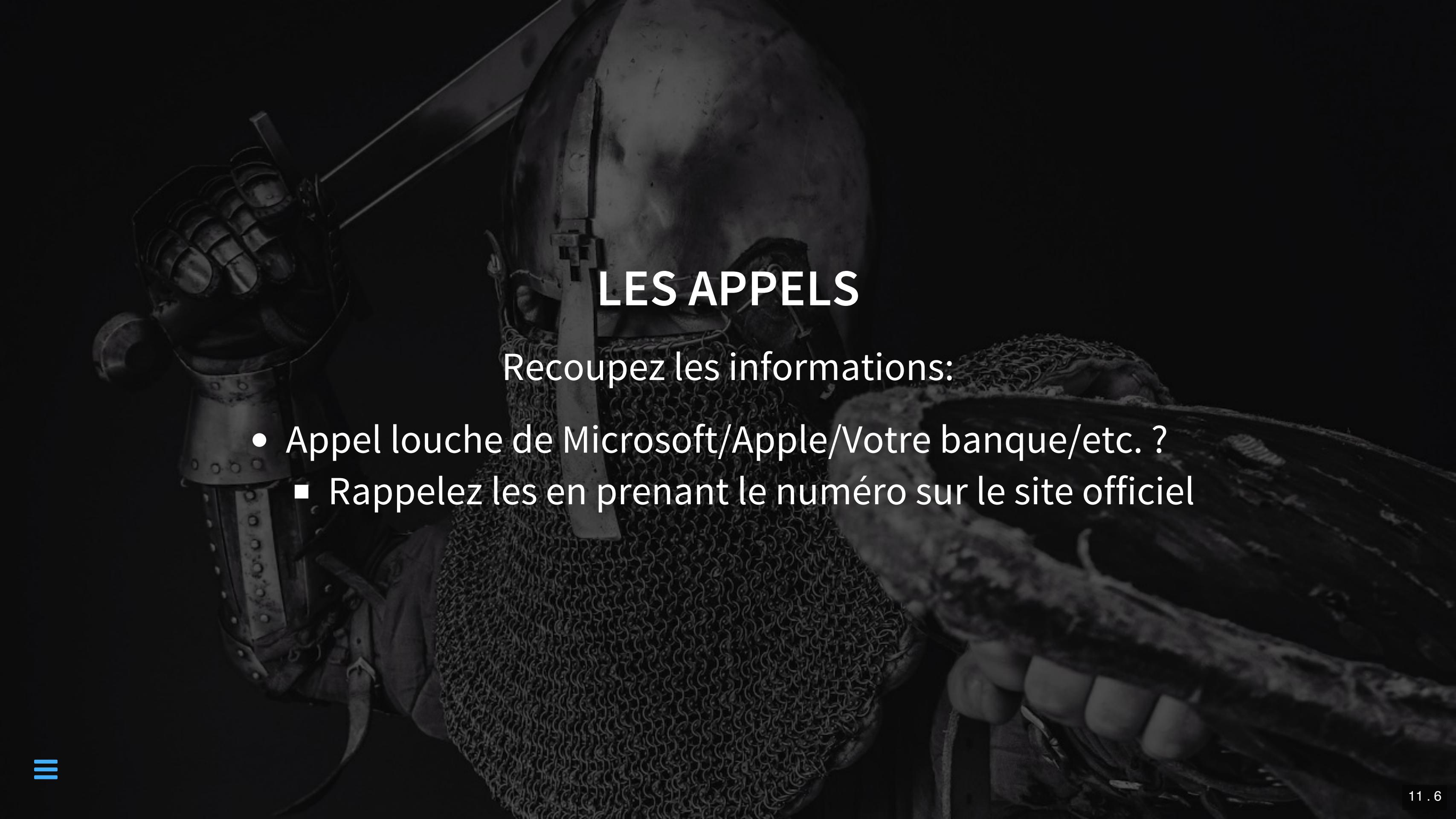
BARRE D'ADRESSE & SMARTPHONE

- Les navigateurs sur smartphone ont tendance à la cacher
 - Cela gagne de l'espace sur l'écran, mais à quel prix...
 - Remonter la page et elle devrait réapparaître

LES EMAILS

Recoupez les informations:

- Email louche d'un ami/collègue?
 - Essayez de le contacter par un autre moyen

A black and white photograph of a knight in full armor. The knight is shown from the waist up, wearing a helmet with a plume and a chainmail hauberk. A broadsword is strapped to their side. The background is dark and textured.

LES APPELS

Recoupez les informations:

- Appel louche de Microsoft/Apple/Votre banque/etc. ?
 - Rappelez les en prenant le numéro sur le site officiel

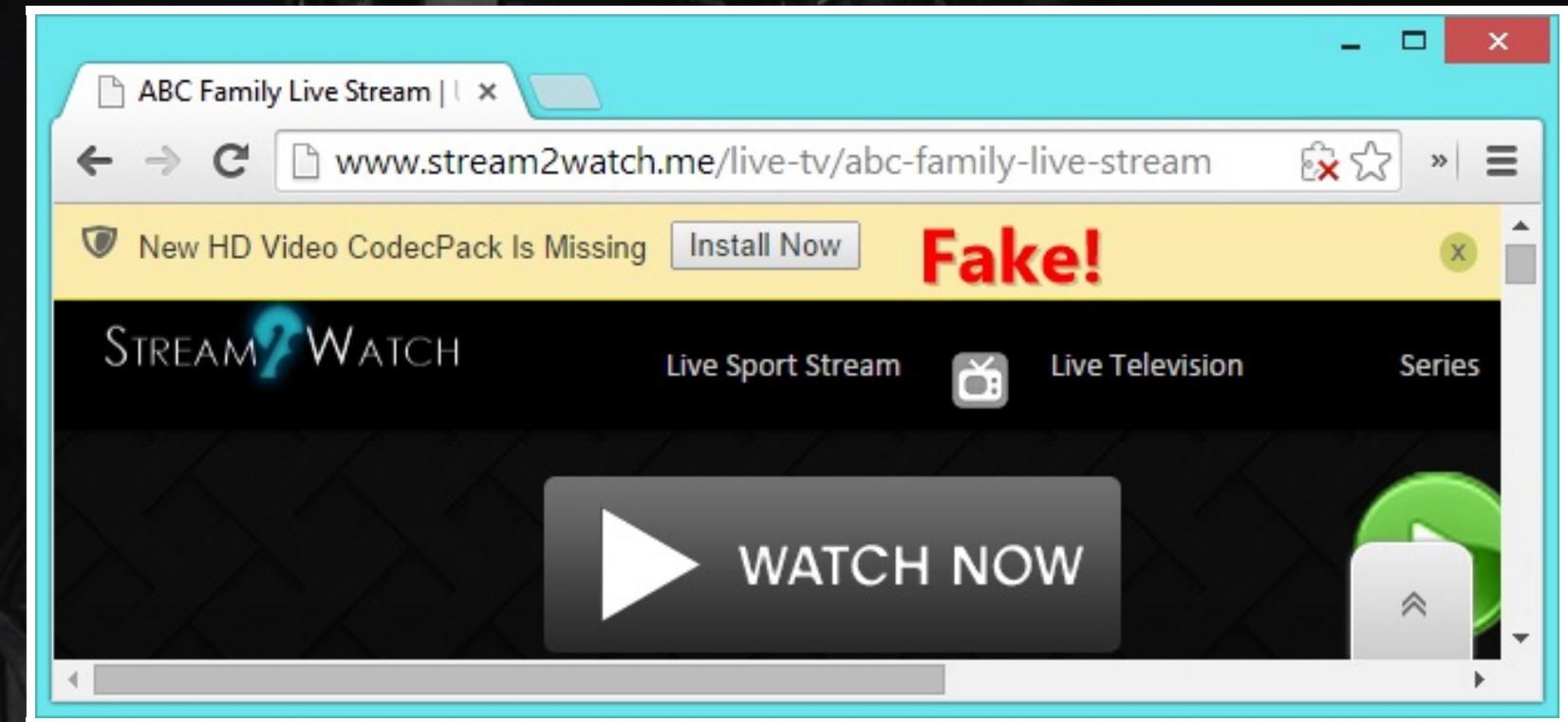
LES RÉSEAUX SOCIAUX

Recoupez les informations:

- "Votre compte XXX a été bloqué pour la raison YYY, cliquer ici pour déverrouiller"
 - Allez manuellement sur le site en question et vérifiez par vous même.

TÉLÉCHARGEMENTS

N'acceptez jamais l'installation d'un plugin, pilote ou codec quand un site vous le demande





PFFF, FACILE
JE CONNAIS DÉJÀ TOUT ÇA!



CE N'ÉTAIT QUE LA MISE EN BOUCHE

Prochaine étape: Techniques avancées



DES QUESTIONS?