

TECHNIQUES DE PHISHING AVANCÉES

ET COMMENT S'EN PROTÉGER

Morgan Hotonnier

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

TECHNIQUES AVANCÉES

- Email Hijacking
- Typosquatting
- Homographes
- Technique "RTL"
- Redirections et raccourcis
- Extensions de fichier
- Pièces jointes dangereuses
- Https = sécurisé?
- La ligne maginot
- Tabnapping

EMAIL HIJACKING

Si un ami/collègue se fait pirater

WOW [Inbox](#) | x

Devon [show details](#) Sep 20 [Reply](#) [Forward](#)

<http://rapidshare.com/files/282512175/install.exe>

Probably a Virus

Evan Wondrasek to Devon [show details](#) Sep 20 [Reply](#)

Hi Devon,

I wanted to verify that you intended to send this email, as it looks like a potential virus. If you did not intend to send this email, I recommend sending out a notification email to its recipients immediately.

Thanks,

Evan

L'attaquant n'a même plus besoin d'utiliser des techniques de spoofing

TYPOSQUATTING

Visitez [rnicrosoft.com](#) pour plus de détails

TYPOSQUATTING

Pardon, je voulais dire mircosoft.com

geon Ahrcvie Crgaieteos Pegas Tgas

Dsyxeila

A frined who has dxsiyela diebcsred to me how she eericnexeps rdnaeig. She can read, but it tkeas a lot of cntncreatiaon, and the lretets semes to “jmup anuord”.

I rmemrebeed rdnaieg aobut [tpmeilogyyca](#). Wdolun’t it be plsbisoe to do it iilnrattecvey on a wbetise wtih Jsaavpicrt? Sure it wuold.

Feel lkie manikg a baomklkroet of tihs or snmthoieg? [Fork it](#) on ghitub.

Dlsiyexa is cerhacriatzed by dtflucifly with lenraing to read fuleltny and wtih aartccue cepmooserhinn dtipese nmarol iticlnneenlg. This idlnceus diffuculty wtih pnligooaochl aeswanres, pnoghoicolal deodicng, pncooisrsg speed, ooragjhrpthc cnodig, aoitudry short-trem meromy, lganuage slikls/vberal choiromnesepn, and/or riapd nanimg.

Deeetoalvnpml rdnieag didors (DRD) is the msot cmomon linnraeg dtiibliasy. Dxsilyea is the msot rnzeeigod of rniedag drresiods, hwveer not all rniedag driesdors are likned to deilysa.

Smoe see deixysa as dctsnt from rinedag dciiutffelis rultnseig from other cuass, scuh as a non-nolocrigual decinfeicy with vsioin or hirnaeg, or poor or iateqnuade rdneiag ioiutcntsrm. There are terhe psoorepd covtiigne suepbyts of dliesyxa (aturdioy, visaul and anetttoianl), aohltugh iudnvdaill ceass of dxselyia are bteter enilpxaed by siifpcec udlirennyg nocirongaelsoabucl detfics and co-ocruicna lnnraeg dilasietlhs (e.g. attatnien-

Psbluhied

03 Mcarb 2106

Tgas

dyixelsa 1

tyegplmoiyca 1

Jcraspavit 1



TYPOSQUATTING

*Décidemment! je voulais bien sûr taper
micrpsoft.com*



HOMOGRAPHES

Wikipedia != Wikipedia

HOMOGRAPHES

Regardons ça de plus prêt

- ee
- aa

COMMENT JE REPÈRE ÇA À L'OEIL NU MOI?!

- Heureusement, les navigateurs sont là pour nous aider
 - Les liens sont toujours affiché en punycode
 - Cela signifie qu'un lien comme celui-ci :
<http://www.paypal.com>
 - Sera affiché de cette manière: <http://www.xn--pypal-4ve.com/>

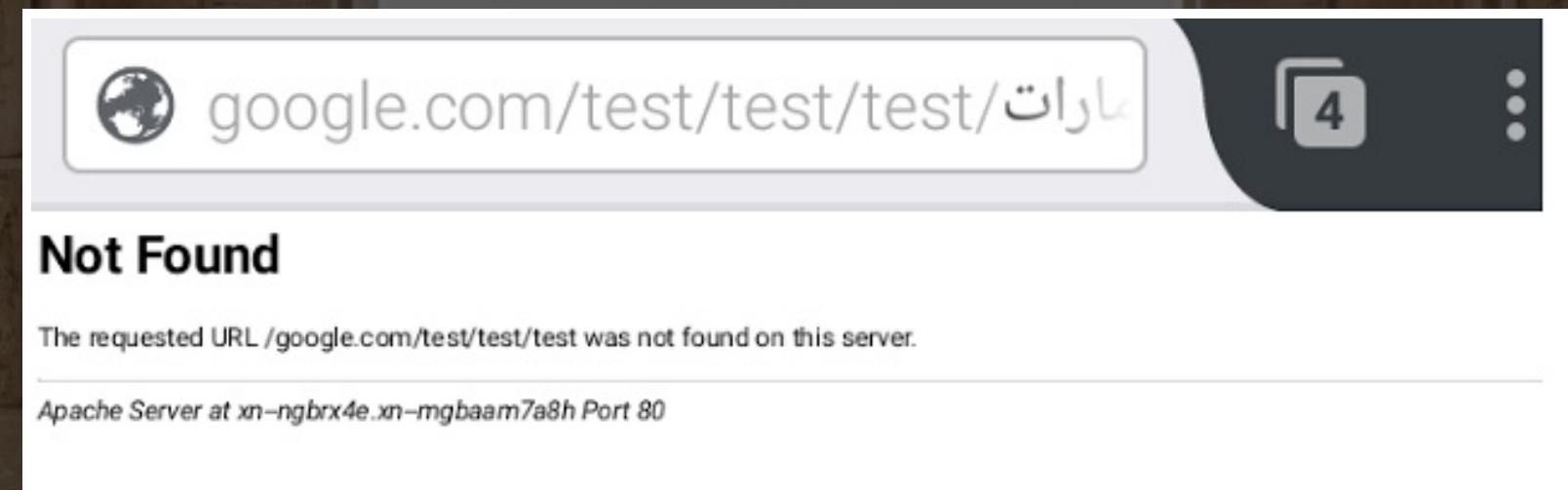


TECHNIQUE RTL

*et iord à ehcuag ed suot sap snosil en suon
euq ecraP*

TECHNIQUE RTL

Le lien <http://عربية.امارات/google.com/test/test/test> était affiché de cette façon



C'est patché...pour l'instant.



REDIRECTIONS

The background image shows a paved road curving through a desert environment with large, layered rock formations. A yellow diamond-shaped road sign with a black winding arrow symbol is positioned on the right side of the road, indicating a sharp turn ahead. Below it is a smaller rectangular sign with the number "15 MPH".

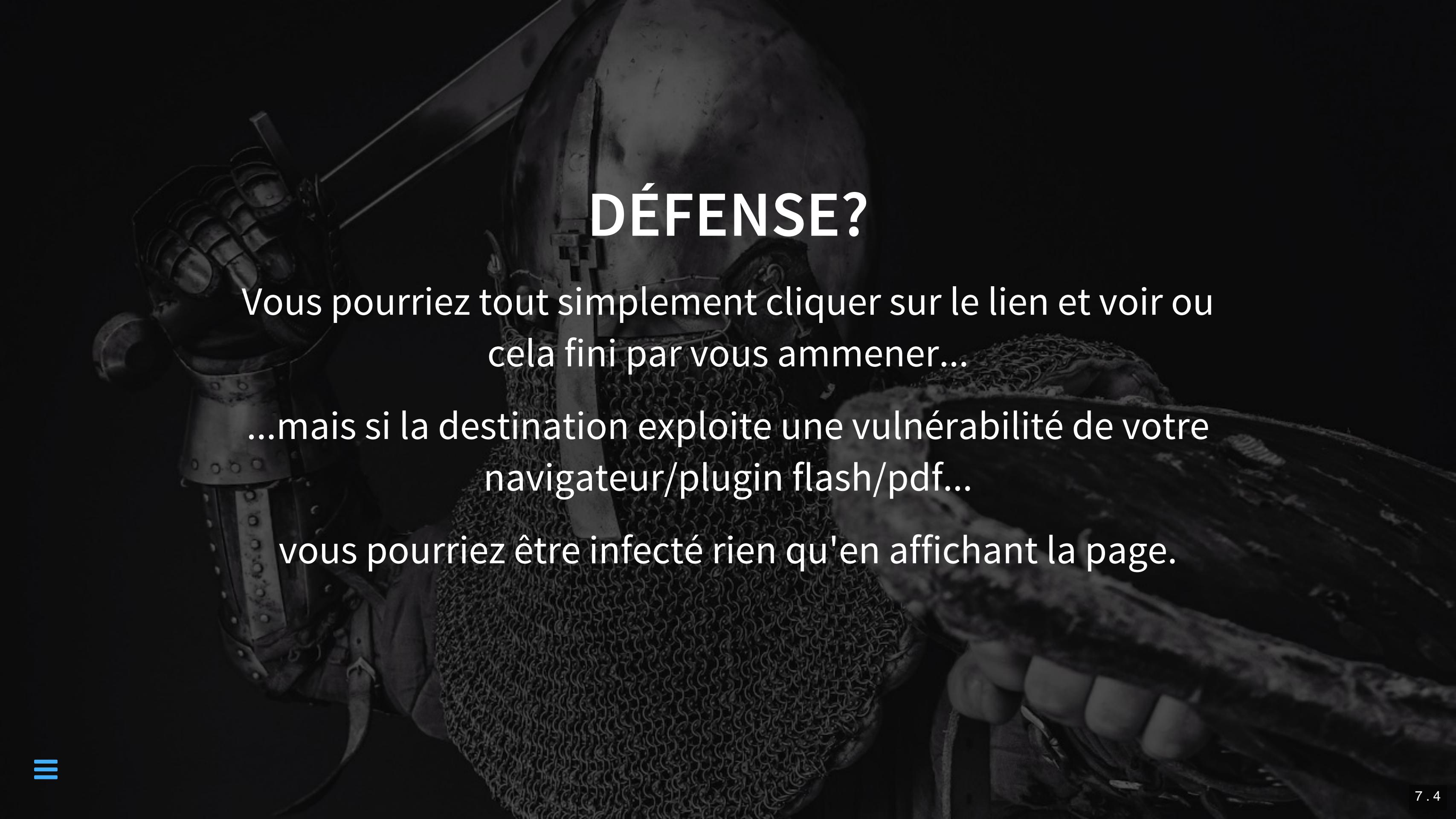
MINI-LIENS

Parce que <http://tiny.cc/recover-gmail-password> inspire confiance, n'est ce pas?

REDIRECTIONS OUVERTES

Que dites vous de ce lien là?

[http://www.ebay.com/longue/url/legitime/redirection.php?
url=http://malicious.example.com](http://www.ebay.com/longue/url/legitime/redirection.php?url=http://malicious.example.com)

A black and white photograph of a knight in full armor, including a helmet and gauntlets, holding a long sword. The armor is detailed with rivets and chainmail. The background is dark and moody.

DÉFENSE?

Vous pourriez tout simplement cliquer sur le lien et voir ou cela fini par vous ammener...

...mais si la destination exploite une vulnérabilité de votre navigateur/plugin flash/pdf...

vous pourriez être infecté rien qu'en affichant la page.

Il existe aussi des "expanders"
<http://www.linkexpander.com/>

Top Link Expander & Decrypter ! UnshortenUrls in no time !

Enter any url below and our link unshortener will uncover the original site it is pointing to

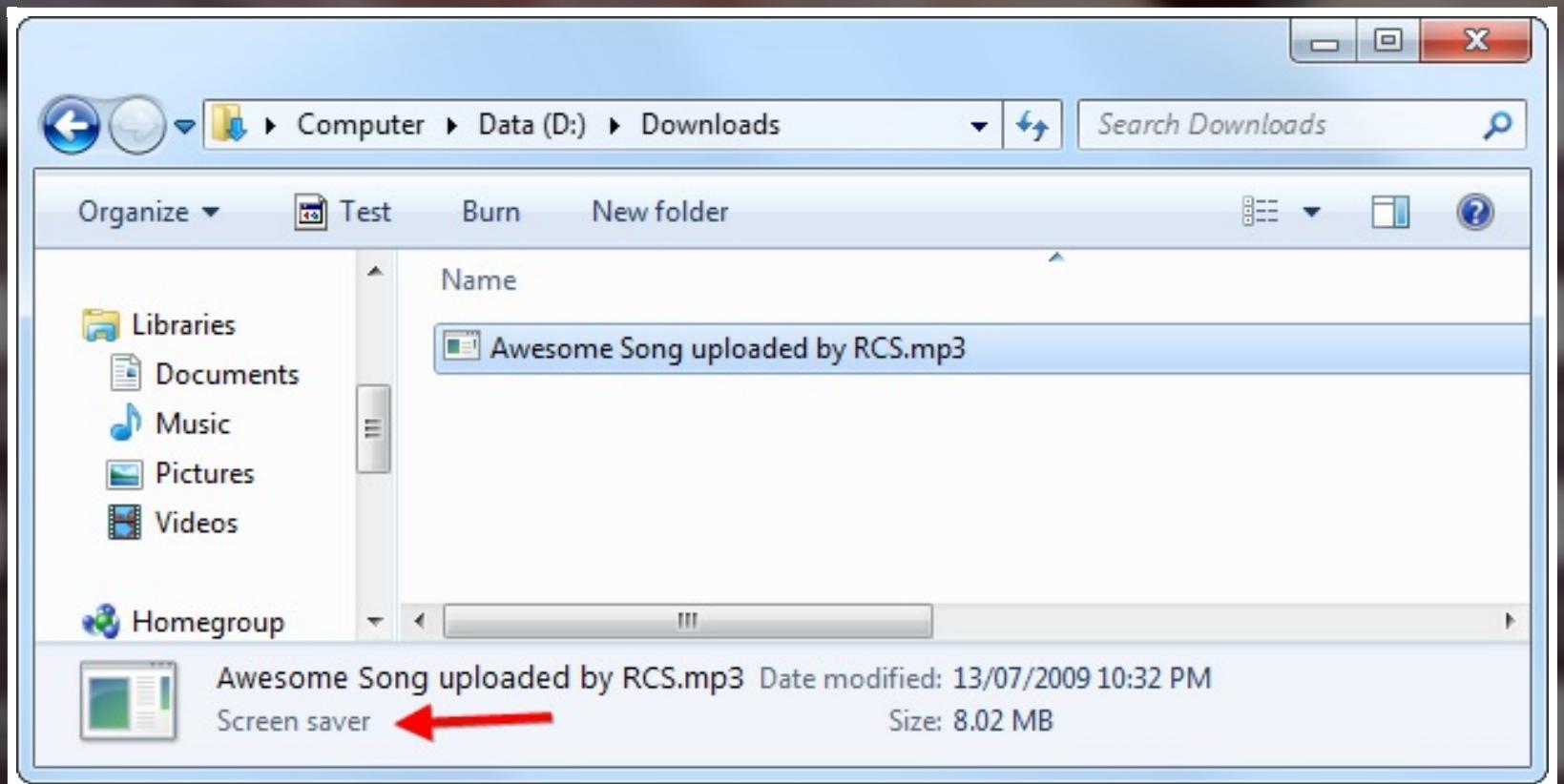
Expand

Uncovered URL is:
<https://www.youtube.com/watch?v=oHg5SJYRHA0>

Title	Description	Keywords	Trust Level	Screenshot
RickRoll'D - YouTube	http://www.facebook.com/rickroll548 As long as trolls are still trolling, the Rick will never stop rolling.	Cotter548, Shawn, Cotter, lol, gamefaqs, CE, reddit, rettocs, no, brb, afk, lawl, pwnt, Rickroll, Rickroll'd, Rick, Roll, Duckroll, Duck, rick, roll, astley,...	Grey	

EXTENSIONS DE FICHIER

Double-cliquer pour ouvrir photo-coquine.jpg.exe



A close-up photograph of a bright green snake with blue spots, coiled around a brown branch. The snake's body is vibrant green with distinct blue markings, and its scales are clearly visible. The background is dark, making the snake stand out.

PIECES JOINTES DANGEREUSES

PIECES JOINTES DANGEREUSES

Ce n'est pas un .exe, je peux donc l'ouvrir sans crainte?



PIECES JOINTES DANGEREUSES

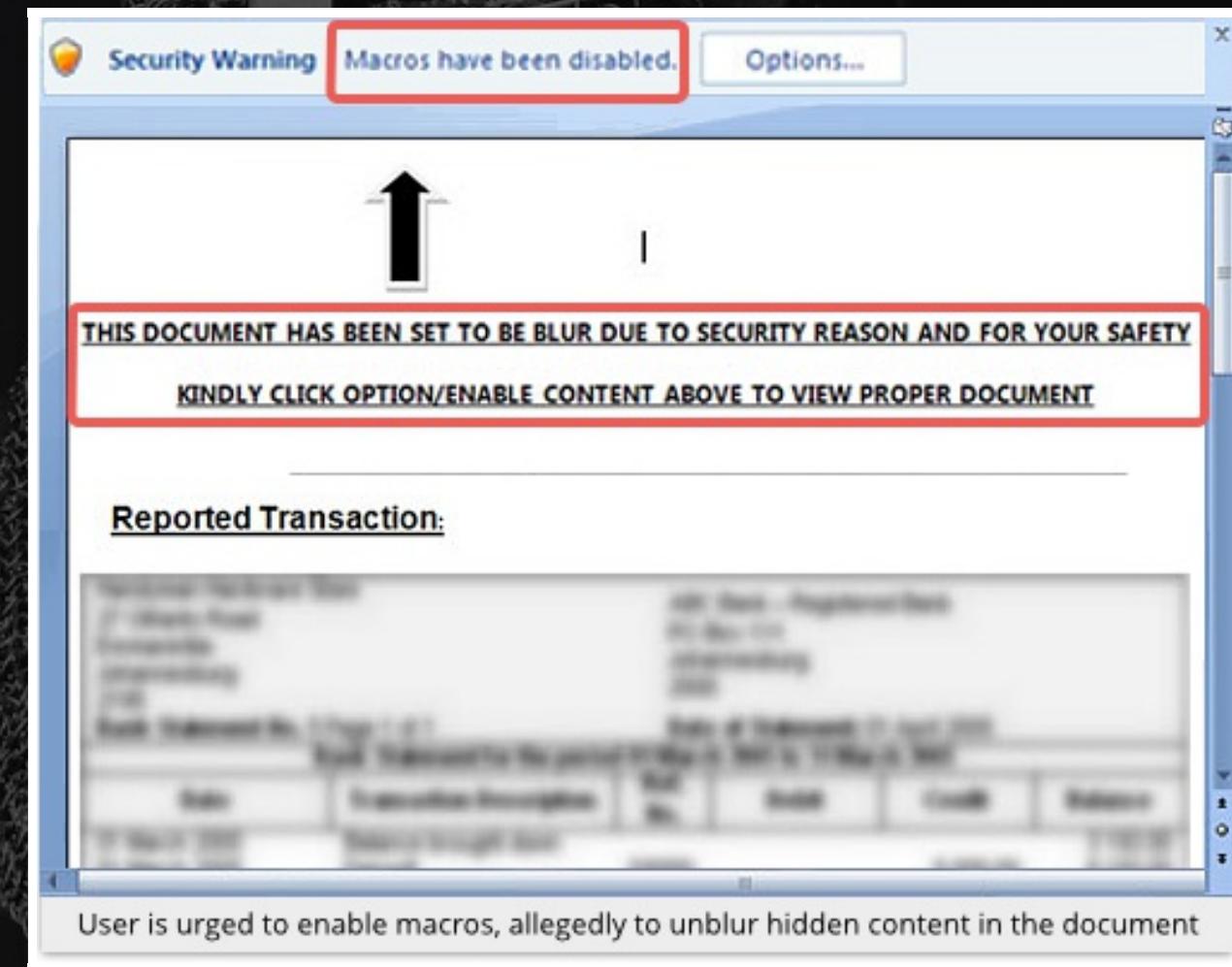
- C'est plus compliqué que ça
- Le nombre d'extensions dangereuses dépasse les 50
 - .pif, .msi, .com, .scr, .msc, .jar, .bat, .cmd, .vb, .js, .ps1, .msh, .lnk, .inf, .reg
 - Mais aussi .svg, .doc, .xls, .ppt...

DÉFENSE?

- Préférez le concept de liste blanche à celui de liste noire
 - N'ouvrez que ce que vous savez être sans risque (jpg, png, txt, pdf)
- Document à risque? N'ouvrez que si
 - Vous connaissez l'Expéditeur
 - Il vous a confirmé (par un autre canal) que le mail venait bien de lui

DÉFENSE?

- Documents offices? N'activez pas les macros
 - Peu importe ce que dit le document



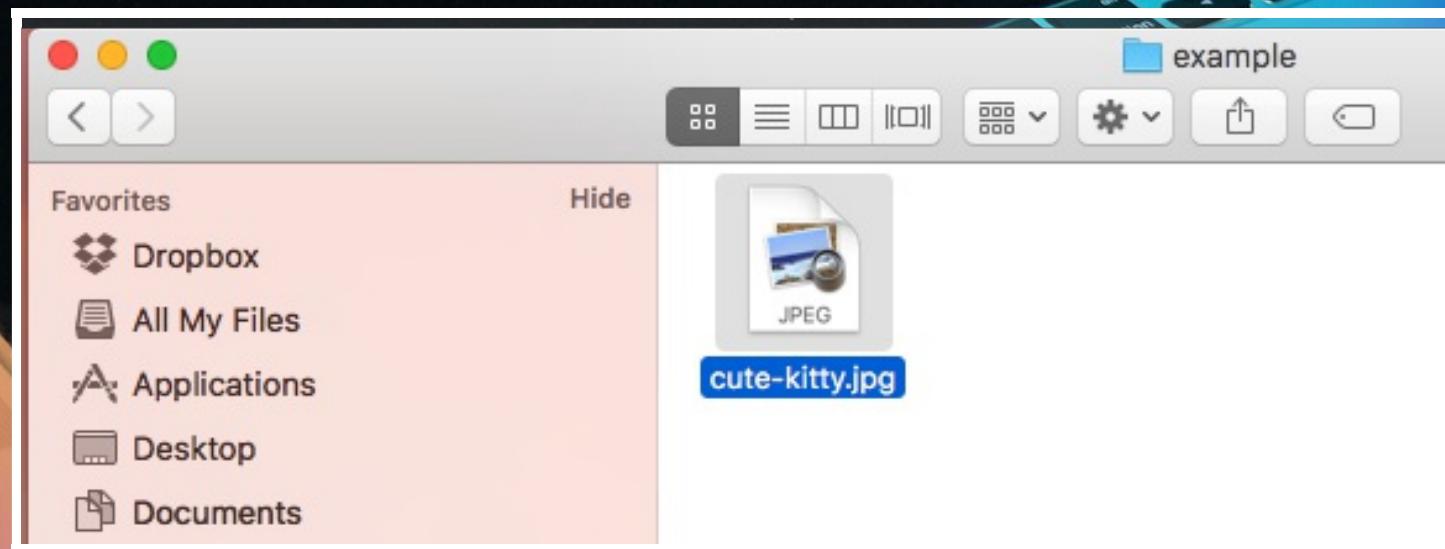


OUI MAIS SUR MAC, ON A PAS DE
VIRUS



Vous pouvez donc ouvrir sans crainte "cute-kitty.jpg"

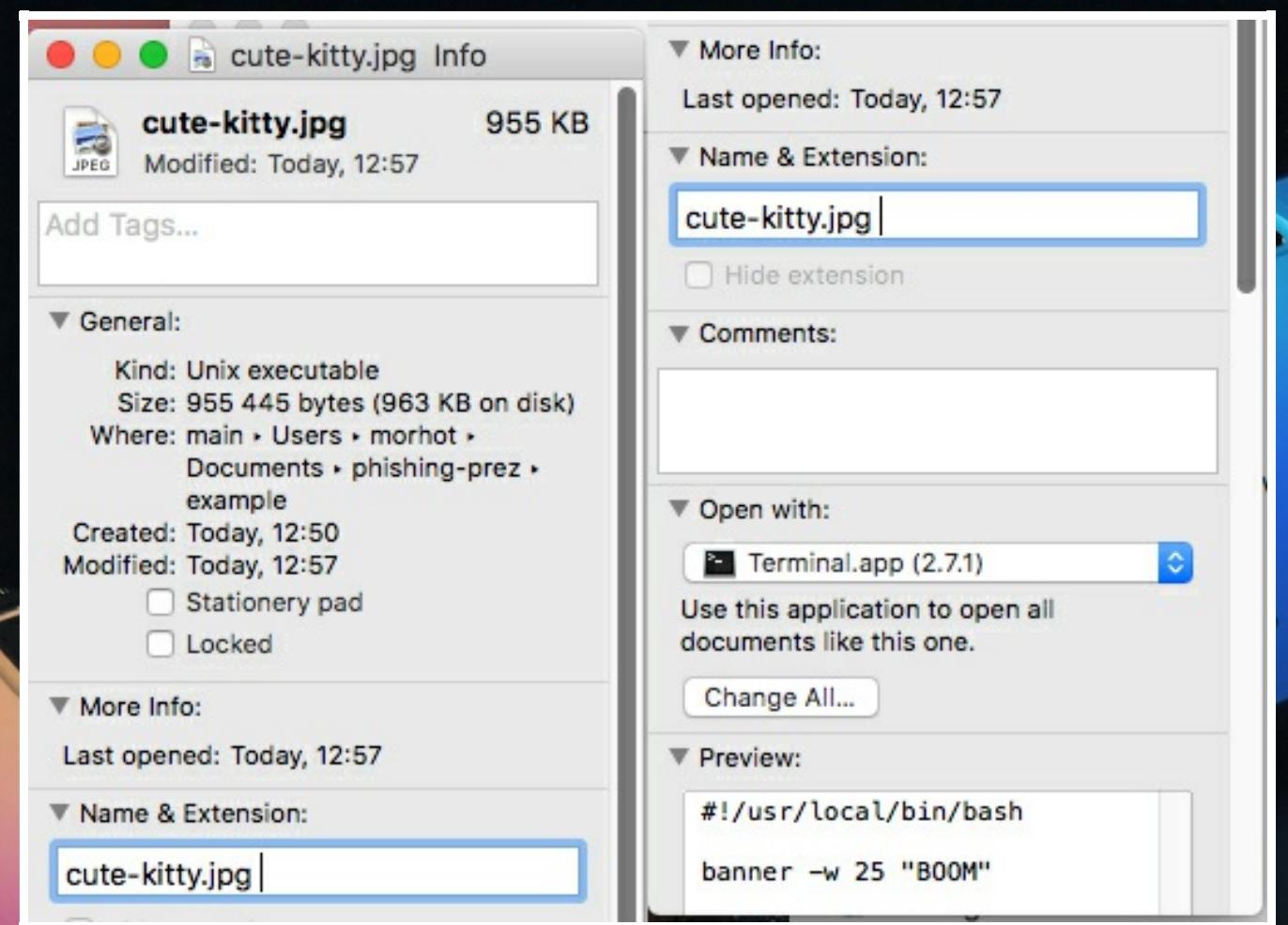
...n'est ce pas?



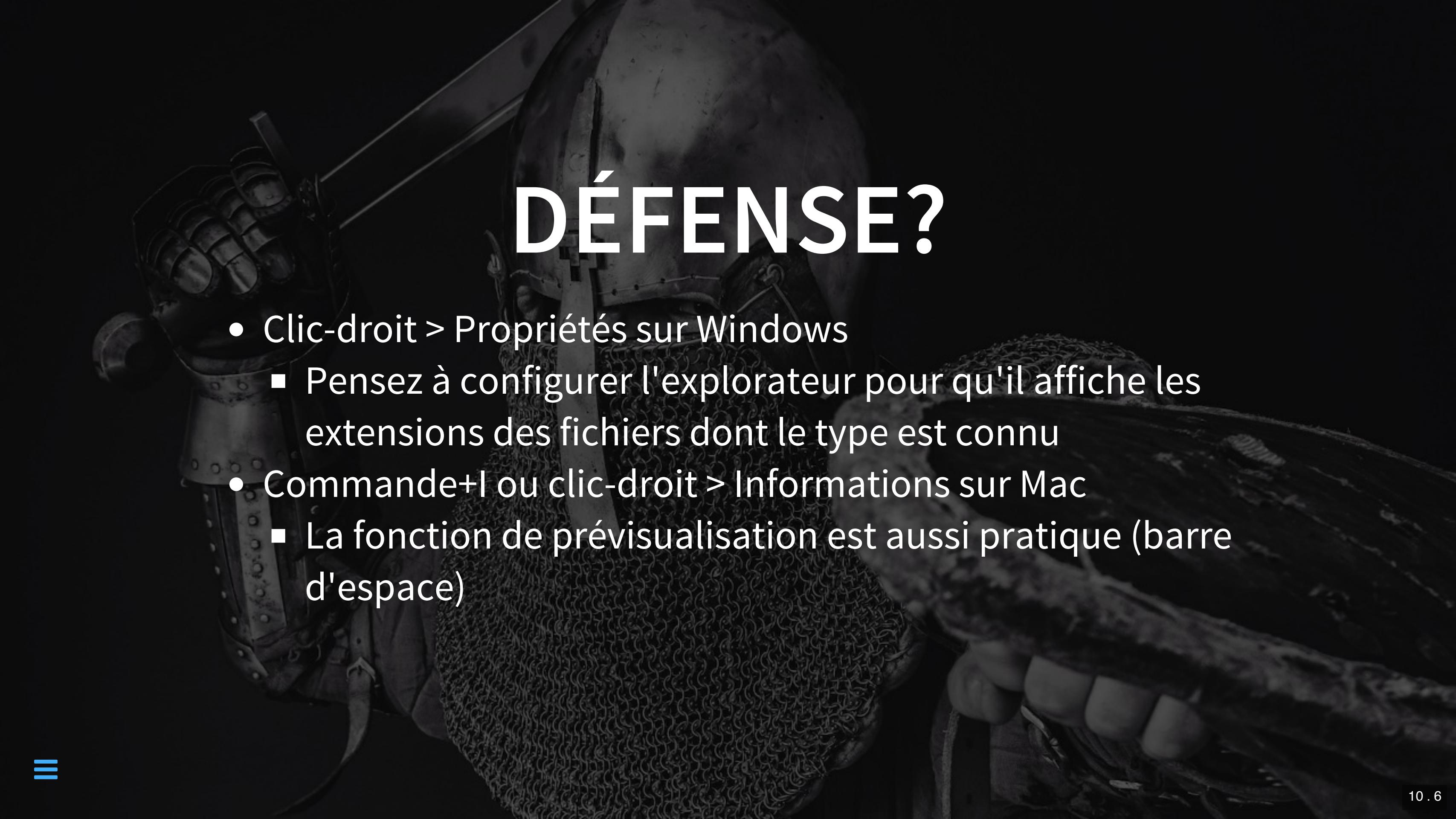
...oops

```
STHMACLT070:~ morhot$ /Users/morhot/Documents/phishing-prez/cute-kitty.jpg` ; e  
xit;  
#  
#####  
#####  
#  
#  
#      ##      #  
#      #####    ##  
#####      #####  
###  
#####  
#####  
####      ####  
#          #  
#  
#          #  
##          ##  
#####  
#####  
#####  
####      ####  
#          #  
#  
#          #  
##          ##  
#####  
#####  
#          #####  
#####  
#####  
#  
#####  
#          #####  
#####  
#####  
#          #####  
#####  
#####  
#
```

".jpg<espace>", pas ".jpg"



Extension inconnue? Marqué comme exécutable ? Ouvrons le donc avec un terminal!



DÉFENSE?

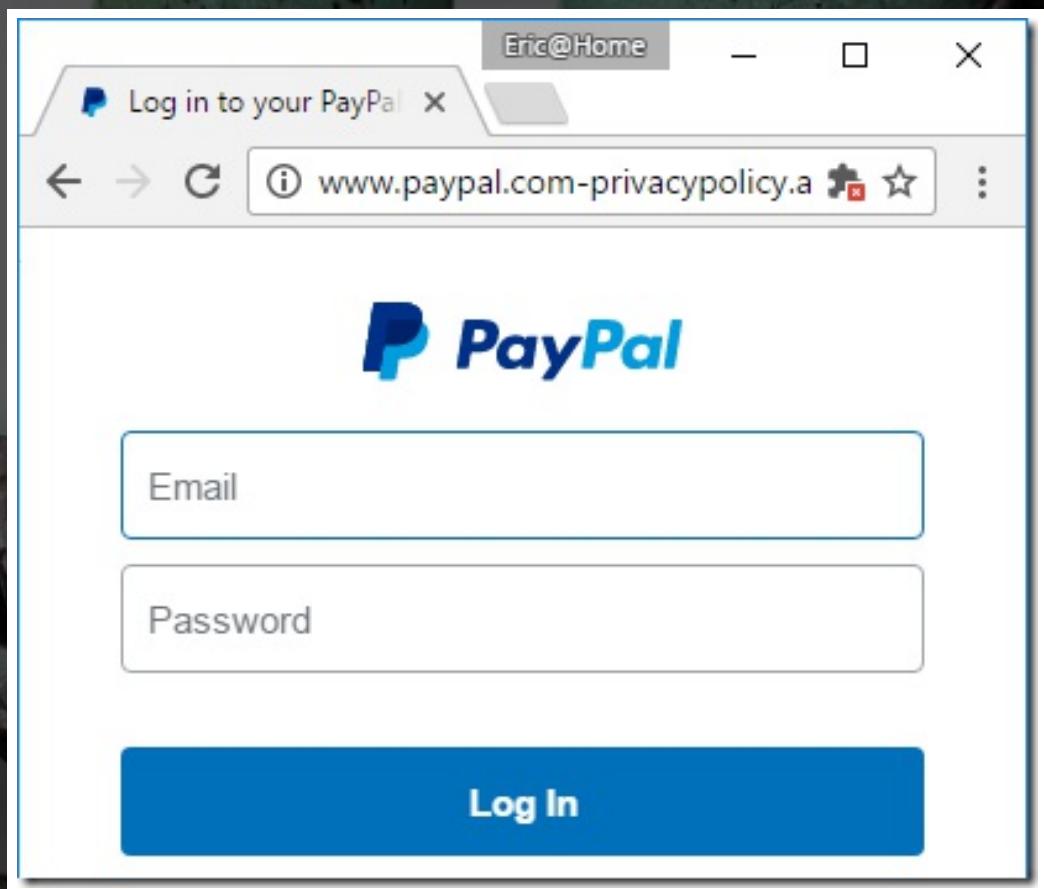
- Clic-droit > Propriétés sur Windows
 - Pensez à configurer l'explorateur pour qu'il affiche les extensions des fichiers dont le type est connu
- Commande+I ou clic-droit > Informations sur Mac
 - La fonction de prévisualisation est aussi pratique (barre d'espace)

LE "CADENAS VERT"

Il y a le petit cadenas, je suis sur un site de confiance

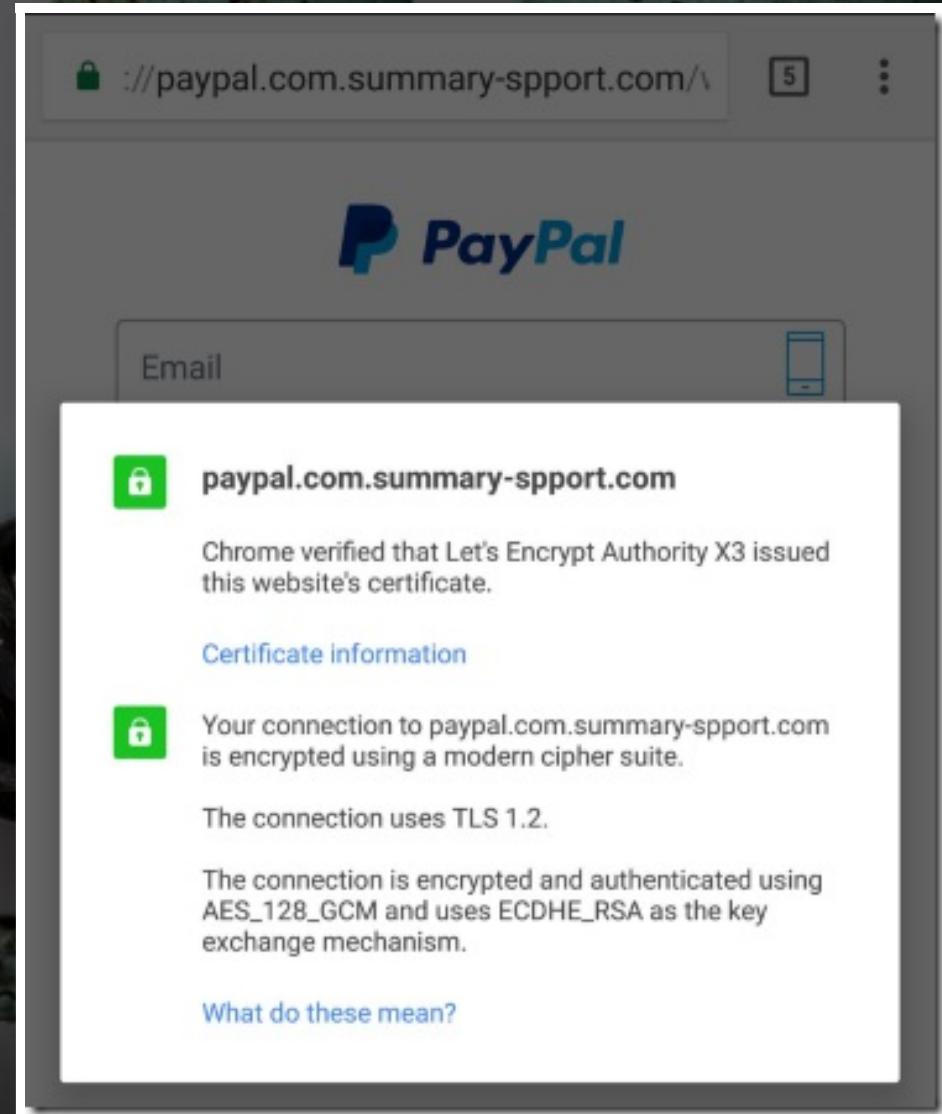
LE CADENAS VERT

Que pensez vous de ce site?



LE CADENAS VERT

...oups

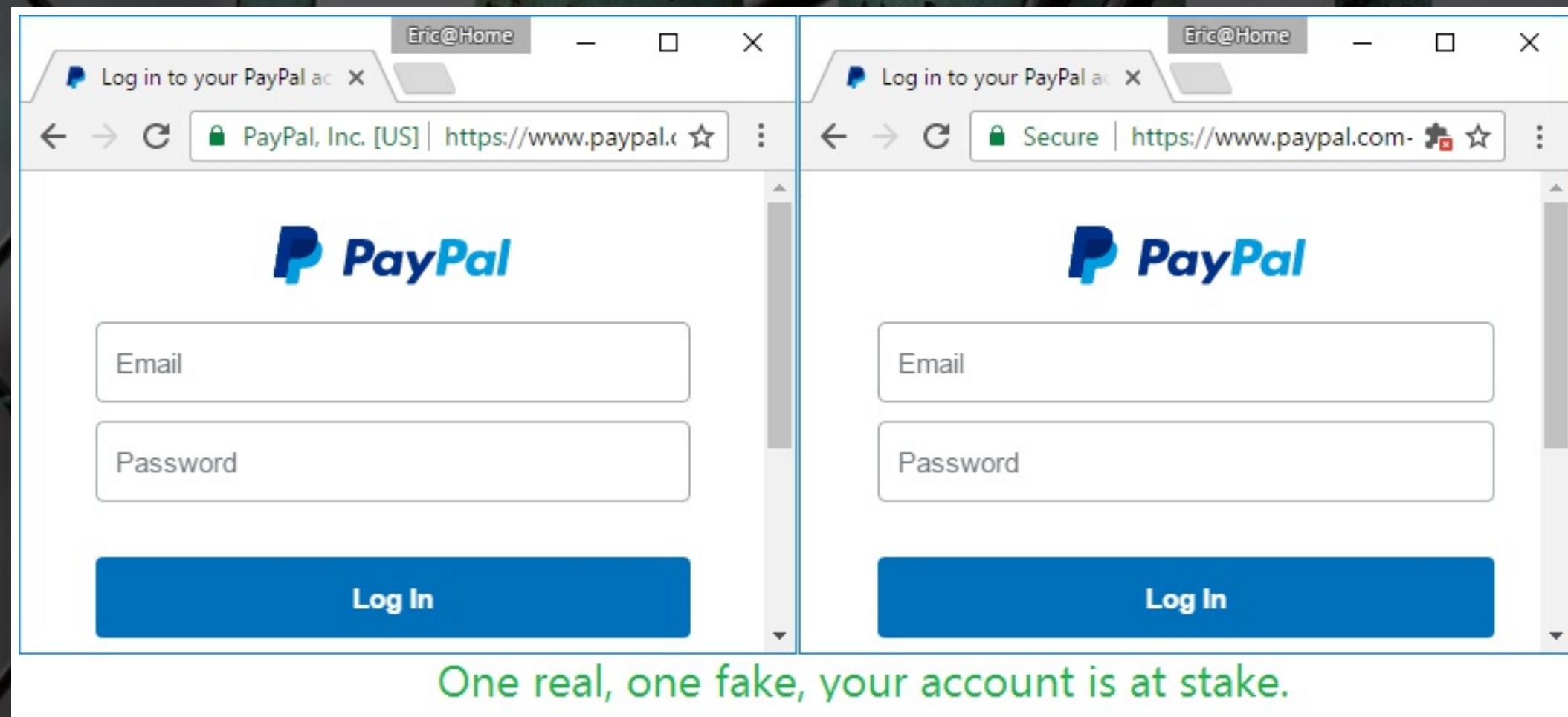


CE QUE SIGNIFIE HTTPS

- Le cadenas dans la barre ne signifie qu'une chose
 - La connexion entre votre ordinateur et le site est chiffrée
 - et le certificat utilisée est reconnue par une autorité de certification...
 - ...comme appartenant à ce nom de domaine
- C'est tout.

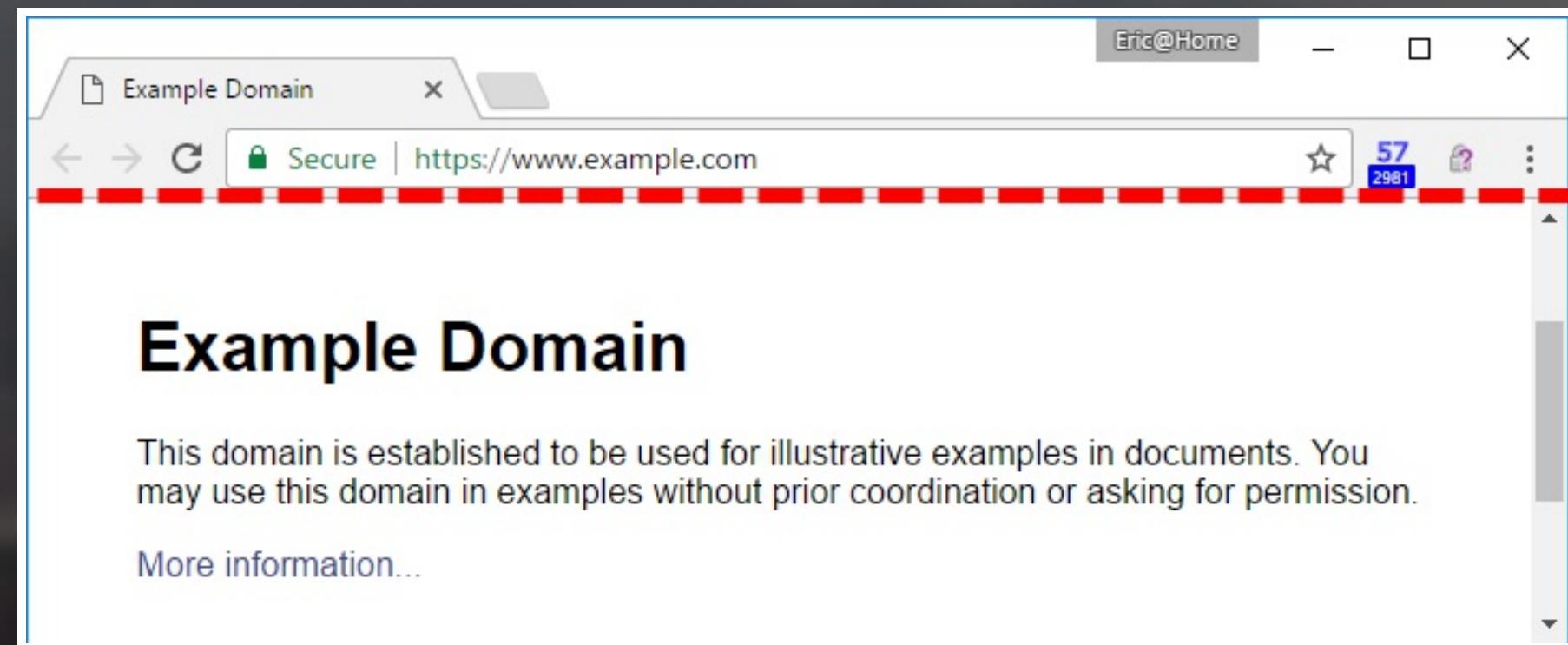
HTTPS EST PARTOUT

- Avant, avoir un certificat valide était long et couteux
 - Maintenant, c'est gratuit et ça prend 5 minutes
 - Les faux sites passent en HTTPS pour inspirer confiance



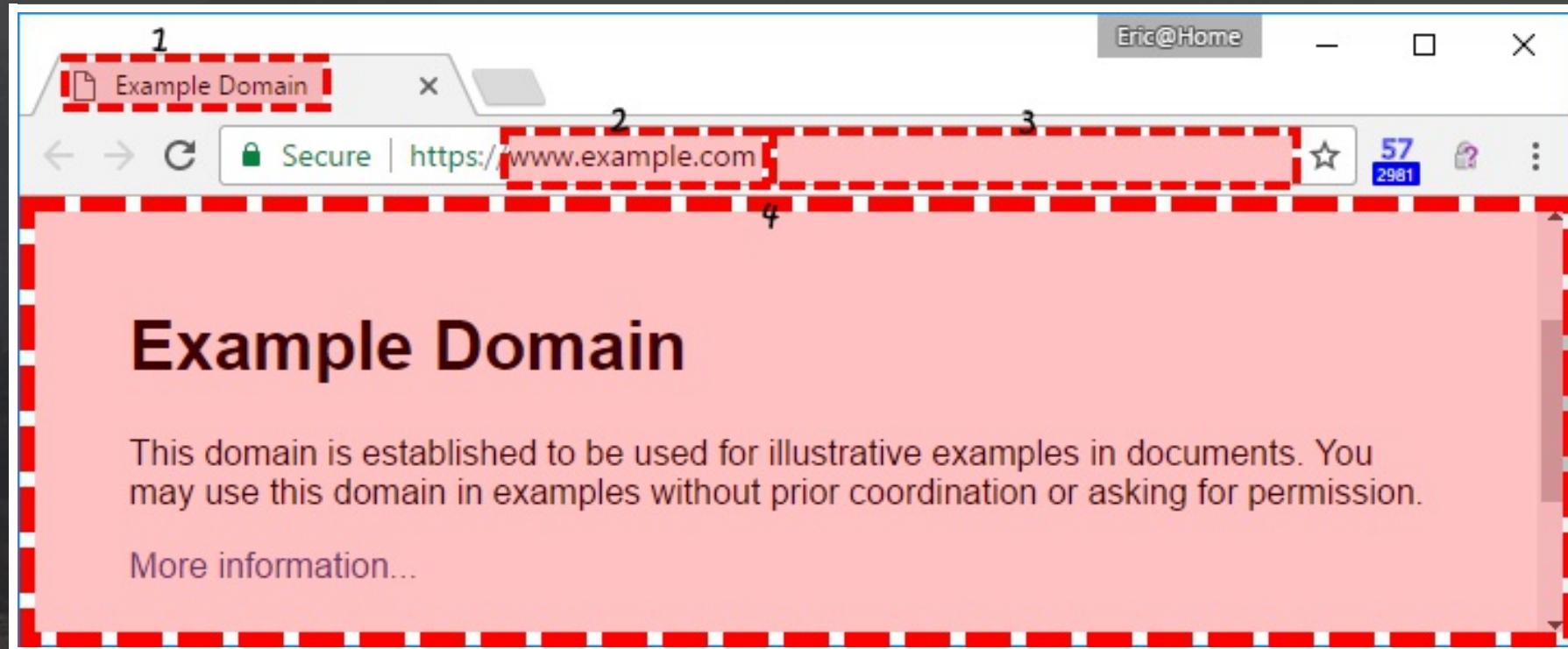
LA ZONE DE CONFIANCE

Passez cette ligne, rien n'est fiable

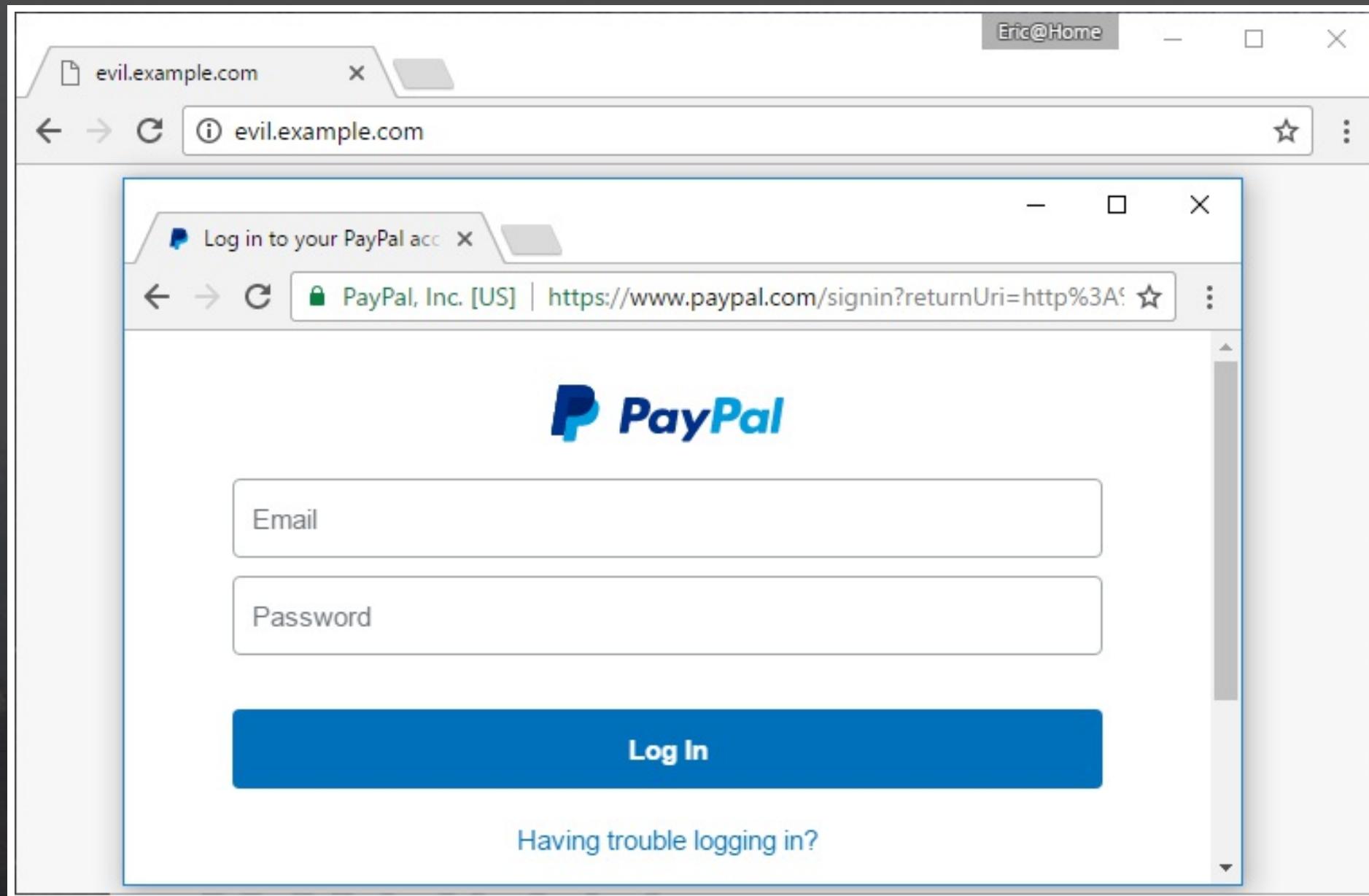


LA ZONE DE CONFIANCE

Et même au dessus de cette ligne, tout est relatif...



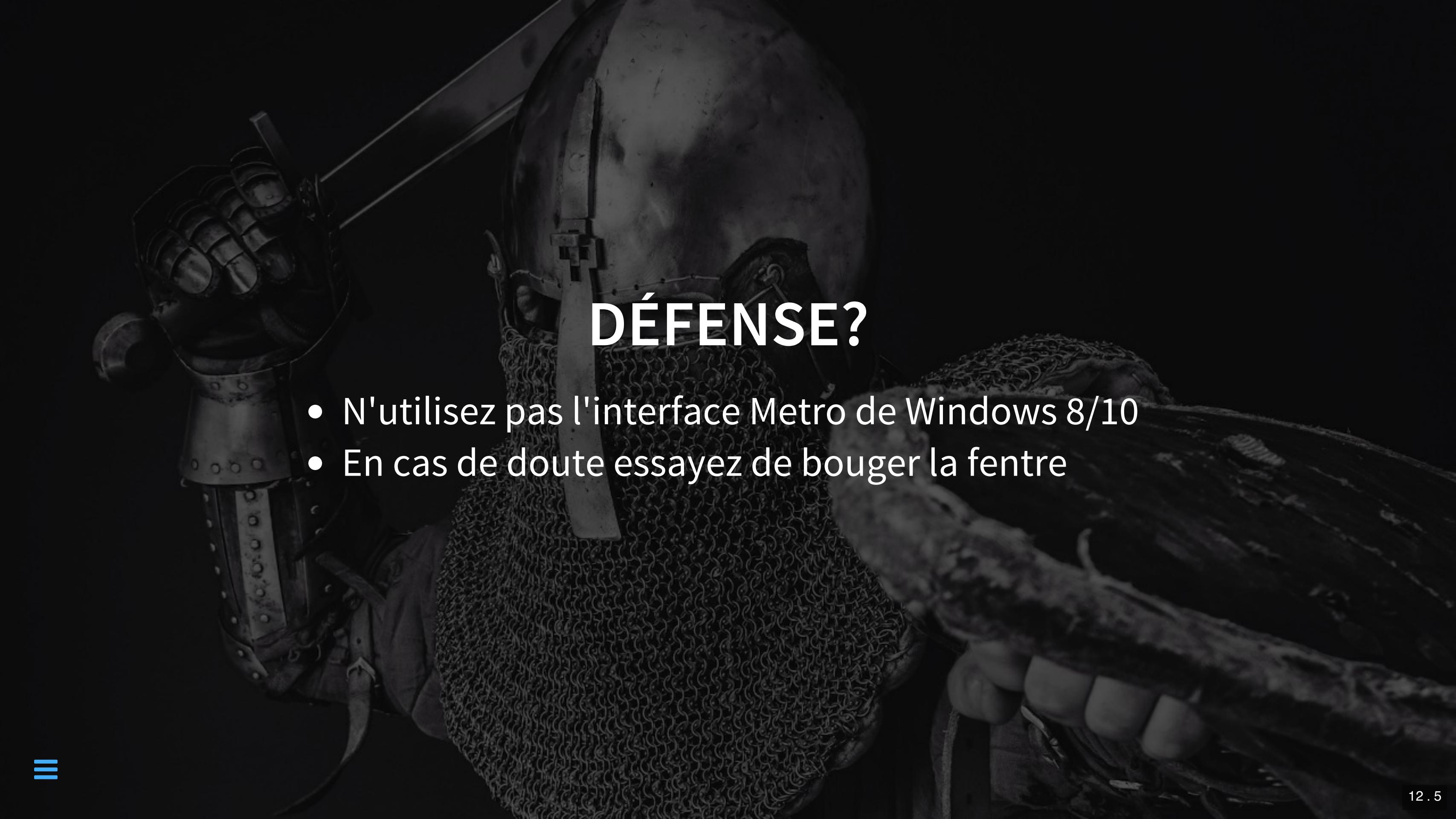
Que pensez vous de ce site?



METRO/MODERNUI

...C'est pire...



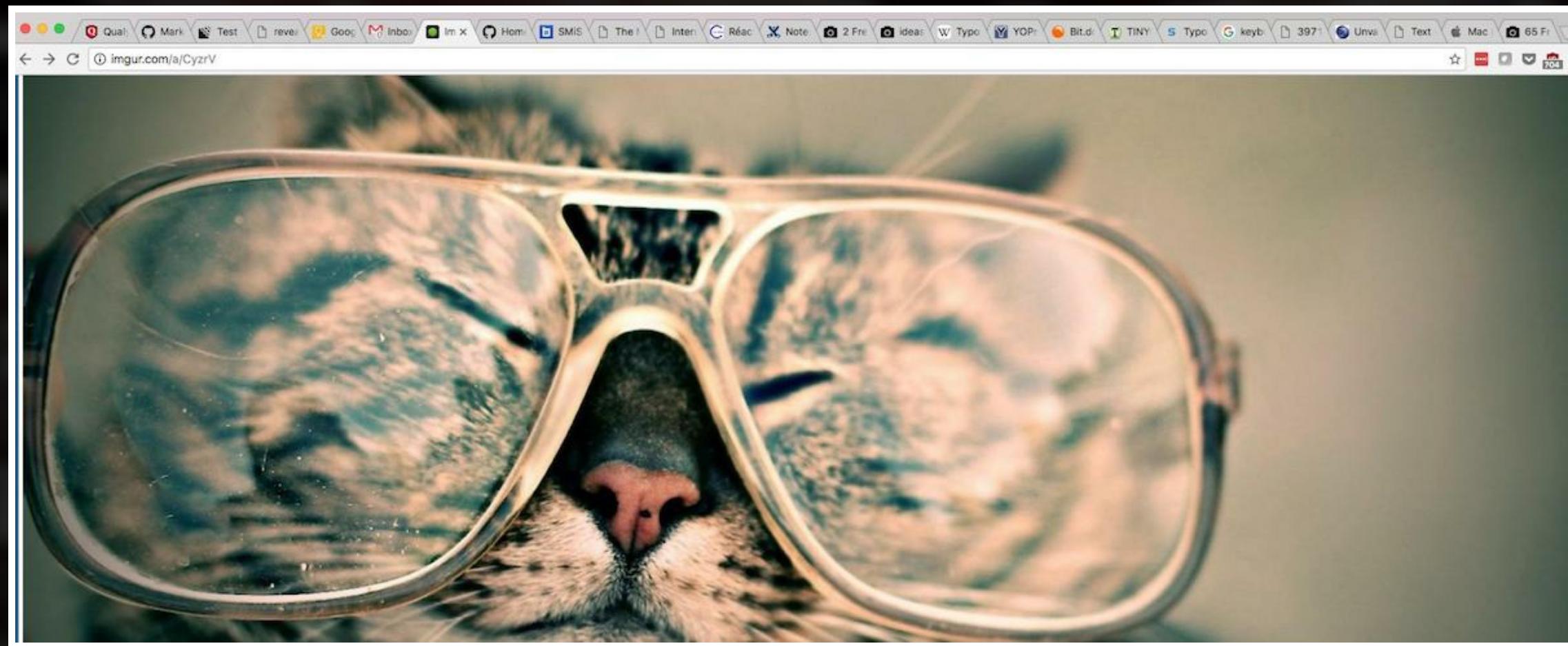
A black and white photograph of a knight in full armor, including a helmet, gauntlets, and chainmail. He is holding a long-sword in his right hand. The background is dark and moody.

DÉFENSE?

- N'utilisez pas l'interface Metro de Windows 8/10
- En cas de doute essayez de bouger la fentre

TABNAPPING

Si votre navigateur ressemble souvent au mien, vous êtes dans le pétrin



DÉMONSTRATION!

Vidéo backup:

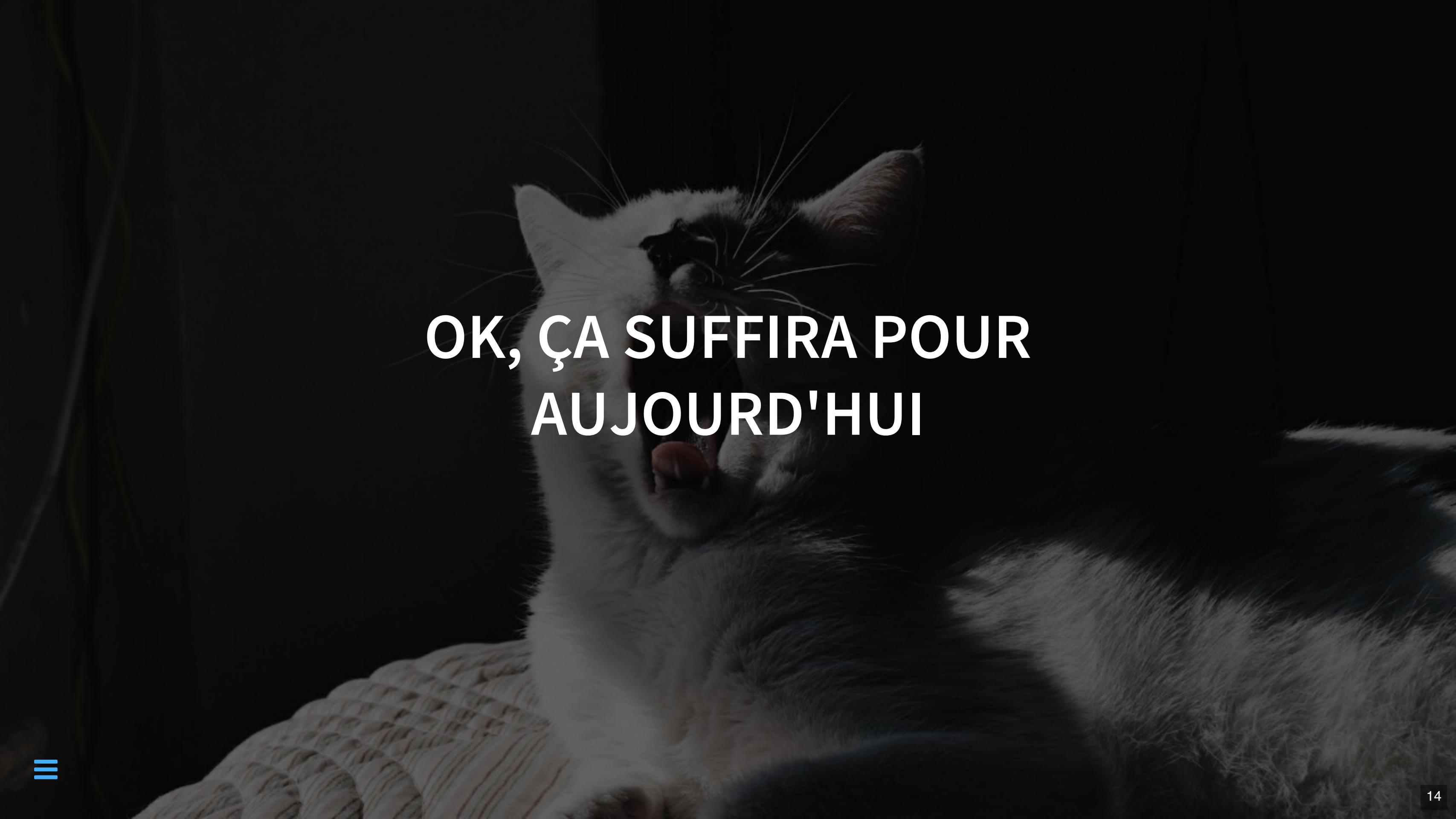
<https://www.youtube.com/embed/97kduHI2OGk>



DÉMO VIDÉO

COMMENT SE DÉFENDRE DE CETTE SORCELLERIE!

- Toujours vérifier la barre d'adresse avant de remplir des données sensibles
 - Pas besoin de cliquer sur entrée, taper dans la fenêtre, c'est déjà trop
- Les gestionnaires de mot de passe aident beaucoup
 - Ils ne feront pas l'autocomplétion vu que ce n'est pas le bon site



OK, ÇA SUFFIRA POUR
AUJOURD'HUI



DES QUESTIONS?