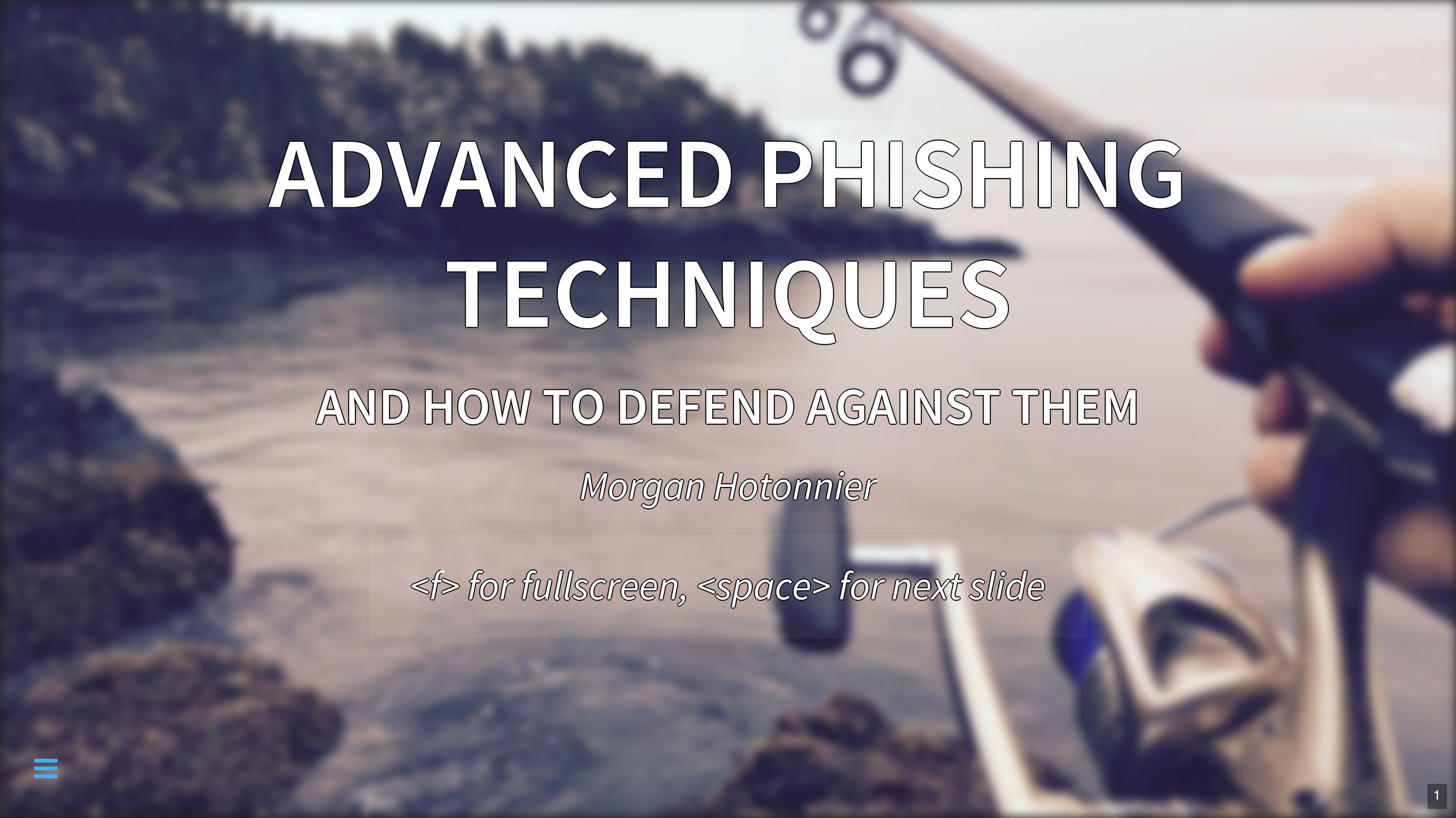


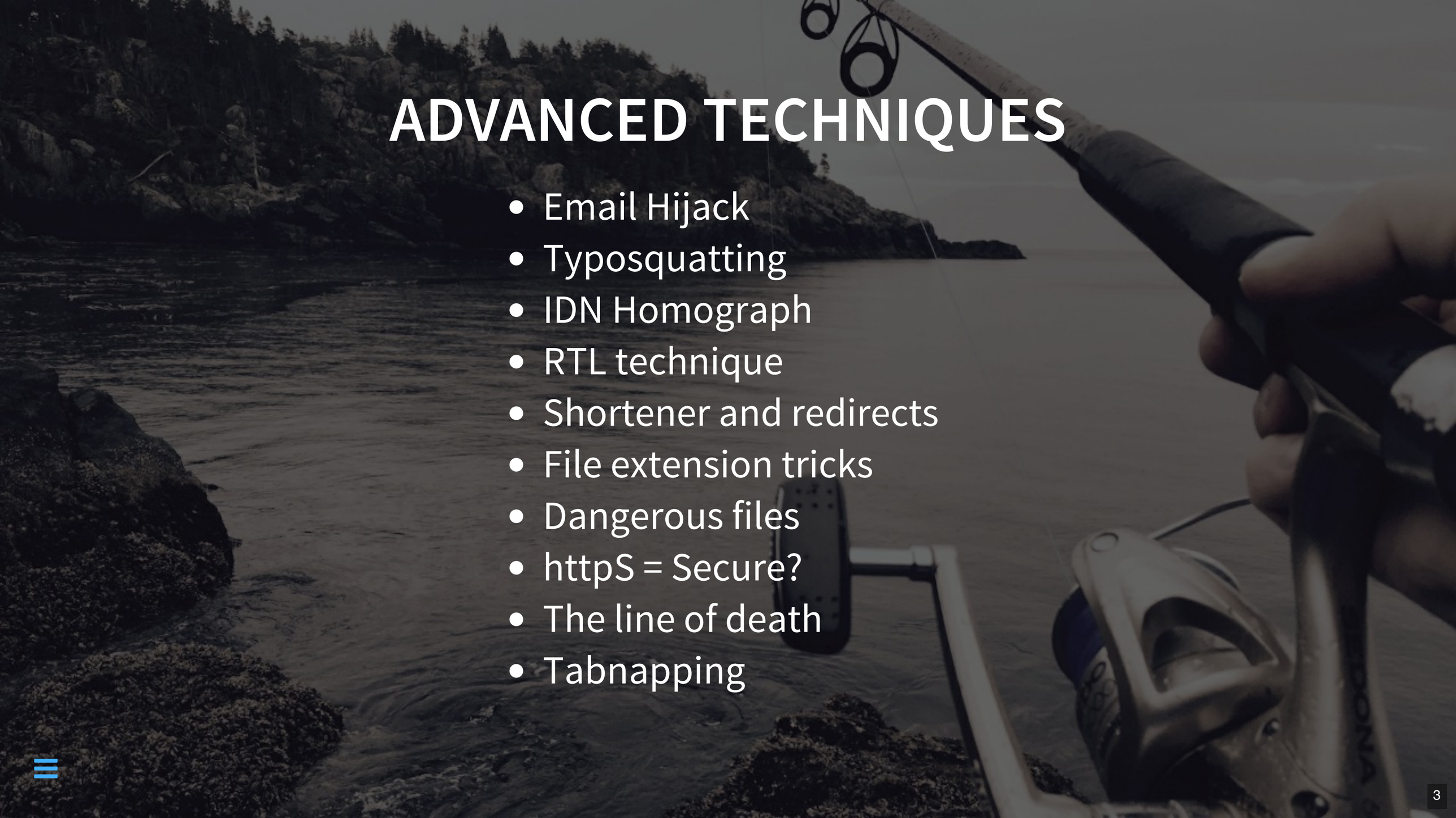
ADVANCED PHISHING TECHNIQUES

AND HOW TO DEFEND AGAINST THEM

Morgan Hotonnier

<f> for fullscreen, <space> for next slide


PREVIOUS TRAINING WAS TOO EASY!

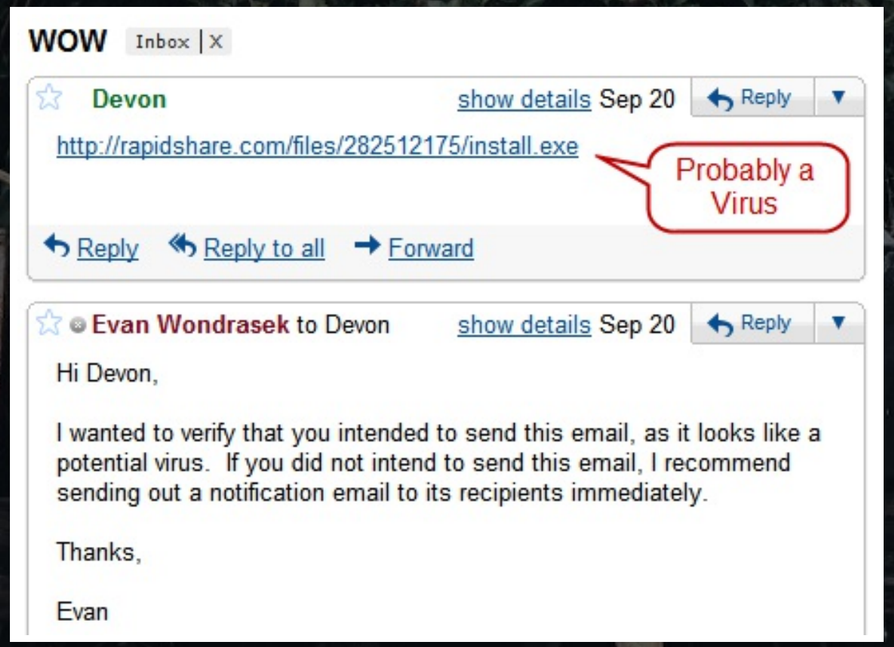


ADVANCED TECHNIQUES

- Email Hijack
- Typosquatting
- IDN Homograph
- RTL technique
- Shortener and redirects
- File extension tricks
- Dangerous files
- httpS = Secure?
- The line of death
- Tabnapping

EMAIL HIJACK

If your friend got hacked



attacker doesn't even need to spoof anything


TYPOSQUATTING
Please visit rnicrosoft.com for more details

TYPOSQUATTING

Sorry, I meant mircosoft.com

goen Ahivcre Catogriees Pegas Tgas

Dyxeslia

A fenird who has dlesixya dcibsreed to me how she ecnieeexprs rdeinag. She *can* raed, but it tkeas a lot of cotoearntncin, and the Itertes smees to “jump aunrod”.

I rmermebeed radieng aoubt tcyolmgiyepa. Wludon’t it be plosbise to do it inetvreiatcly on a witsbee wtih Jpciaarsvt? Sure it wloud.

Feel Ikie mnakig a borlameokkt of tihs or sthminoeg? Fork it on gtiuhb.

> Dsieyxla is carreaiectzhd by dlufticfiy wtih lnnreaig to raed fltulney and wtih acutacre cpohmeosrenin deistpe nomarl icgelnlneite. Tihs icdelnus dcftfiiuly wtih phoicnlagool aesnaewrs, pocnogloiahl dnciedog, pcsnosrieg seepd, otrhgpohiarc cdiong, audiorty shrot-trem moemry, lgnugaae sikIls/vaebrl chieresnpoomn, and/or ripad nnimag.

> Datvmpneloeel rdinaeg desiodrr (DRD) is the msot coommn lairenng distiilbay. Diseylxa is the msot riozncgeed of rnadieg dsoiedrrs, heoevwr not all rdiaeng dderosirs are lkenid to dsyleixa.

> Some see delisyxa as dcsinitt from rnedaig diuifclteifs rinusletg form oethr caeuss, scuh as a non-noraciouegll dccnieiefy with visoin or heiarng, or poor or iqatndaeue reidang icuttnisorn. Three are tehre poporsed ciitnovge sypbutes of dseyixla (aitduory, visual and atoentaintl), atouhlgh iauiidndvl caess of dxyeslia are betetr eeanxplid by sifiecpc umeldnyig

Piueshbld
03 Mrach 2016
Tags

dixslyea [1]

tmoyyclgpiea [1]

Jrapsavcit [1]

TYPOSQUATTING

Damn! I meant micrpsoft.com

HOMOGRAPHS

Wikipedia != Wikipedia

HOMOGRAPHS

Let's put them next to one another

- ee
- aa

HOW CAN I SERIOUSLY SPOT THAT?!

- Thanksfully browsers got your back
  - Link are displayed in **punycode**
  - This makes a text like this : http://www.paypal.com
  - Look like this: http://www.xn--pypal-4ve.com/

URL BAR RTL ATTACK

erehwyreve thgir ot tfel morf daer t'nod ew esuaceB

RTL TECHNIQUES

The link http://عربي.امارات/google.com/test/test/test was displayed like this

It's patched...for now.

REDIRECTIONS

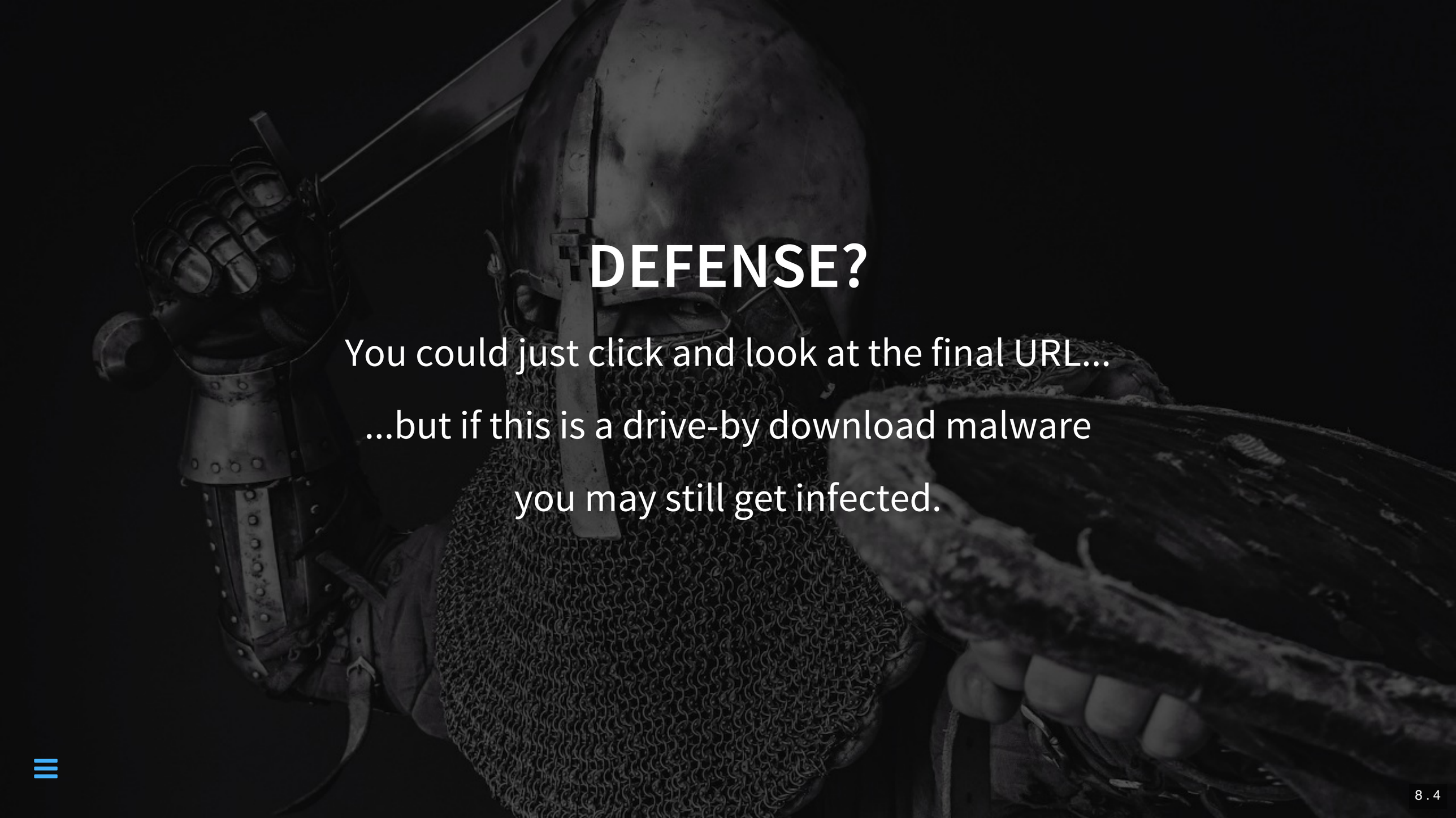
SHORTENER

Because http://tiny.cc/recover-gmail-password looks safe, right?

OPEN REDIRECTS

What about this one?

http://www.ebay.com/totally/legit/long/url/redirect.php?
url=http://malicious.example.com



DEFENSE?

You could just click and look at the final URL...

...but if this is a drive-by download malware

you may still get infected.

You can also use "link expander" services such as
http://www.linkexpander.com/

Top Link Expander & Decrypter ! Unshorten Urls in no time !

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

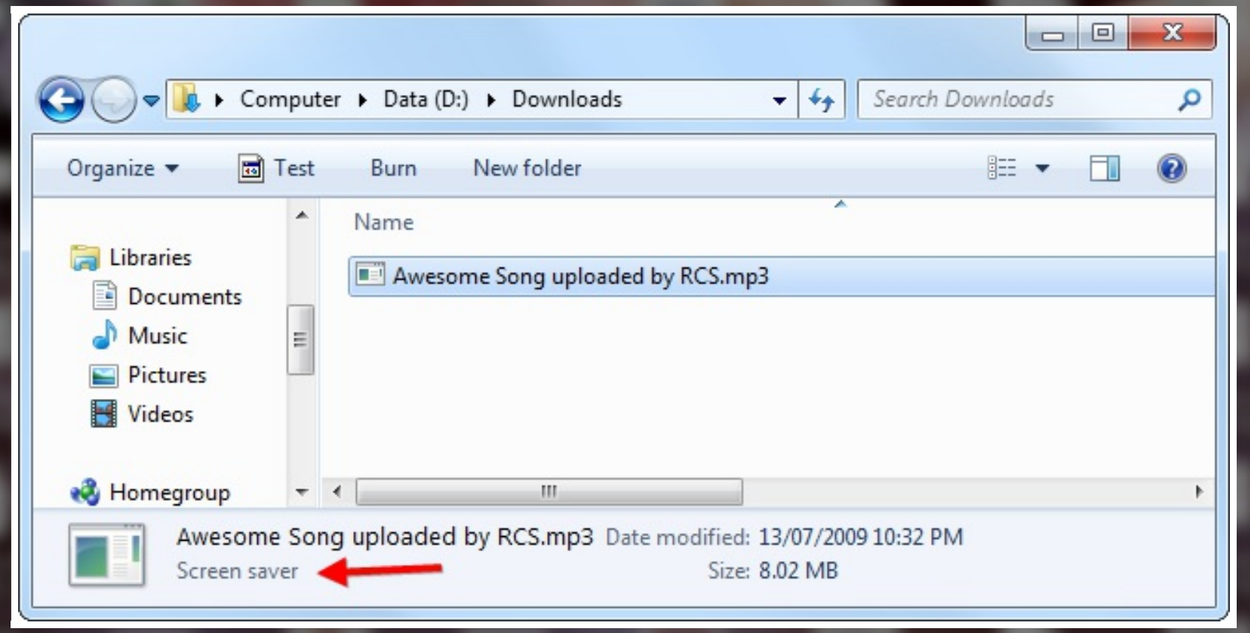
http://tiny.cc/recover-gmail-passv Expand

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	

FILE EXTENSIONS

Double click to open nude-pics.jpg.exe



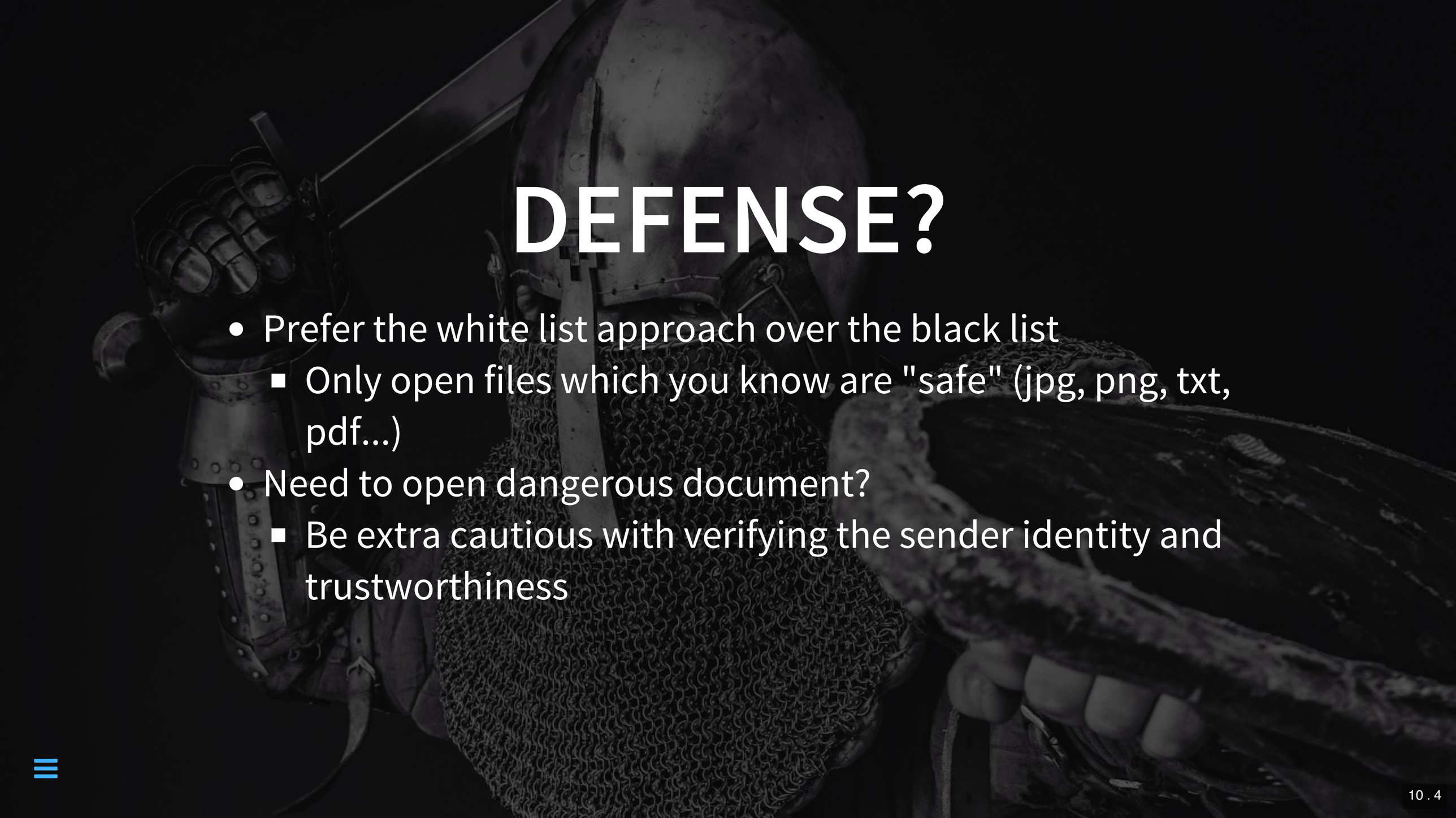

DANGEROUS FILES

DANGEROUS FILES

If it does not end with .exe, I can open it safely, right?

DANGEROUS FILES

- It's a bit more complicated
- There is more than 50 dangerous extensions
  - .pif, .msi, .com, .scr, .msc, .jar, .bat, .cmd, .vb, .js, .ps1, .msh, .lnk, .inf, .reg
  - But also .svg, .doc, .xls, .ppt...

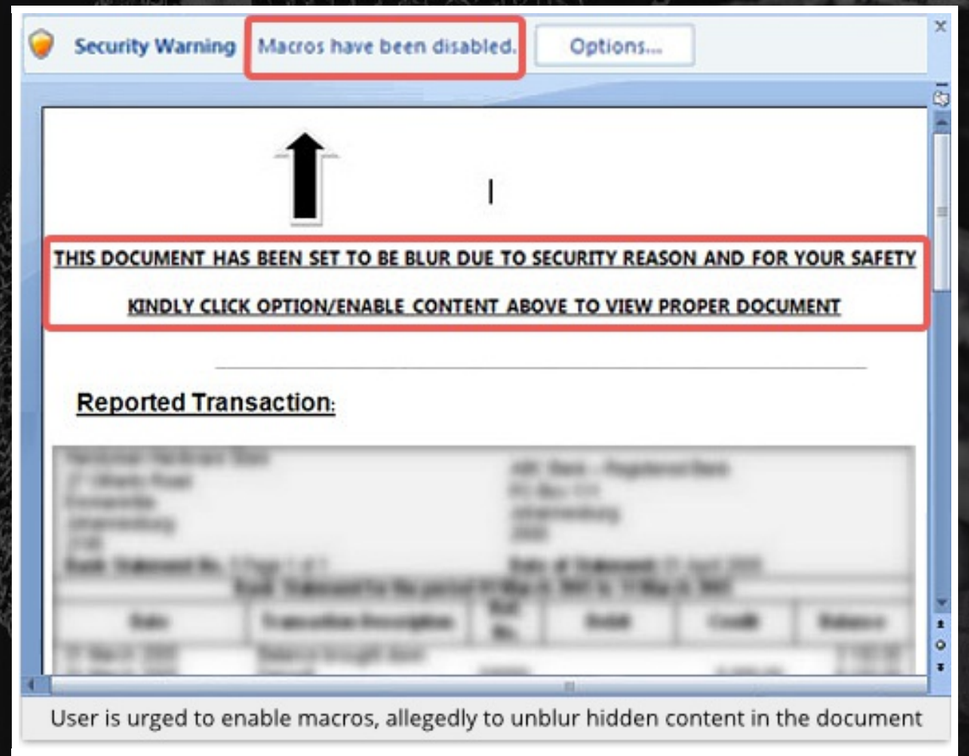


DEFENSE?

- Prefer the white list approach over the black list
  - Only open files which you know are "safe" (jpg, png, txt, pdf...)
- Need to open dangerous document?
  - Be extra cautious with verifying the sender identity and trustworthiness

DEFENSE?

- What about Office documents? Don't activate macros, whatever the document might say
  - Crooks will entice you to do so with fake motives

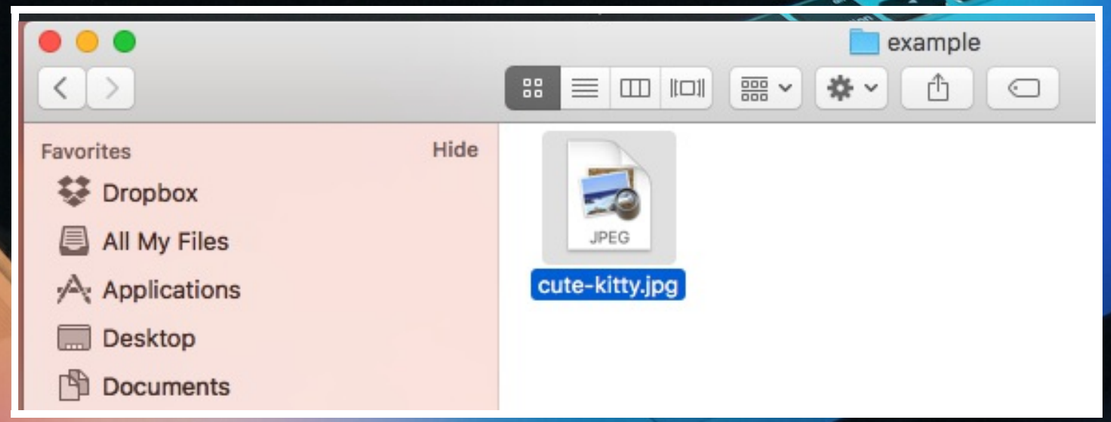


User is urged to enable macros, allegedly to unblur hidden content in the document


EVERYTHING IS SAFER ON MAC
fn
control
option
command
option
command


You can then safely open "cute-kitty.jpg "

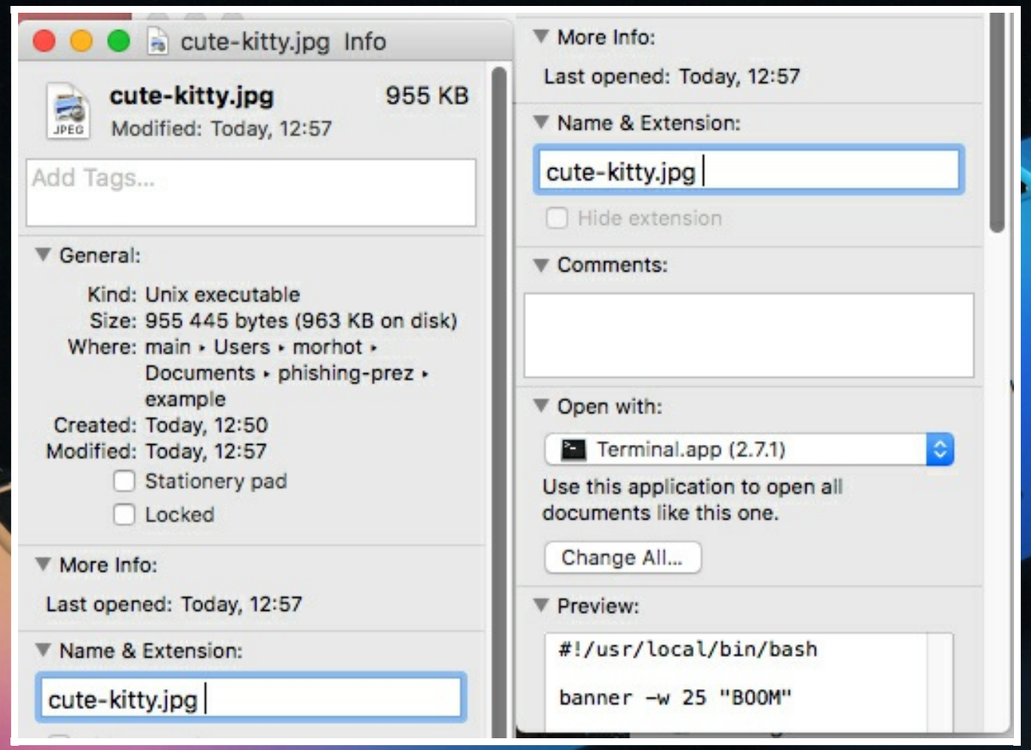
...right?


example
Favorites
Hide
Dropbox
All My Files
Applications
Desktop
Documents
JPEG
cute-kitty.jpg

...oops


morhot — cute-kitty.jpg — 80×39
STHMACLT070:~ morhot$ /Users/morhot/Documents/phishing-prez/cute-kitty.jpg\ ; exit;

".jpg<*space*>", not ".jpg"



Unknown? Executable ? Let's open it with Terminal!

DEFENSE?

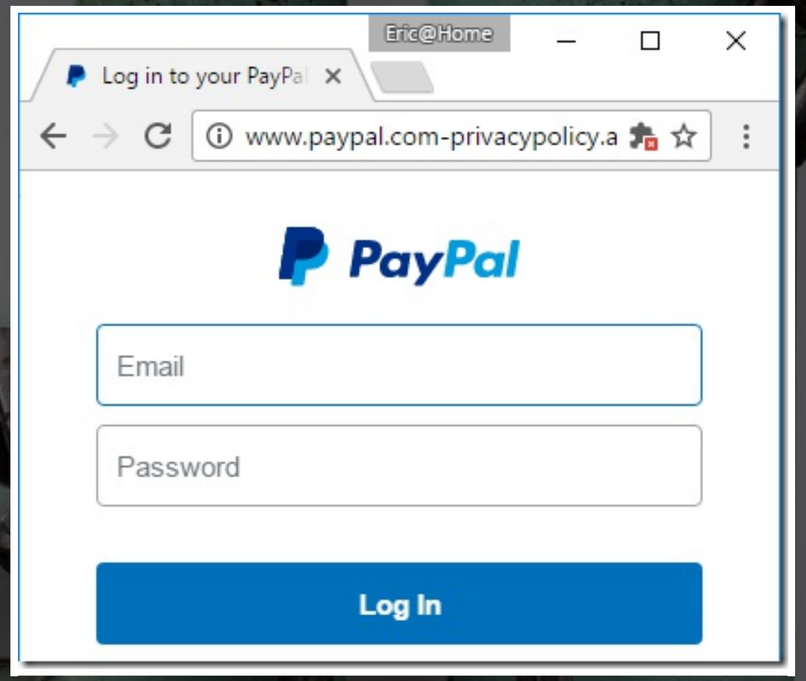
- Right-click > Properties on Windows
  - Also configure it to always show known extensions
- Cmd+I or Right-click > Get Info on Mac
  - Preview function can help a lot too

THE "GREEN PADLOCK"

There is the green padlock, I'm safe then, right?

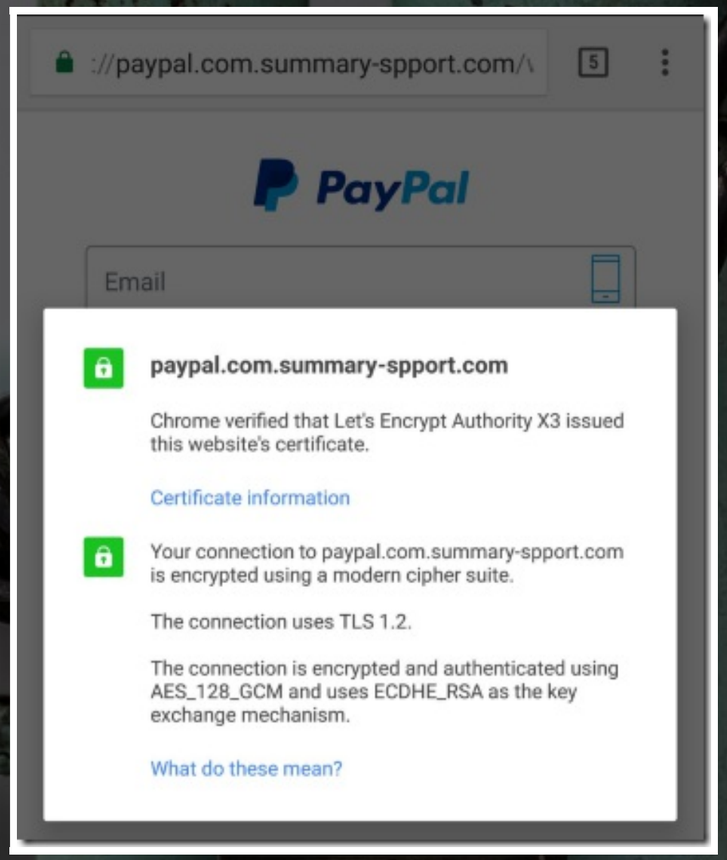
THE GREEN PADLOCK

What do you think of this website?



THE GREEN PADLOCK

...woops

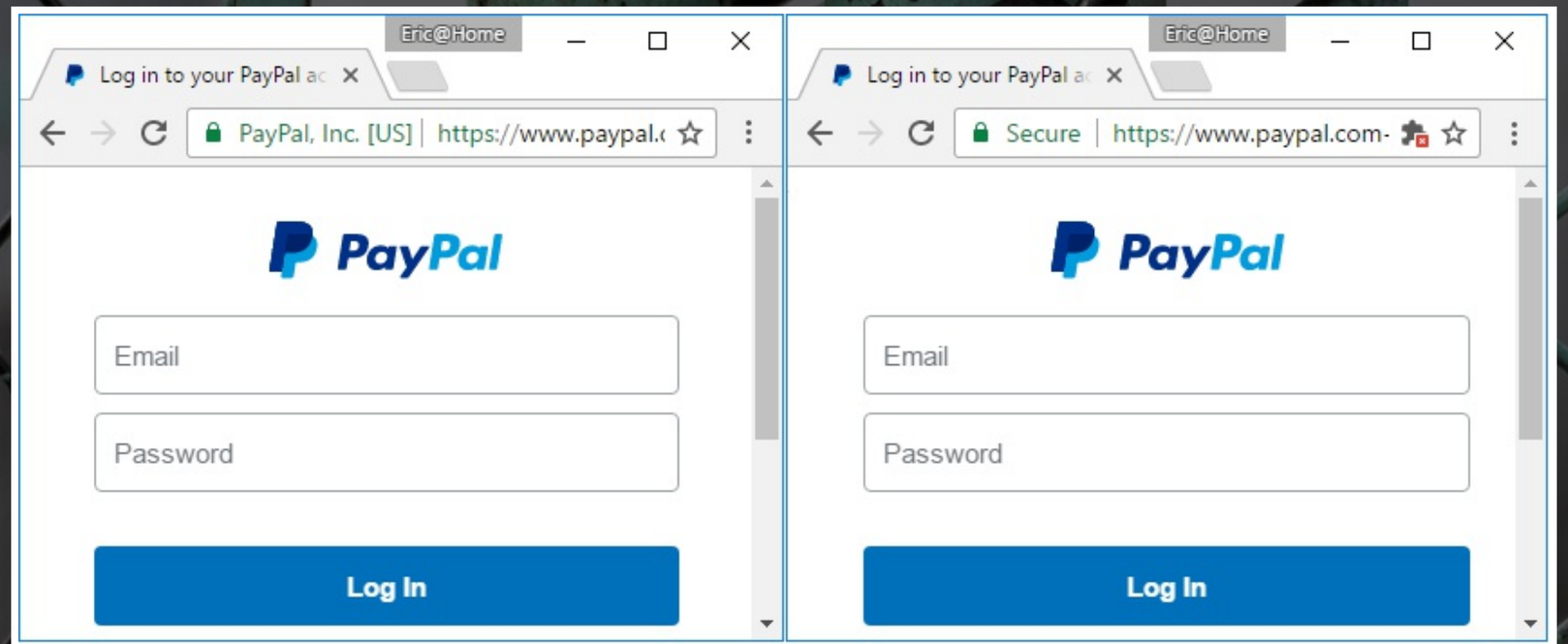


HTTPS TRUE MEANING

- The green padlock only means one thing
  - The communication between your computer and the website is encrypted...
  - ...and the certificate used for the encryption have been proved to be legit...
  - ...for *THIS* domain
- That's all.

HTTPS IS EVERYWHERE

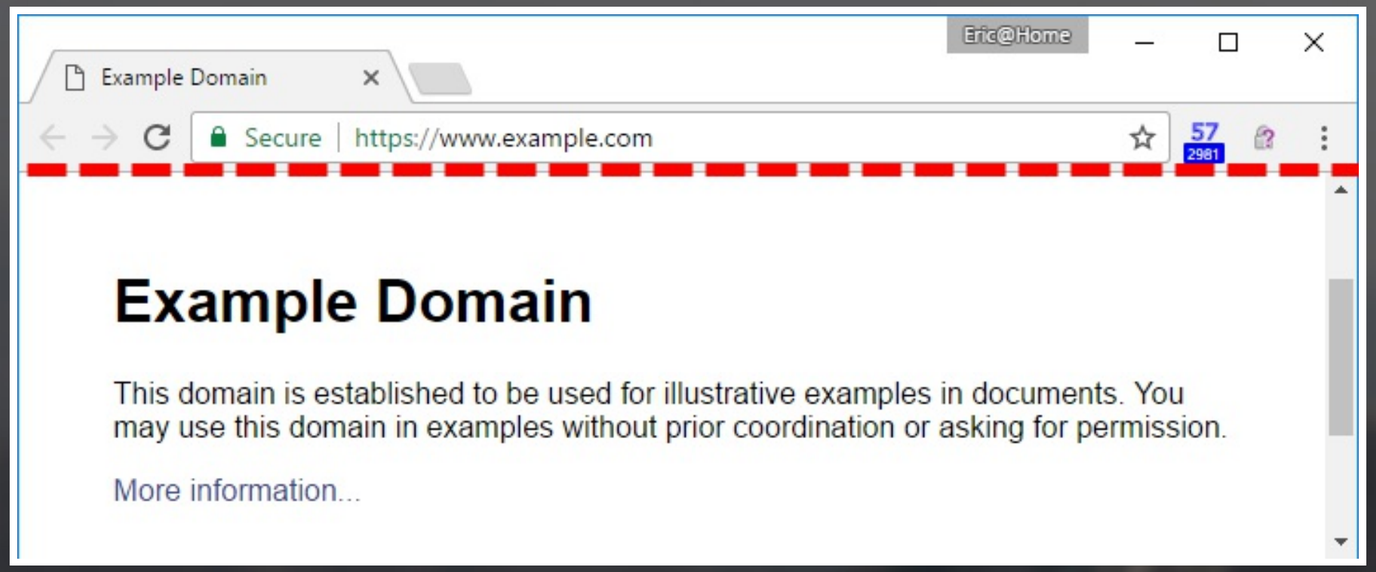
- Getting a recognized certificated used to be long and costly
  - Now, it's free and takes less than 5 minutes
  - Phishing website use HTTPS to look trustworthy



One real, one fake, your account is at stake.

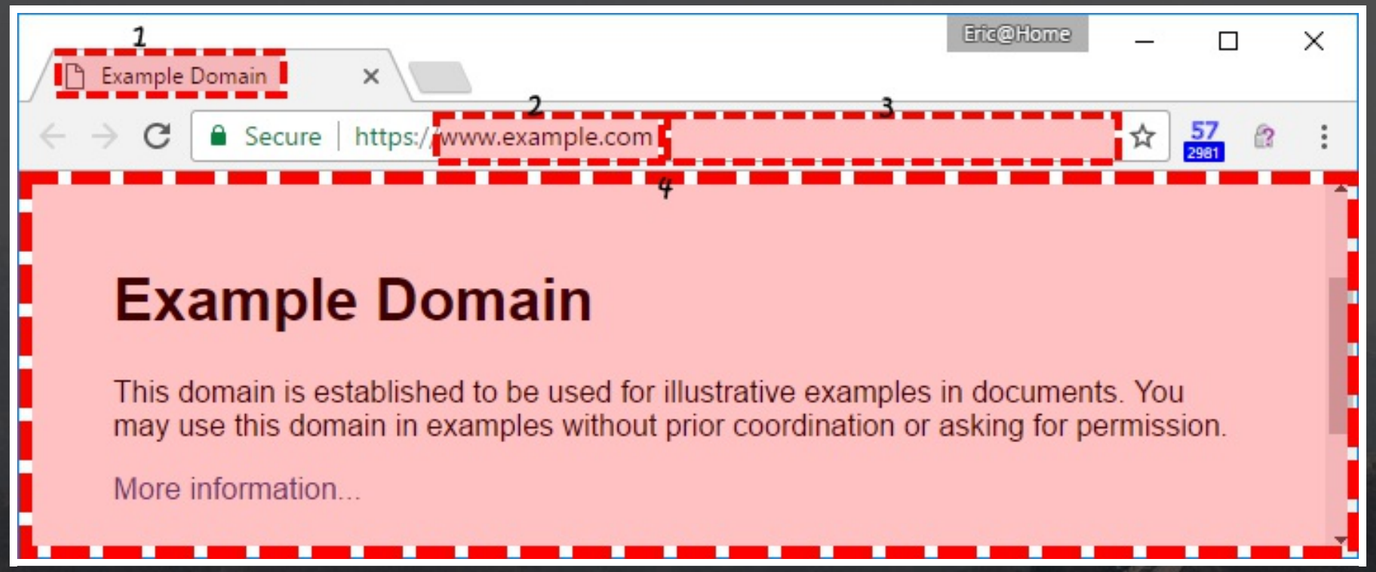
THE LINE OF DEATH

Beyond this line, you can't trust anything

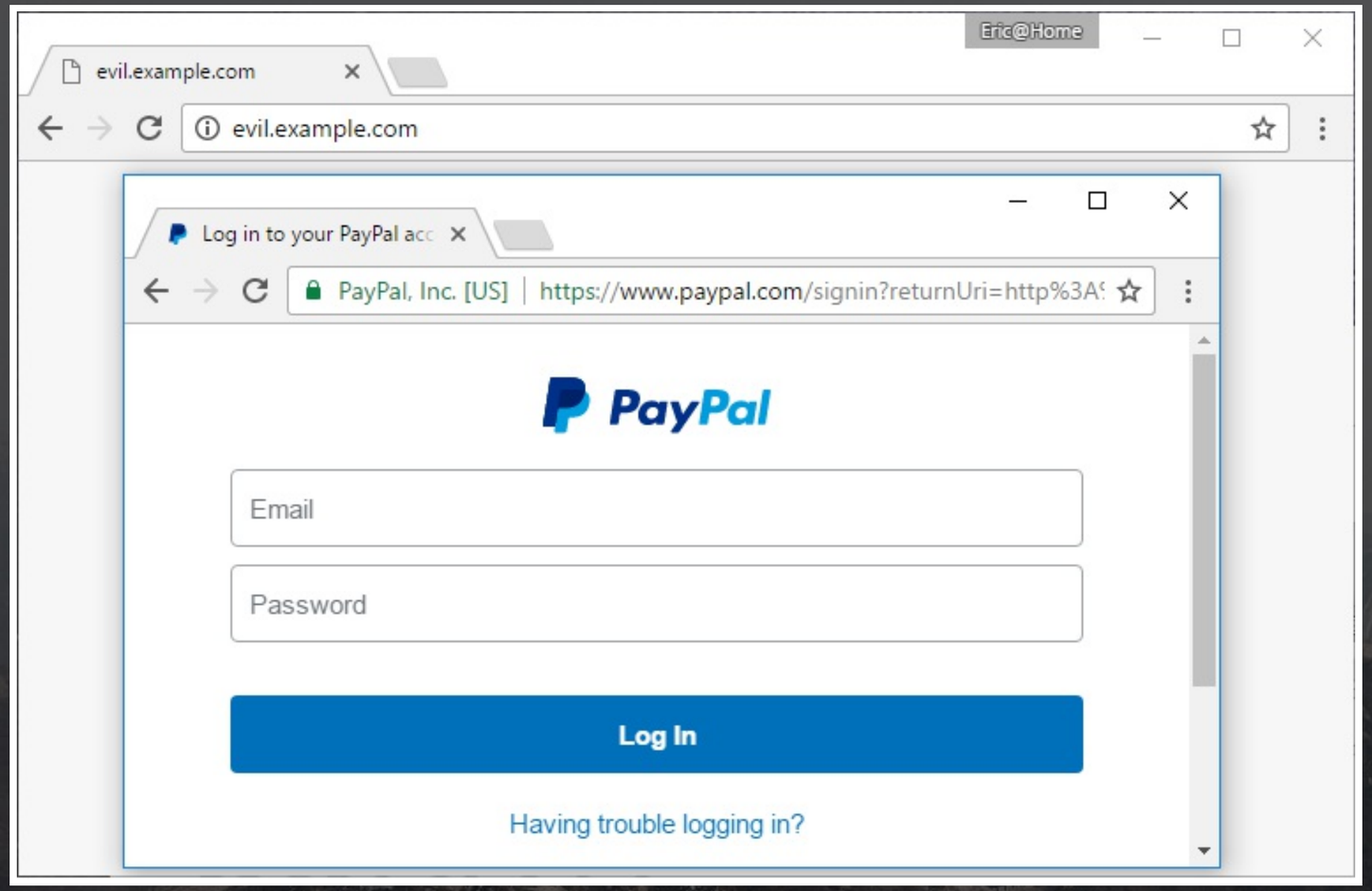


THE LINE OF DEATH

Even above this line, trustworthiness is...relative

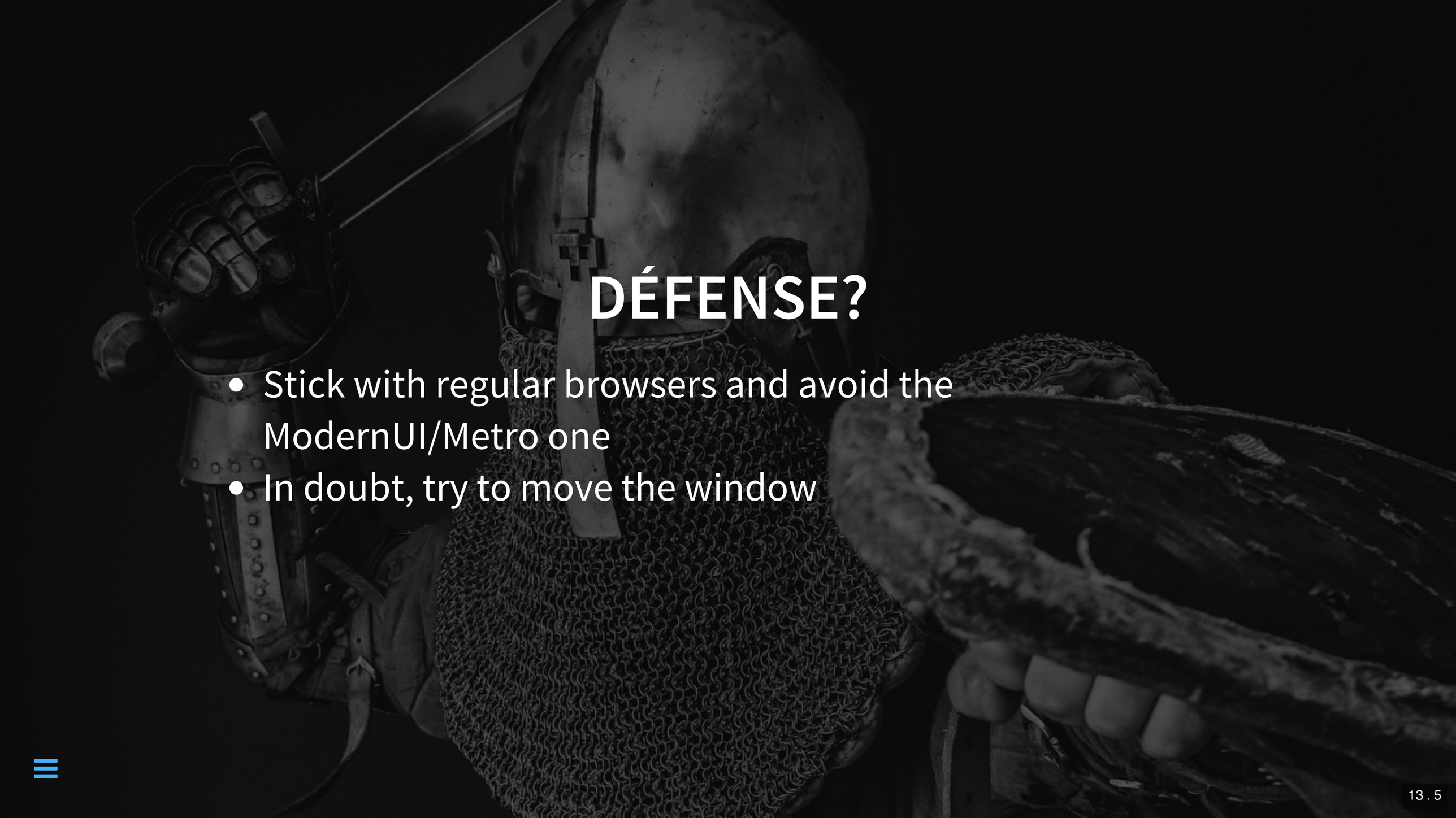


What do you think of this website?



METRO/MODERNUI

...It's even worse...

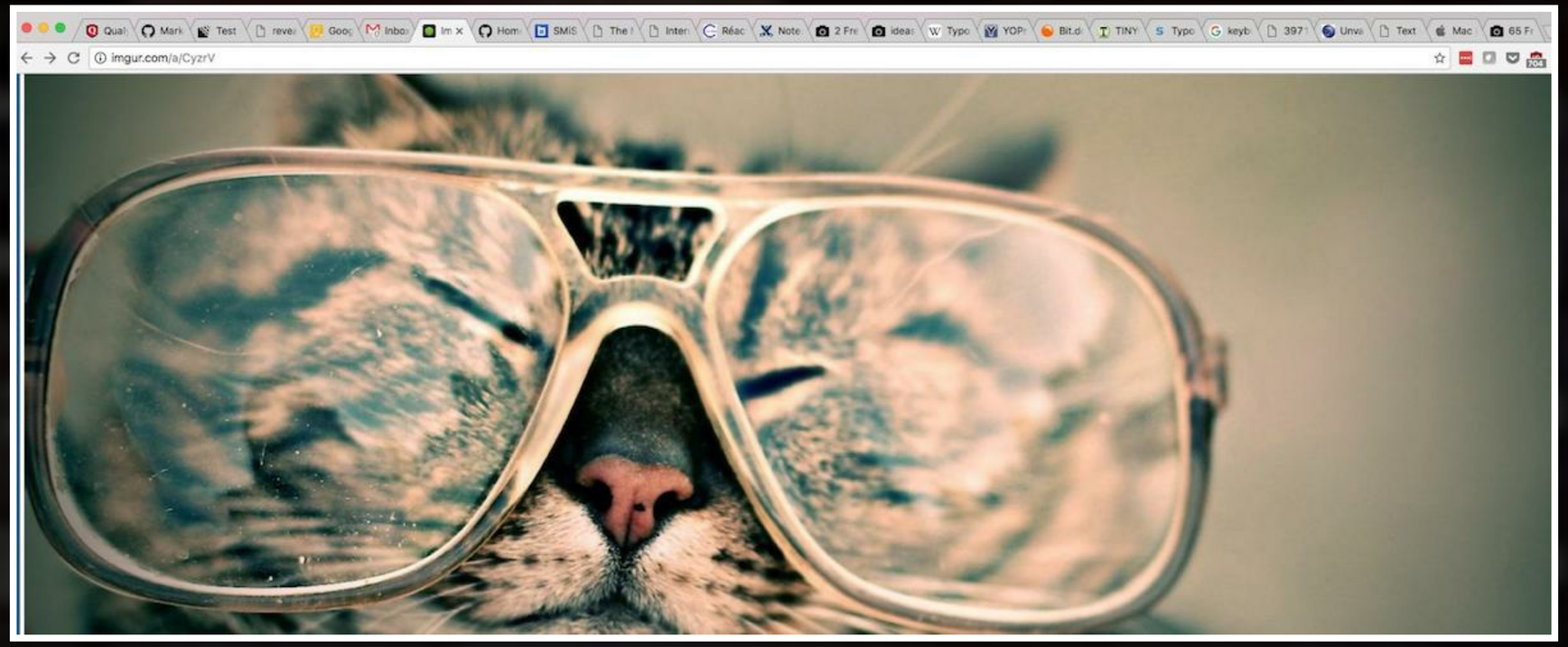


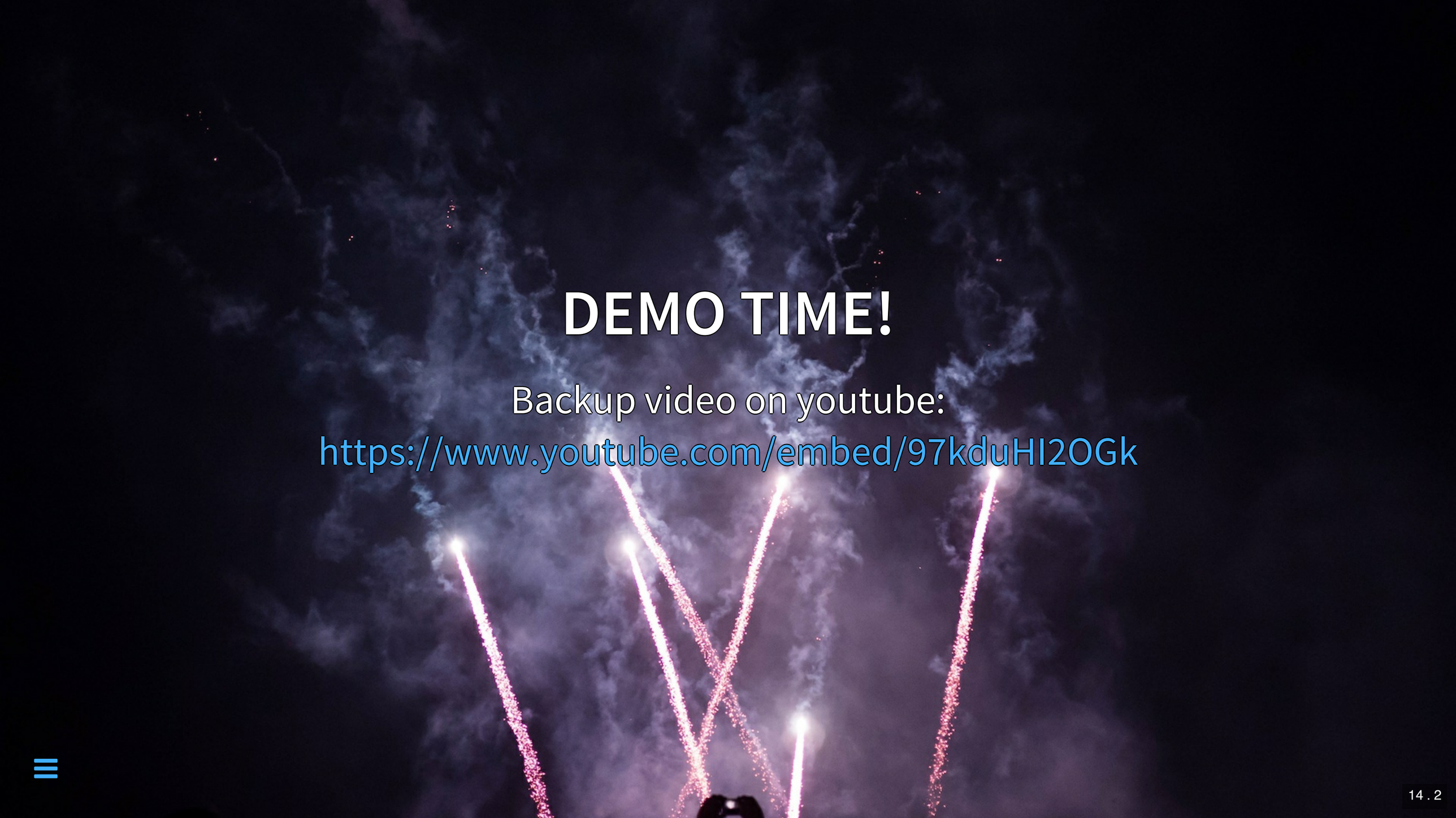
DÉFENSE?

- Stick with regular browsers and avoid the ModernUI/Metro one
- In doubt, try to move the window

TABNAPPING

If your browser often looks like mine, you're in trouble




DEMO TIME!
Backup video on youtube:
https://www.youtube.com/embed/97kduHI2OGk


DEMO VIDEO

HOW CAN I DEFEND AGAINST SUCH MADNESS?

- Look at the URL before logging in
- Password managers help a lot
  - They won't autocomplete if it's not the right website


OK, THAT'S ENOUGH FOR TODAY


ANY QUESTIONS?