

PHISHING TECHNIQUES

AND HOW TO DEFEND AGAINST THEM

Morgan Hotonnier

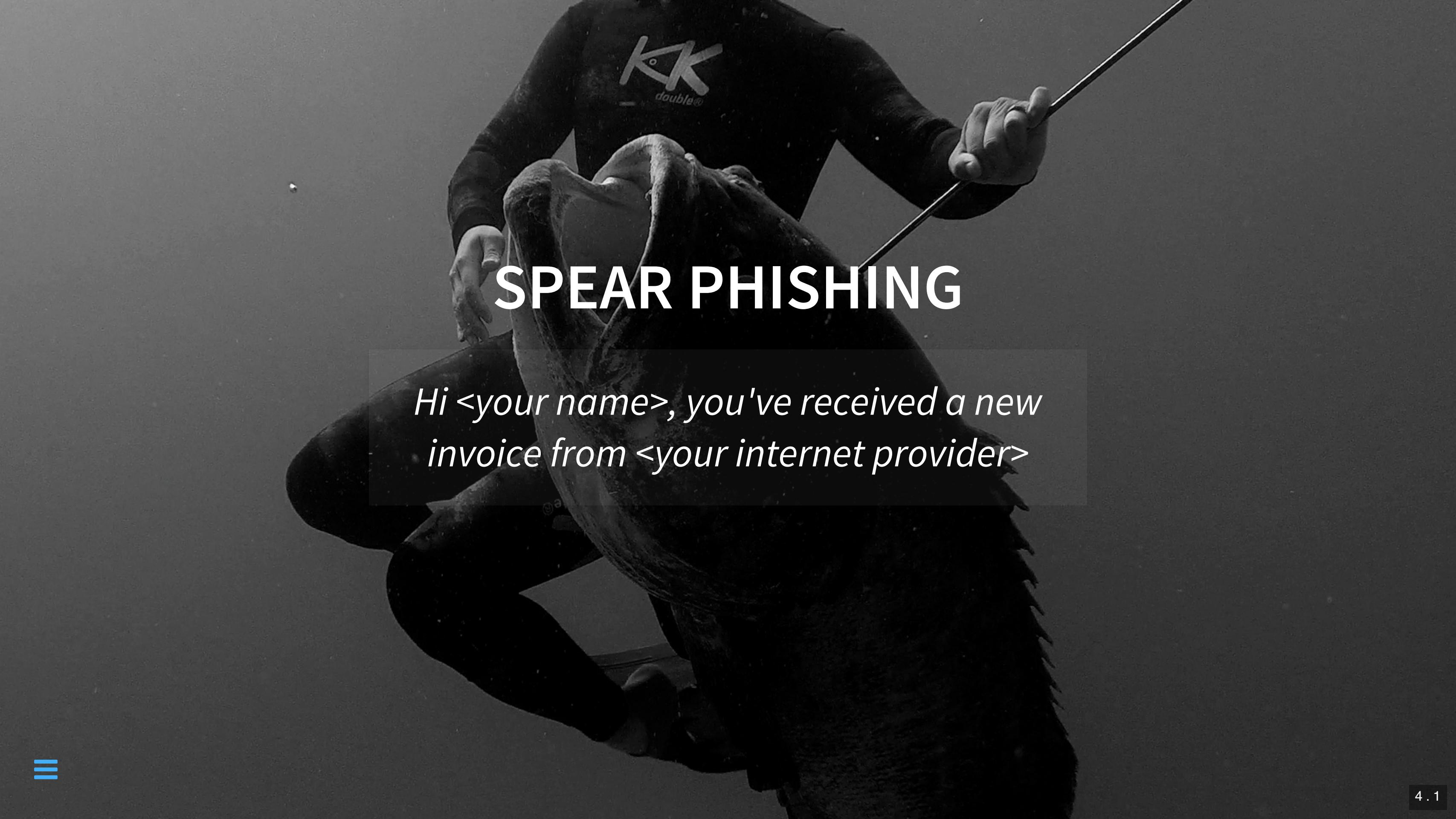
<f> for fullscreen, <space> for next slide

PHISHWHAT?

- Technique to **manipulate** you into
 - revealing sensitive information
 - installing a malware
 - sending money
 - all of the above

PHISHING "LEVELS"

- Classic, mass phishing
- Spear phishing
- Whaling



SPEAR PHISHING

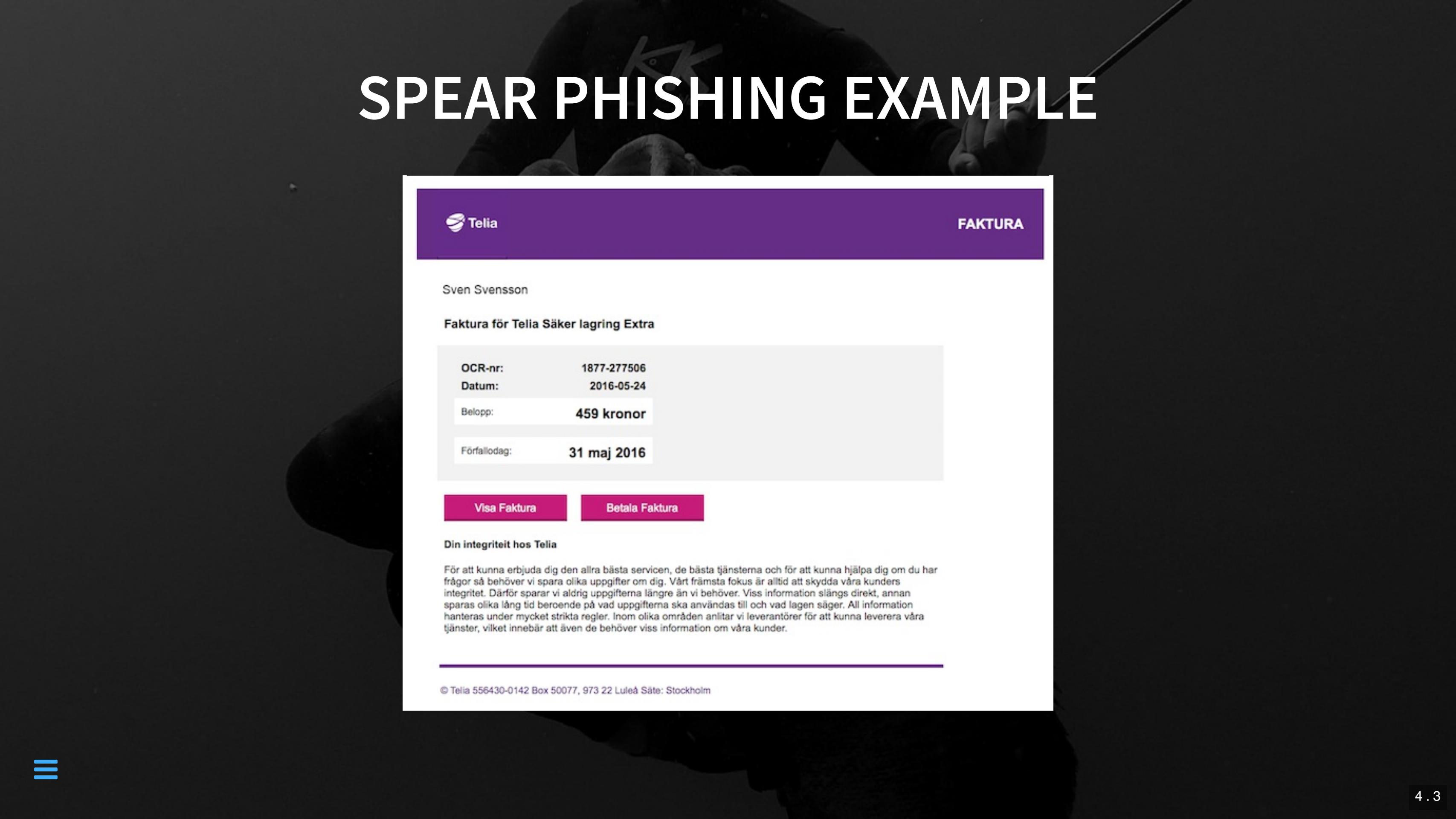
*Hi <your name>, you've received a new
invoice from <your internet provider>*

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

WHAT IS SPEAR PHISHING

- Phishing++
- Tailored to specific individuals or groups
- Using personal details collected from social medias, previous hacks, etc

SPEAR PHISHING EXAMPLE



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 integritet 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



WHALING

Can we send out a wire transfer today?

WHAT IS WHALING

- Spearphishing++
- Targets "big" victims (important or wealthy)
 - CEO, CFO, etc
- Uses detailed personal information and corporate lingo

WHALING EXAMPLE

● 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

IT'S NOT JUST ABOUT EMAILS!

- Vishing
- Smishing
- Social media

VISHING

"Hi! I'm from Microsoft tech support"

WHAT IS VISHING

- Phishing by phone, more expensive for the attacker
 - But greater conversion rate :)
- They have call centers dedicated to this kind of scam
- Don't trust the CallerID, it can be faked



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

VISHING SAMPLE

Bank of America



A blurred background image of a person sitting at a desk in a dark room, looking at a laptop screen. The person is wearing a dark t-shirt and shorts. The laptop screen displays a message: "You've received a MMS, click [here](#) to open".

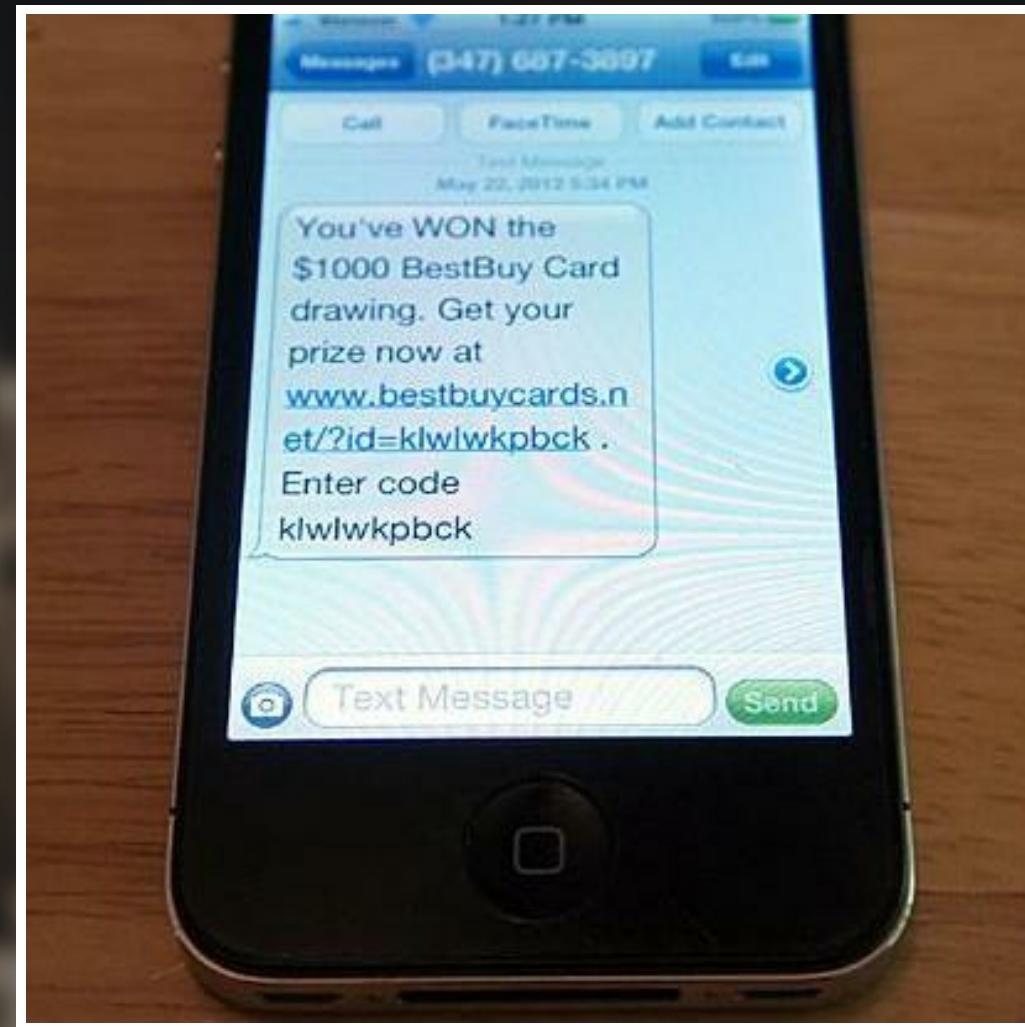
SMISHING

"You've received a MMS, click [here](#) to open"

SMISHING EXAMPLE



When it's too good to be true...



...it probably is



What were you doing in this video? Lol!

SOCIAL NETWORK PHISHING

As always, preying on human weaknesses:

- Curiosity
- Fear of being banned from the platform
- Sex

Curiosity kills the cat

A screenshot of a smartphone screen showing a Facebook post. The post contains a warning about a phishing scam. A red box highlights the word "Phishing Scam" in the post, and a red arrow points from this box to a link in the comment section.

If someone post a comment to one of your posts that say's "What are you doing in this video" and gives a link...it's a virus! Don't click it!

19 minutes ago · ·

and like this.

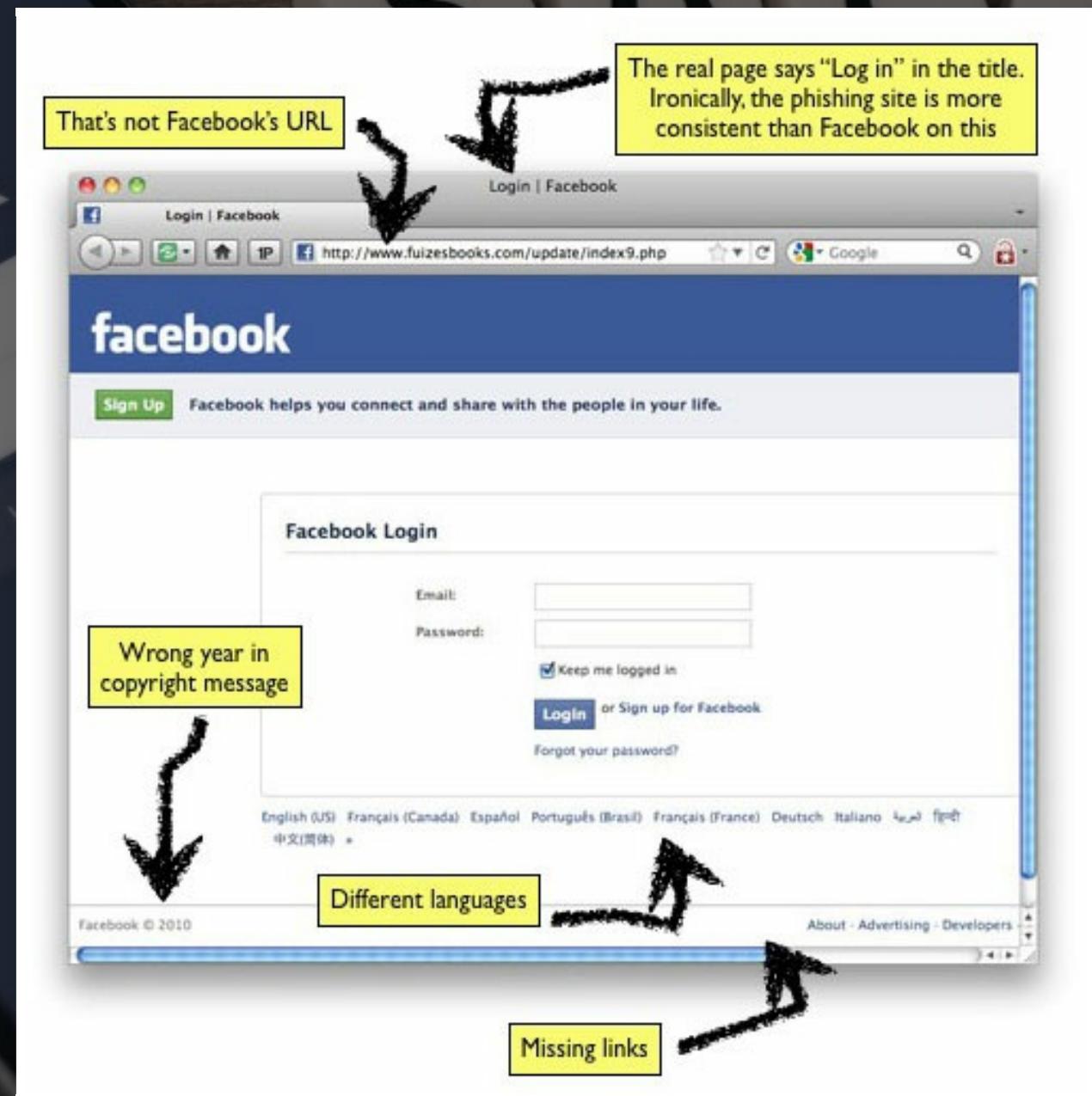
Whats up wut are you doinggg in this vvideoooooo???? lol!! <http://apps.facebook.com/o/mglozzz/?shjfmowx>

3 minutes ago

Phishing Scam

...or at least your sensitive data

You need to login again...wait what?

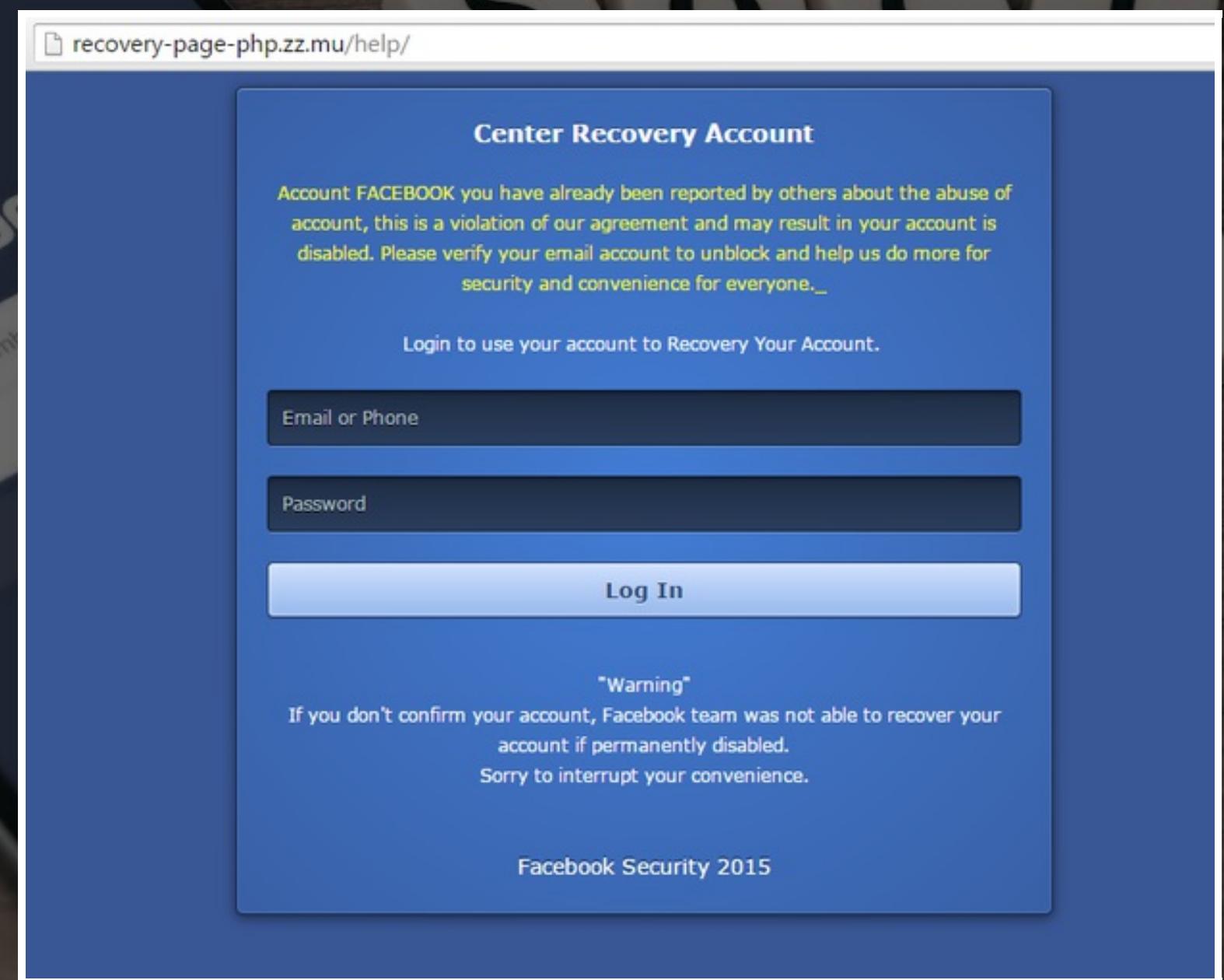


If you don't do what I say you will be deactivated



Don't mess with the Facebook police

Wow, he clicked! Mmmm, give me your login details!



He complied again?!

...Simon says: give me your credit card number!



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

*“Cover up that bosom, which I can't endure
to look on.”*

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

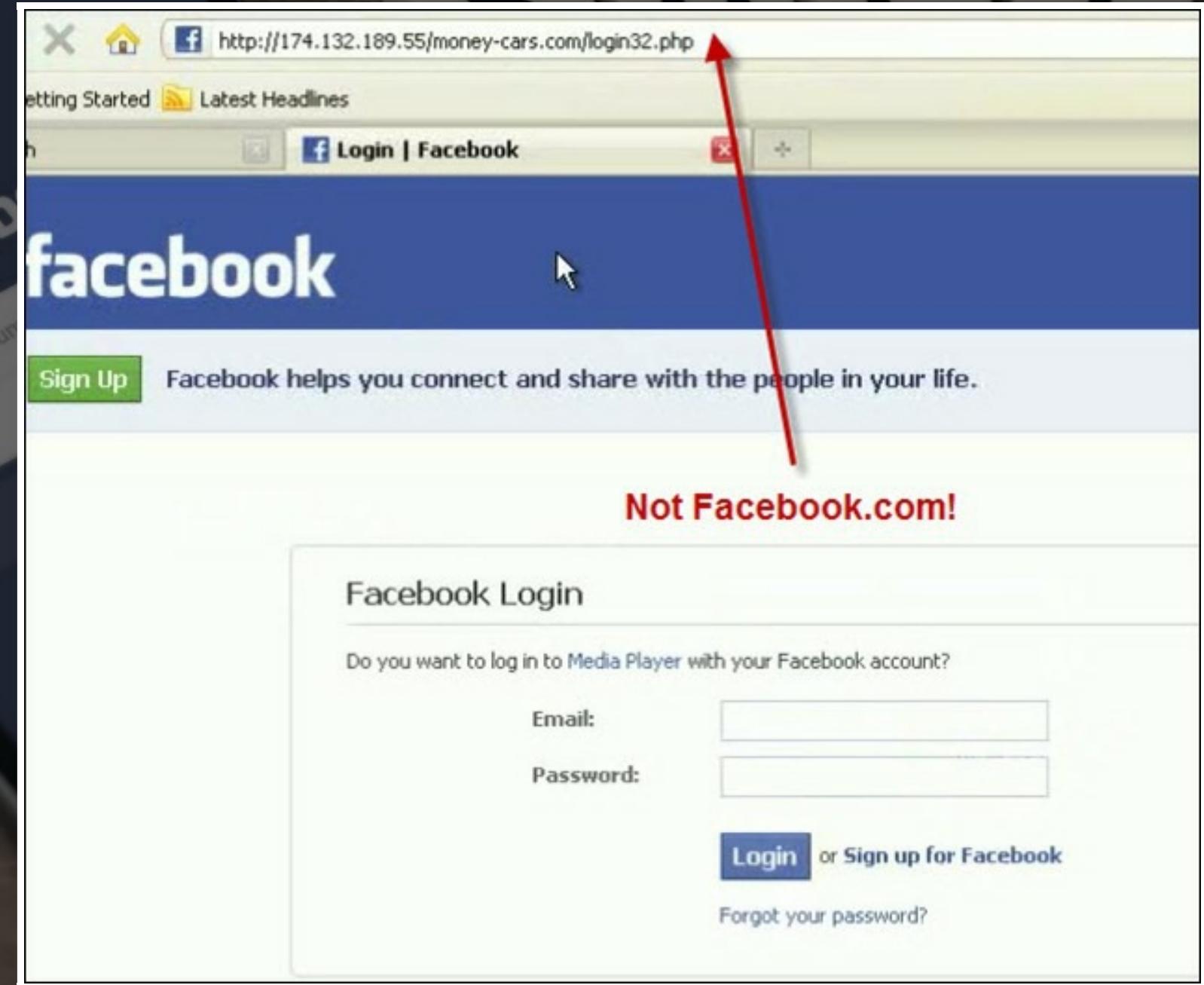
Latest Headlines

+  Length: 3:17
3 minutes ago

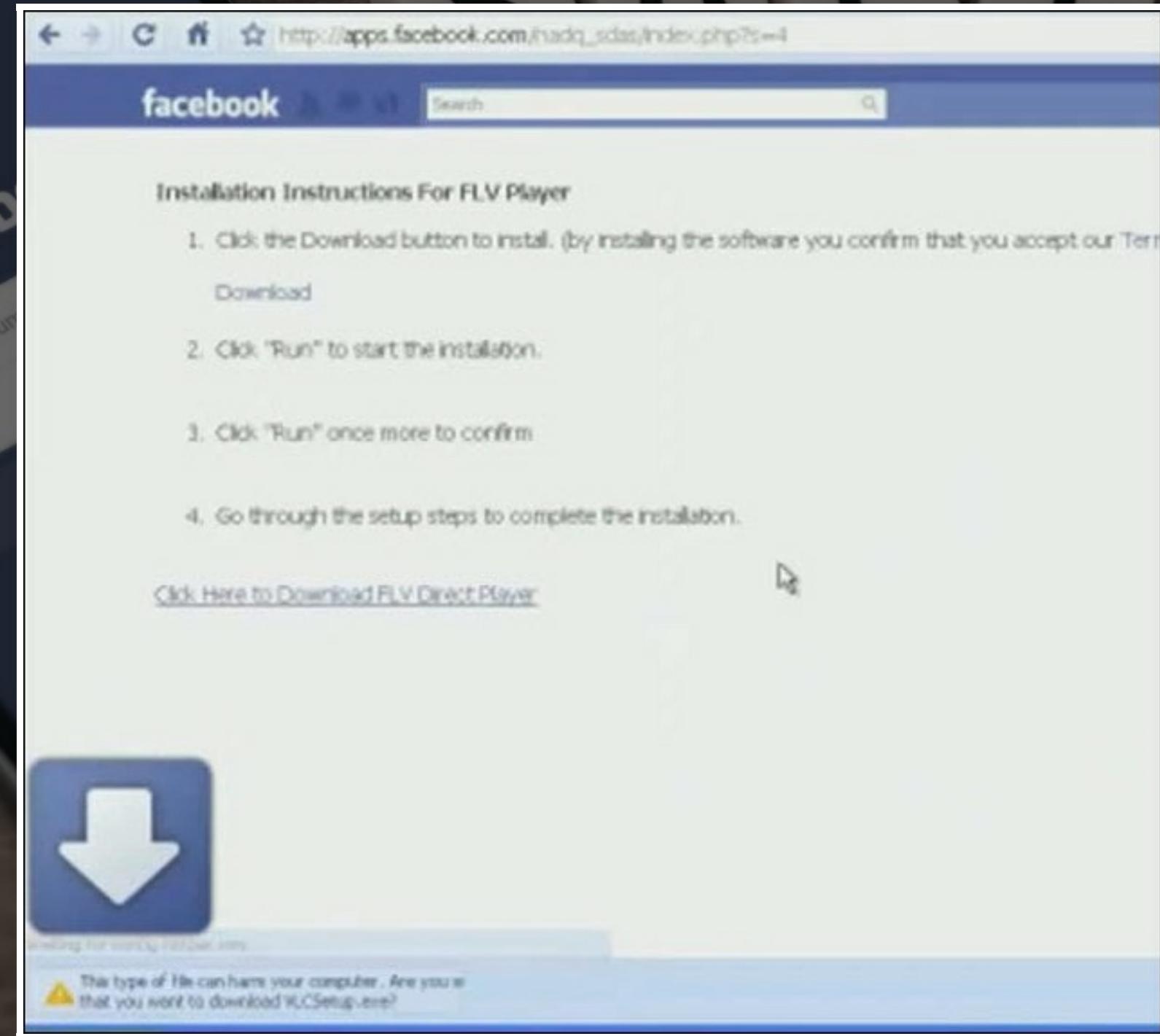
Lamar Johnson **this is without a doubt the most hilarious video ever. LOL!**
  Naughty Camera Prank! [HQ]
apps.facebook.com
Length: 3:17
4 minutes ago

Thadeus Ngiela **this is without a doubt the most hilarious video ever. LOL!**
  Naughty Camera Prank! [HQ]
apps.facebook.com
Length: 3:17
5 minutes ago

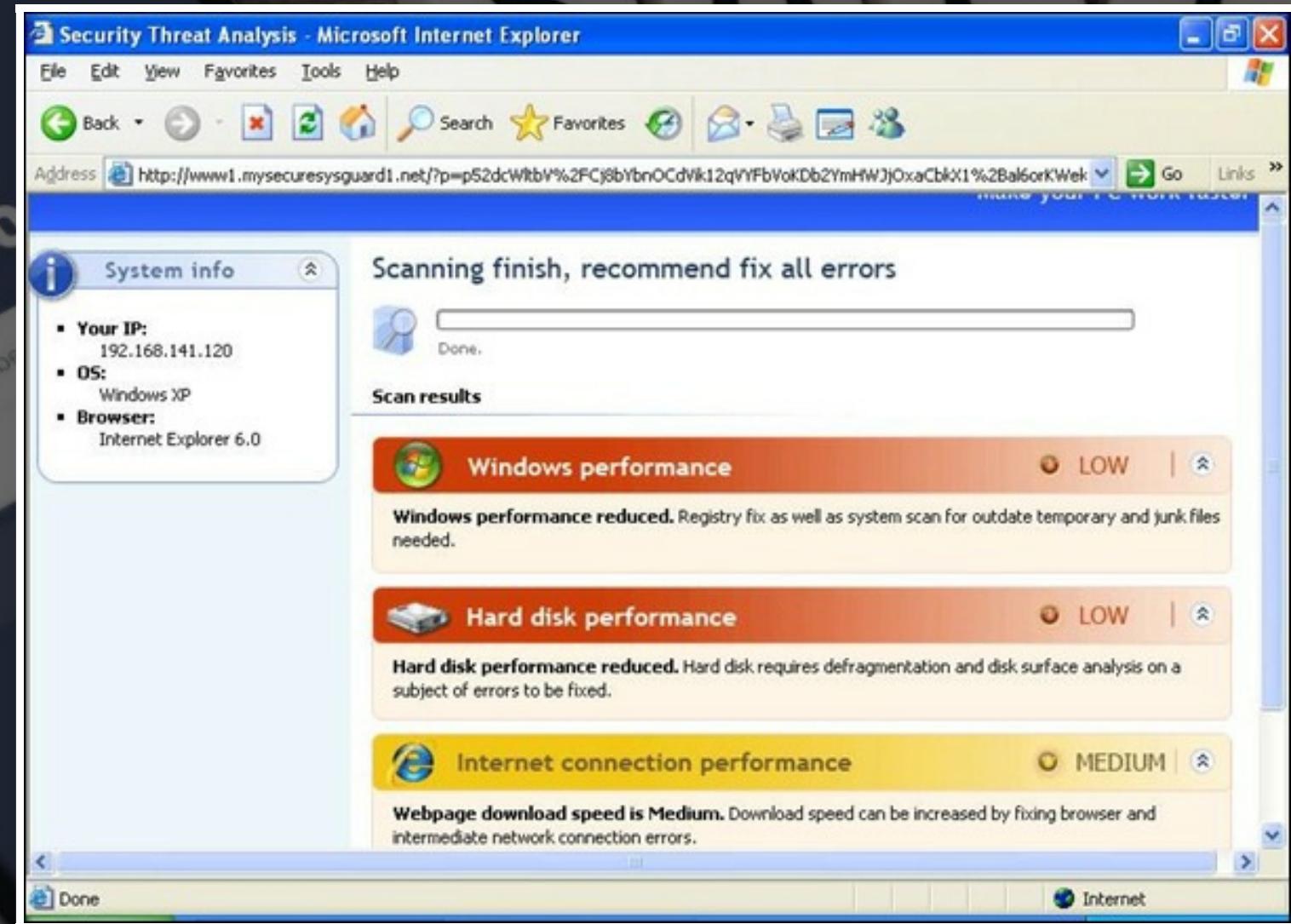
Again, please give me your password



Also, please download this totally fake video player plugin



#IronyAward, you have a virus!



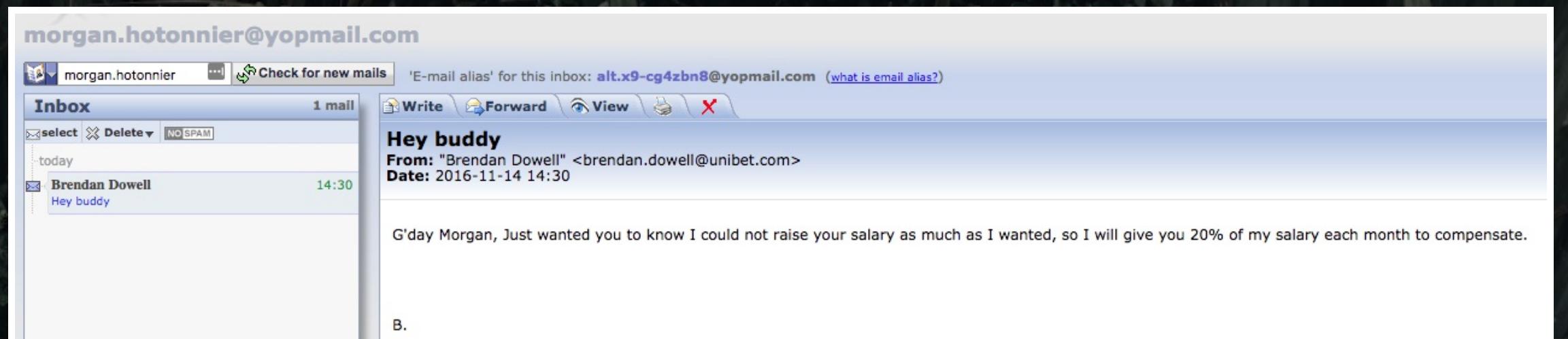
Just pay for my fake antivirus and everything will go away

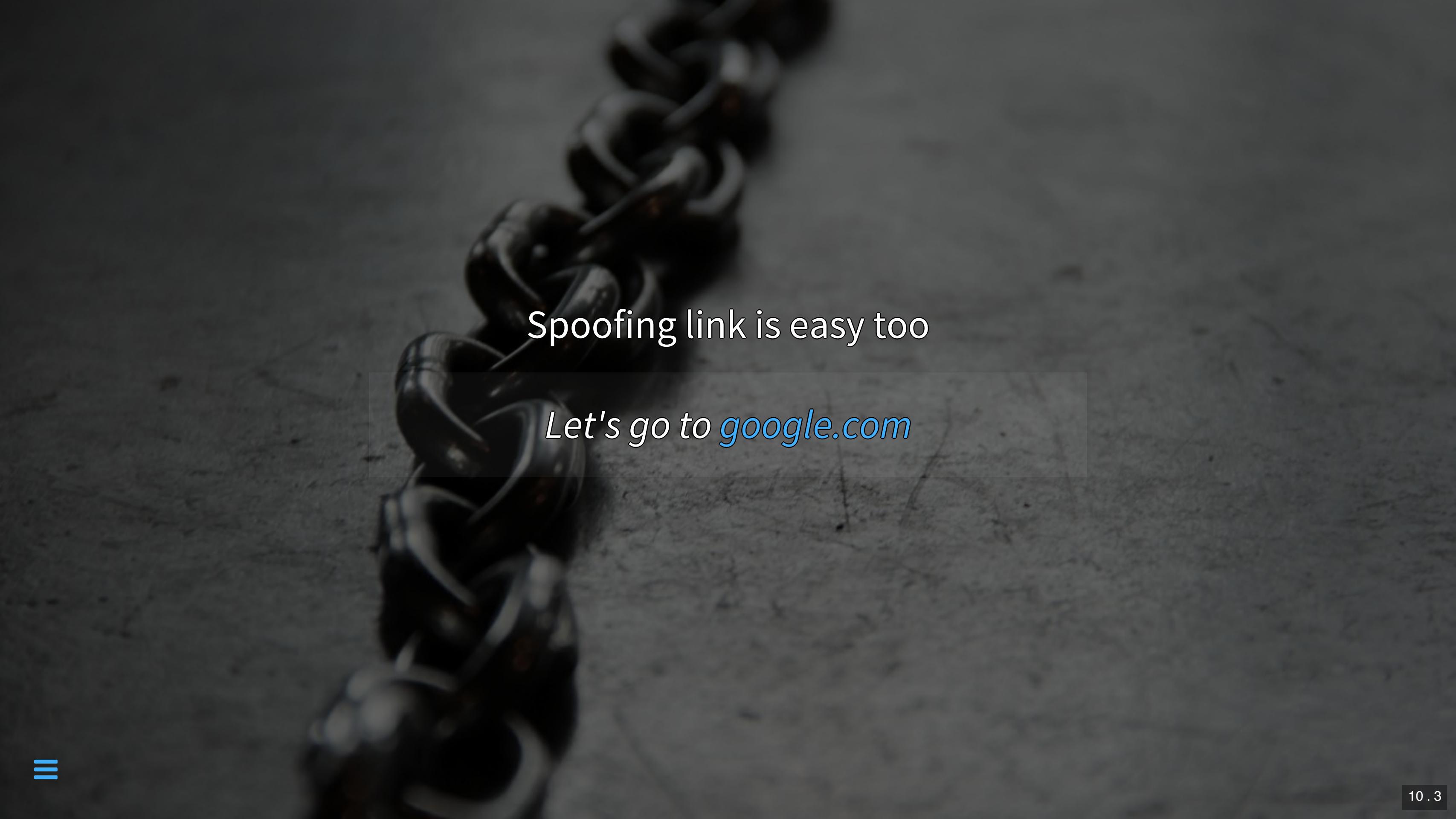


SPOOFING

The most common phishing technique

Spoofing email is doable





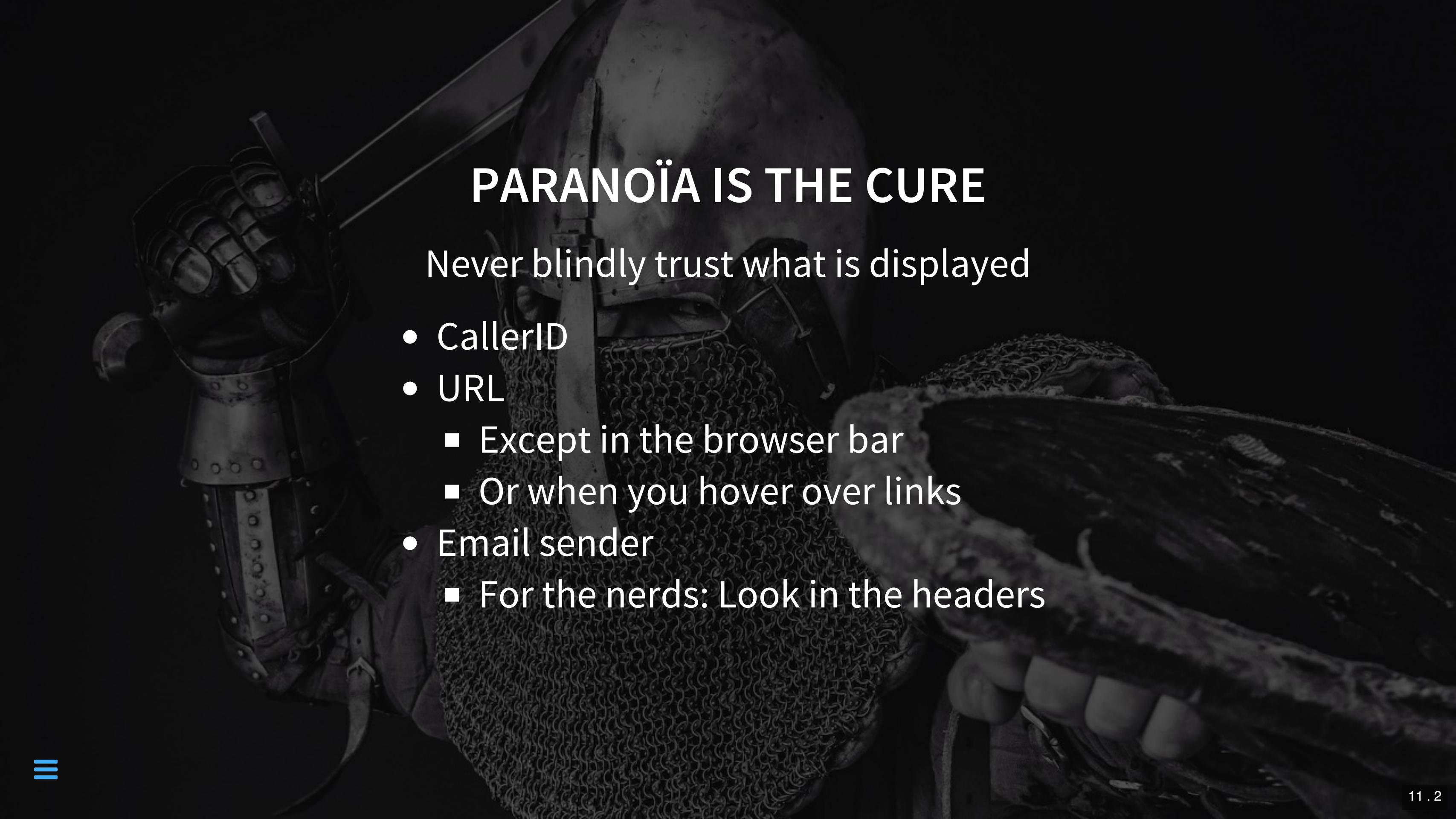
Spoofing link is easy too

Let's go to google.com

SPOOFING CALLERID? EASY PEASY

A black and white photograph of a knight in full armor. The knight is wearing a helmet with a visor, chainmail, and leather gauntlets. He is holding a long-sabre with both hands. The background is dark.

HOW TO DEFEND YOURSELF?

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

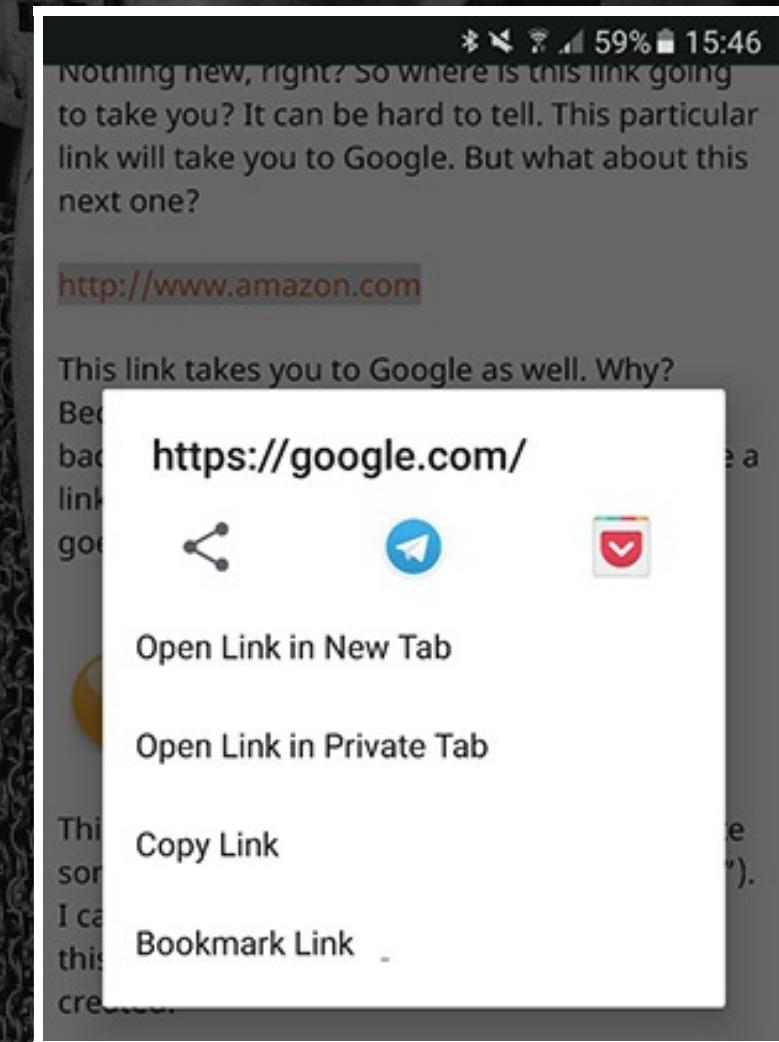
PARANOÏA IS THE CURE

Never blindly trust what is displayed

- CallerID
- URL
 - Except in the browser bar
 - Or when you hover over links
- Email sender
 - For the nerds: Look in the headers

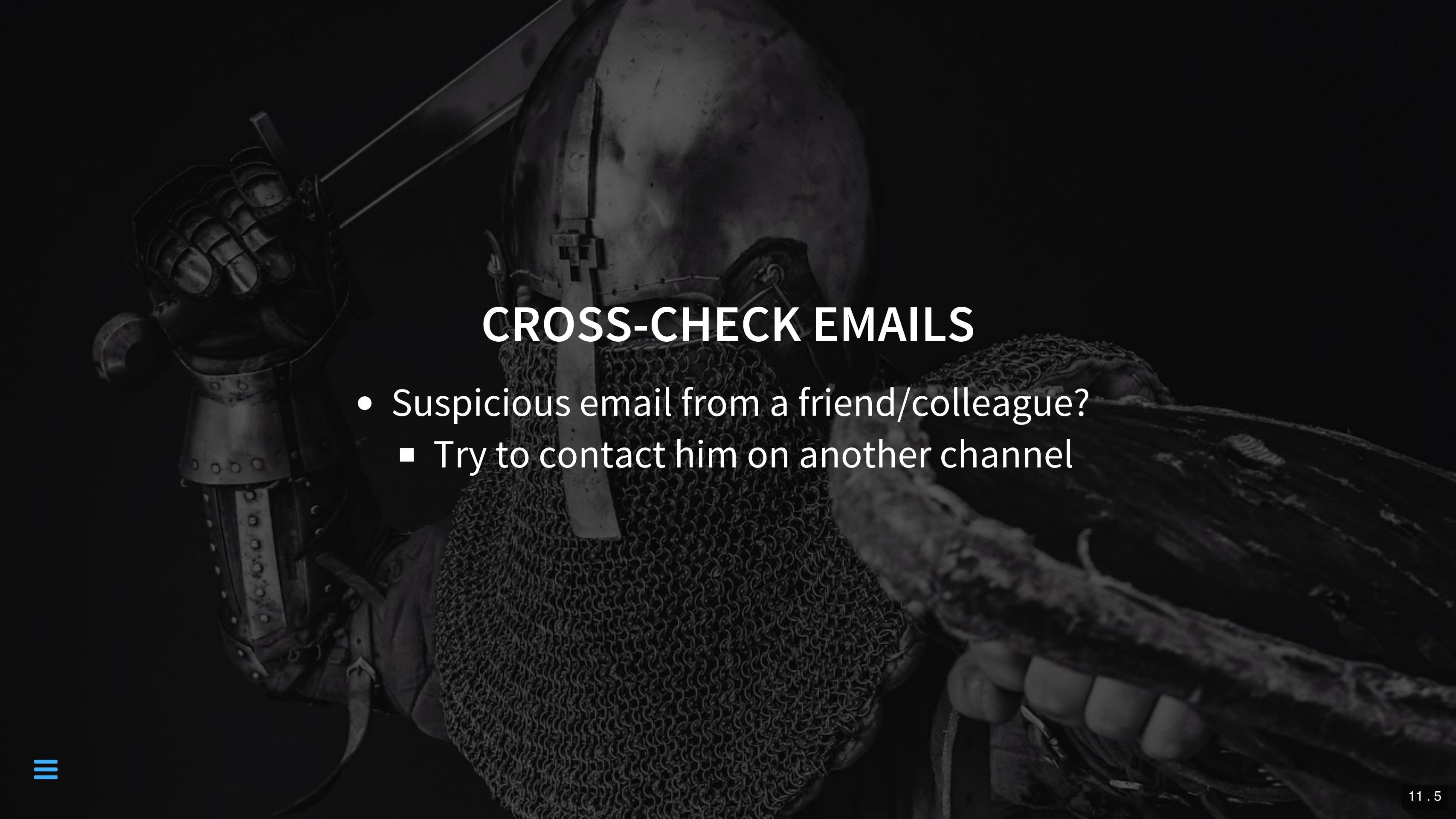
LINKS ON SMARTPHONES

- Long press on links to show the real destination



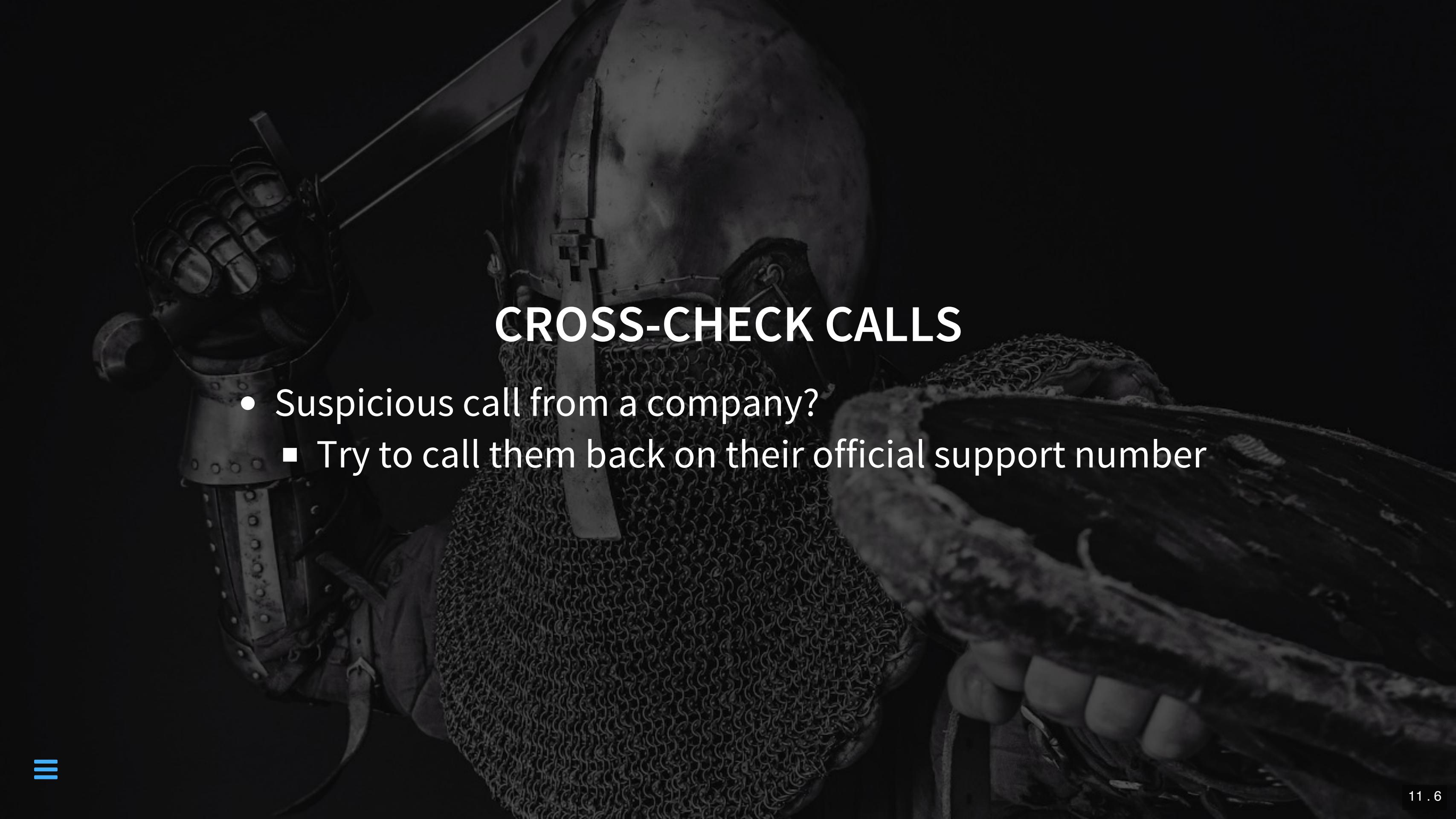
URL BAR ON SMARTPHONES

- Smartphone browsers tend to hide address bar
 - Saving some screen space, but at a cost
 - Just scroll up a page and it will come back

A black and white photograph of a knight in full armor. He is wearing a helmet with a visor, chainmail, and leather straps. He is holding a long-sword with both hands, the hilt visible in his left hand and the blade extending towards the bottom right. The background is dark and out of focus.

CROSS-CHECK EMAILS

- Suspicious email from a friend/colleague?
 - Try to contact him on another channel



CROSS-CHECK CALLS

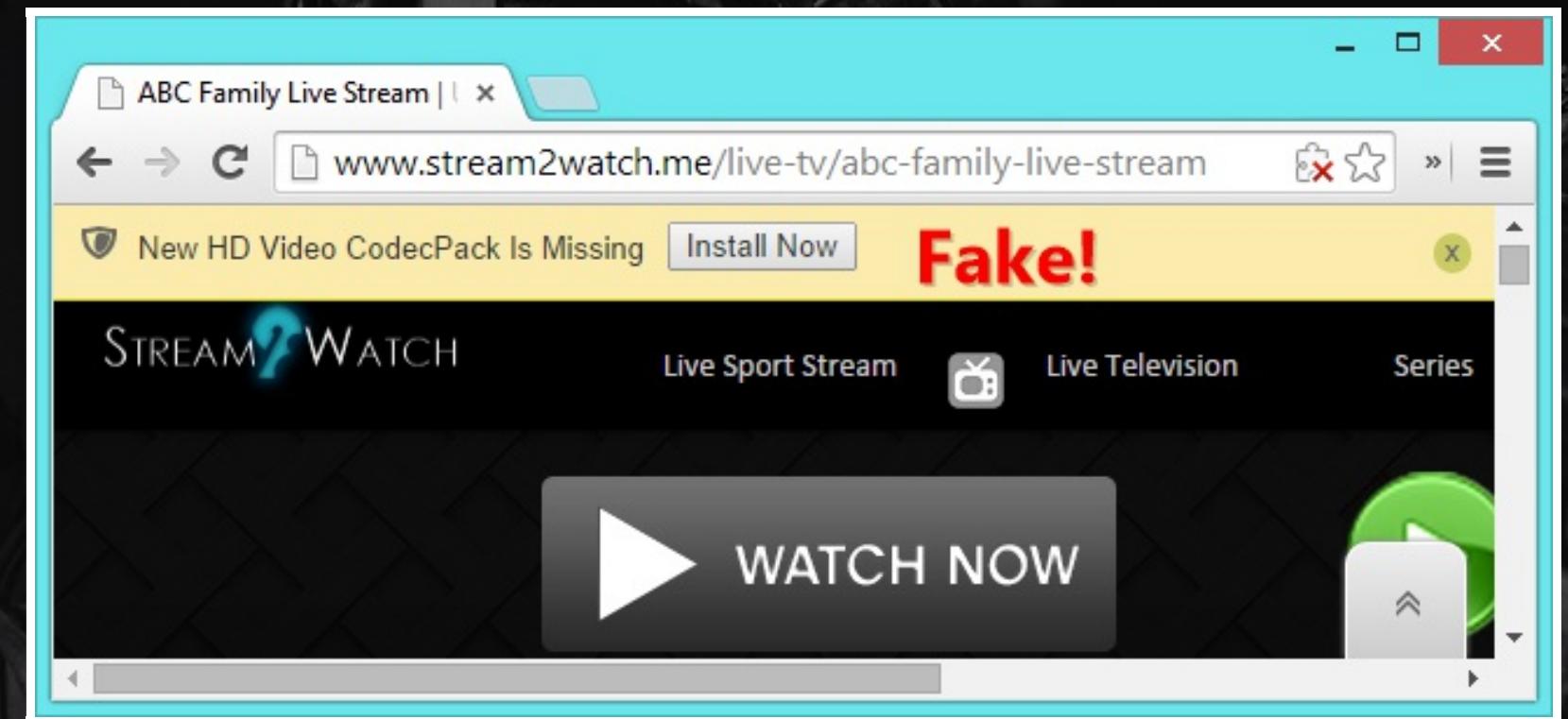
- Suspicious call from a company?
 - Try to call them back on their official support number

CROSS-CHECK SOCIAL MEDIA

- Your Facebook account has been banned, click here to unblock
 - Just go to facebook.com manually and check yourself

BEWARE OF DOWNLOADS

Never accept any plugin, driver, codec, installer you did not explicitly look for





COME ON, I'M TOO SMART FOR
THESE TRAPS!



LET'S MEET ONCE MORE THEN... :)

UPCOMING: ADVANCED PHISHING
TECHNIQUES



ANY QUESTIONS?