# PHISHING TECHNIQUES

## AND HOW TO DEFEND AGAINST THEM

*Morgan Hotonnier*

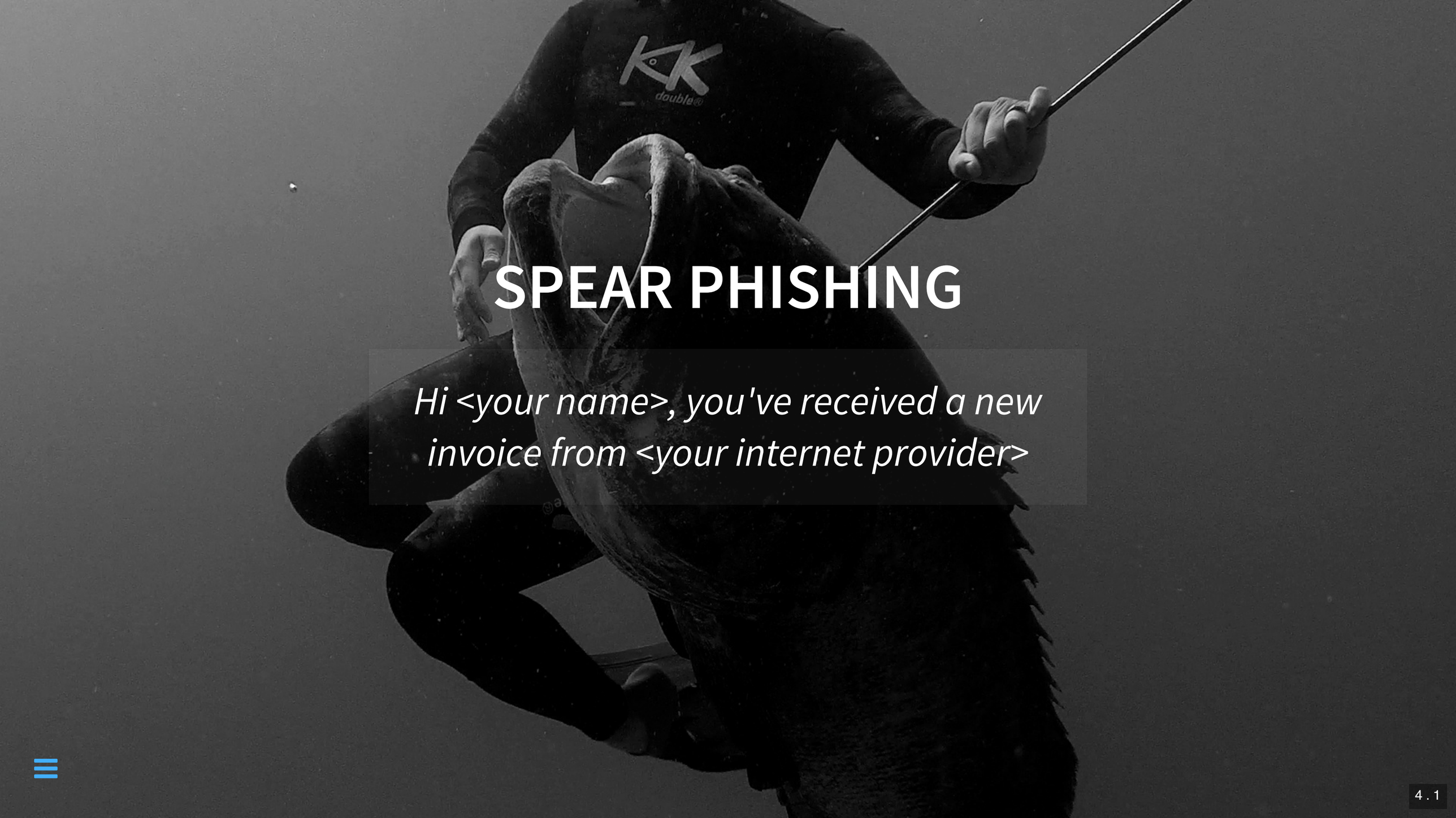
*<f> for fullscreen, <space> for next slide*

# 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**



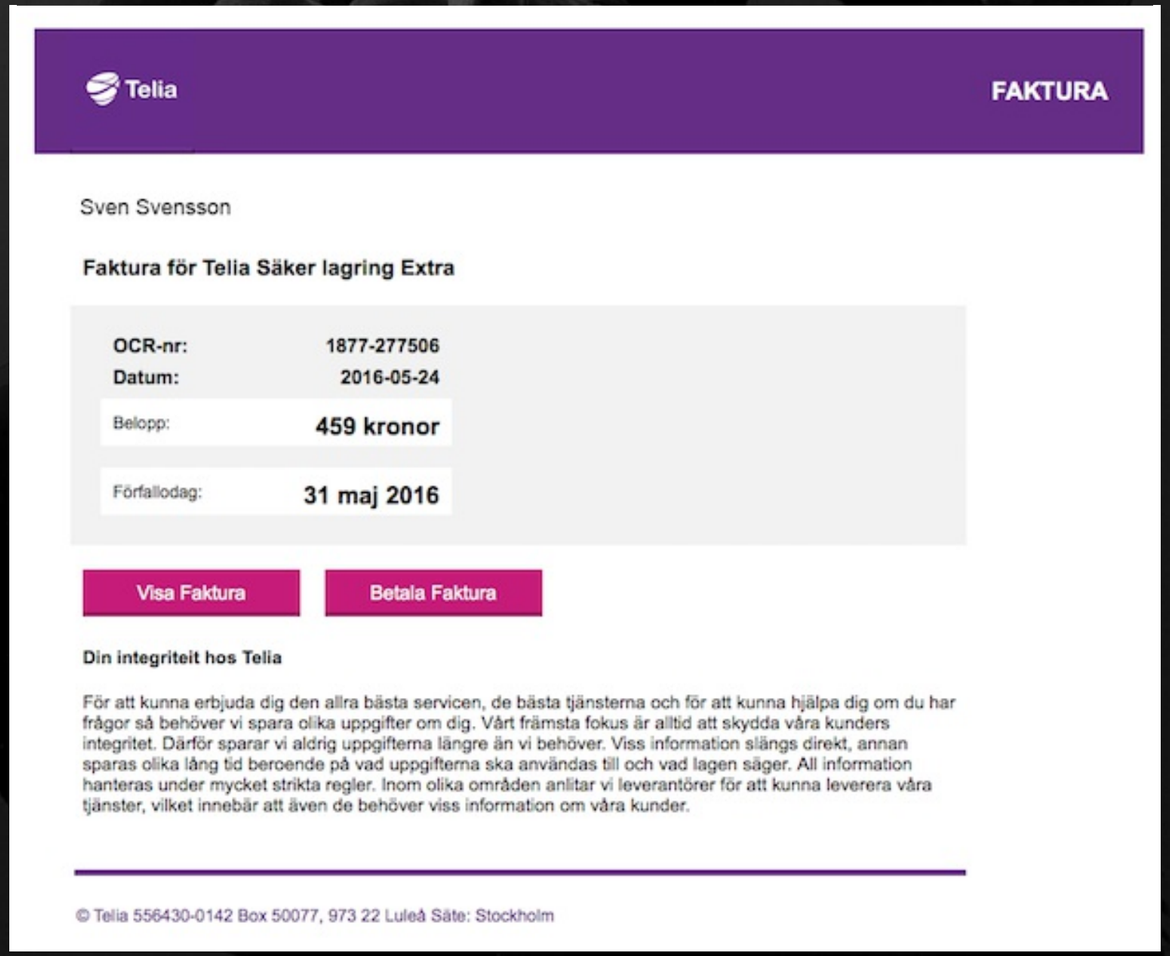
# SPEAR PHISHING

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

# 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**

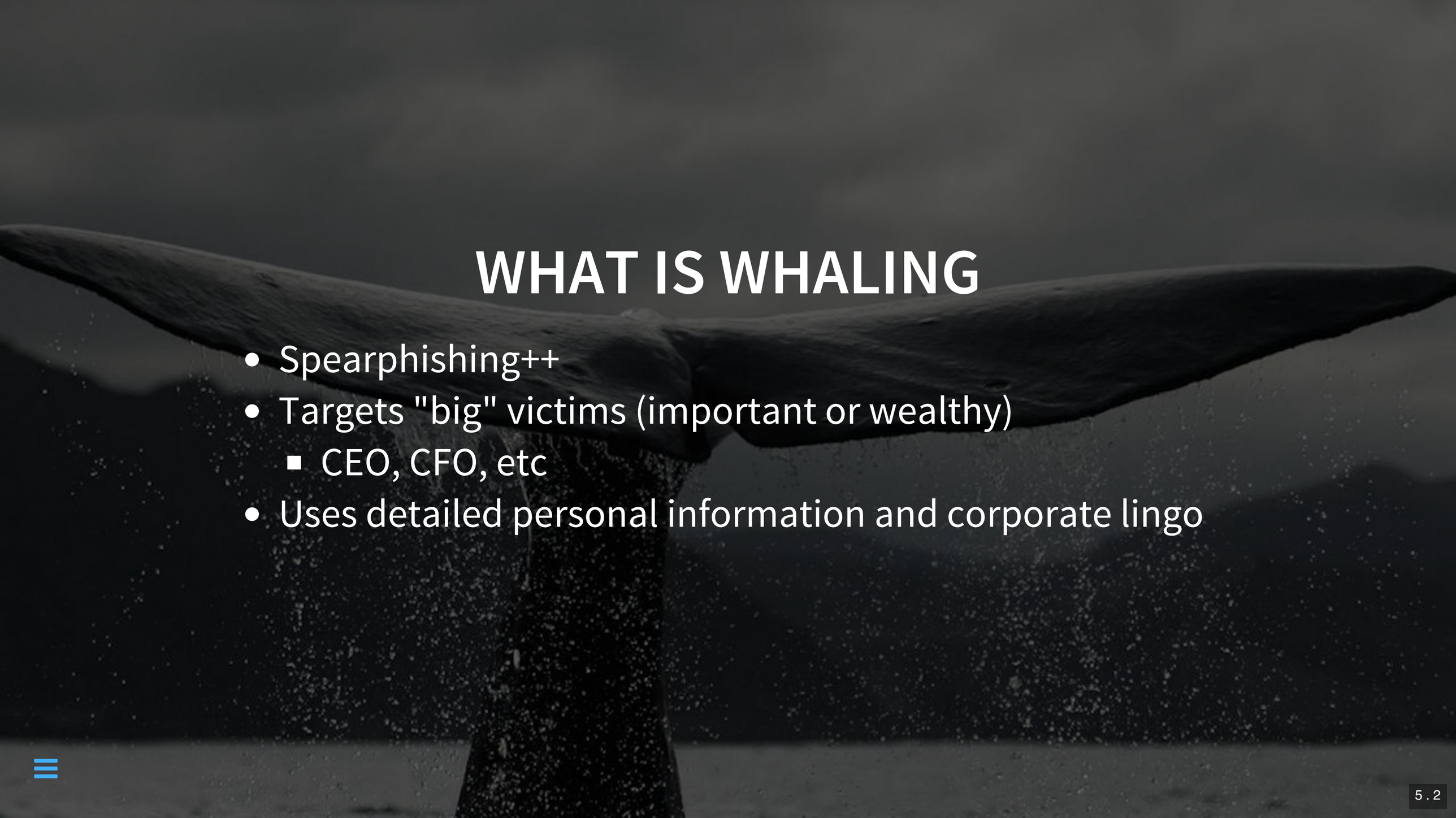
| | |
|---|---|
| **OCR-nr:** | **1877-277506** |
| **Datum:** | **2016-05-24** |
| Belopp: | **459 kronor** |
| Förfallodag: | **31 maj 2016** |

Visa Faktura  Betala Faktura

**Din 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.

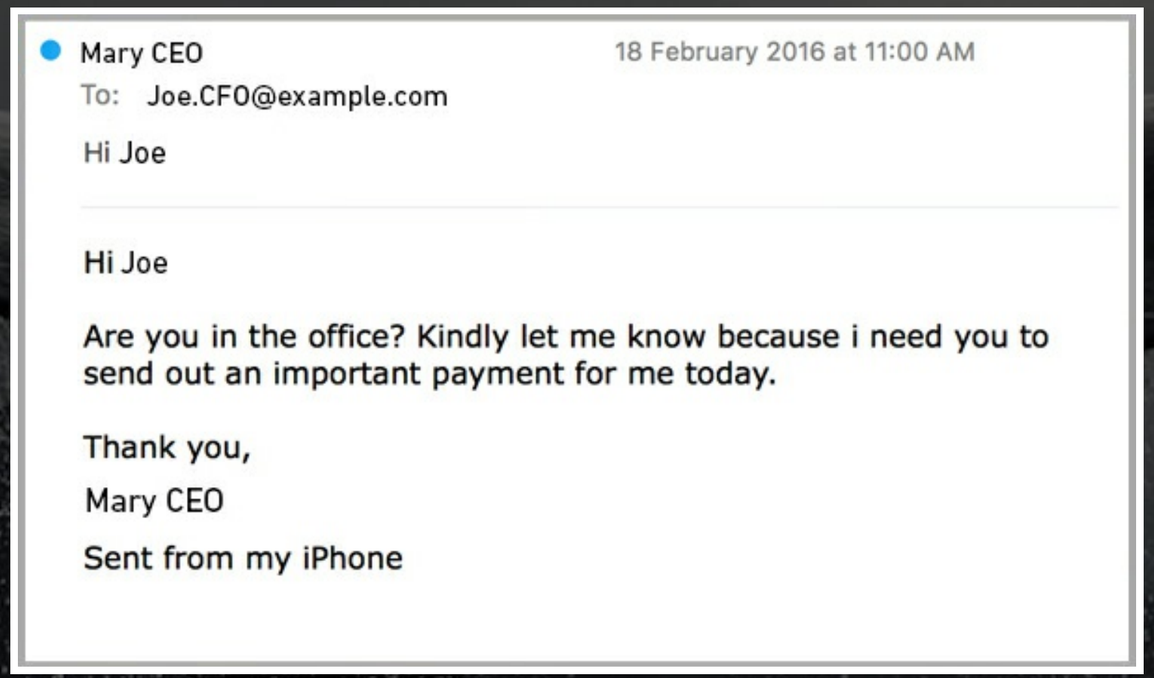

WHALING
Can we send out a wire transfer today?



# WHAT IS WHALING

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

# WHALING EXAMPLE

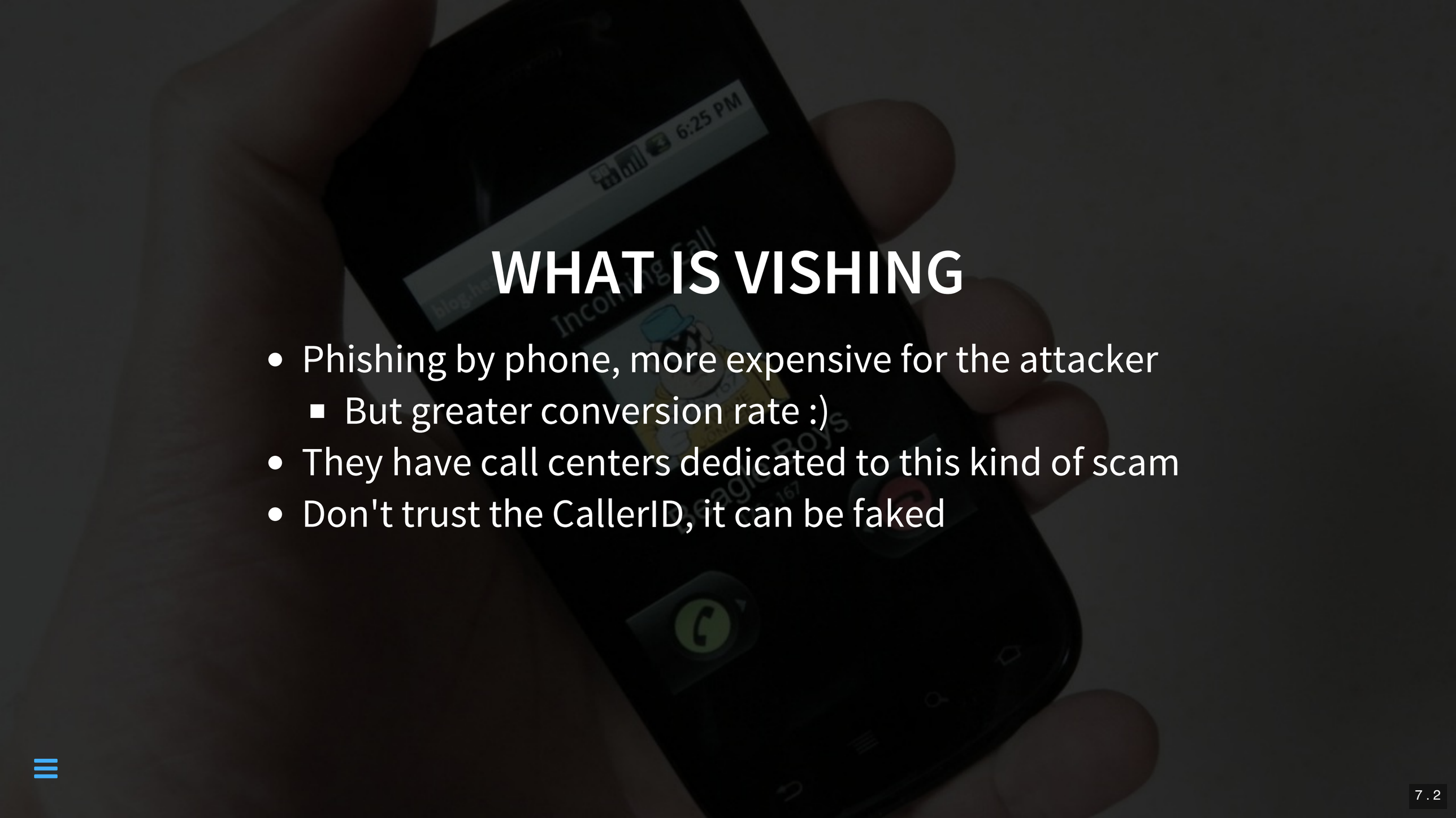


# IT'S NOT JUST ABOUT EMAILS!

- 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
IRS
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


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

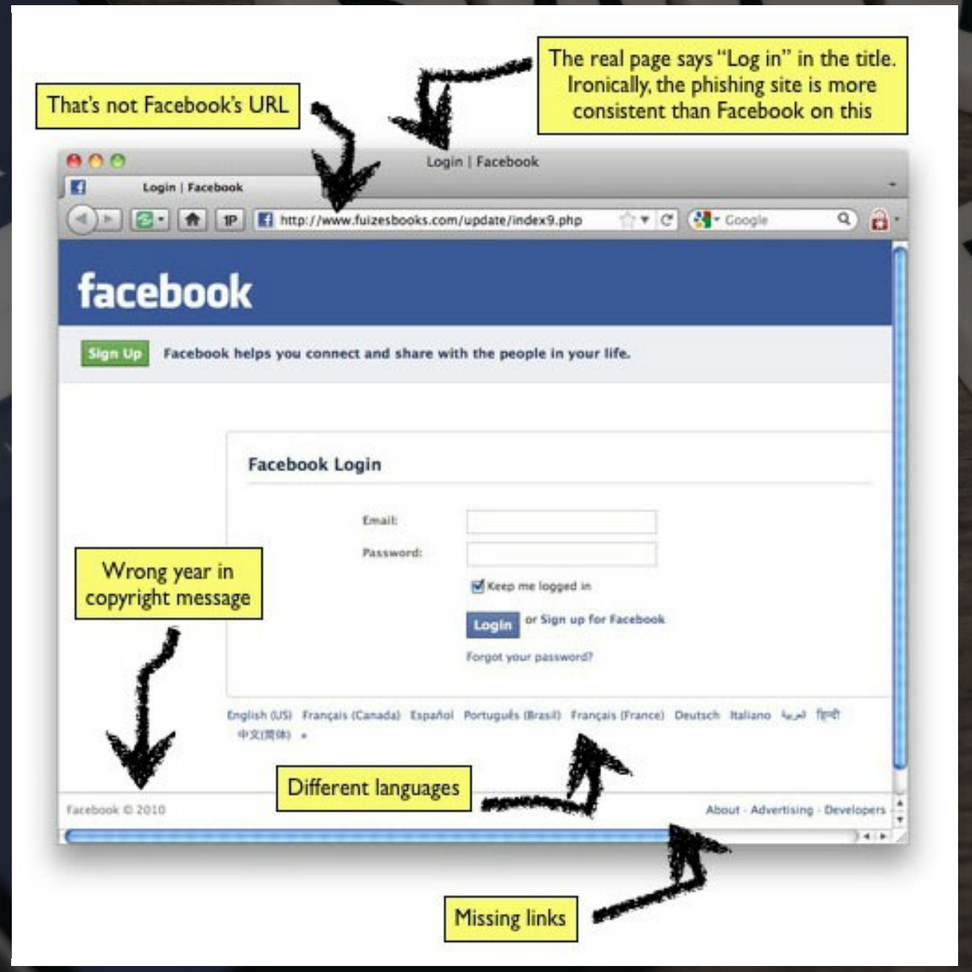
As always, preying on human weaknesses:

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

# Curiosity kills the cat


...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

**Kanthep Kant** https://www.facebook.com/permalink.php?story_fbid=1393558697636379&id=1393558287636420

**Facebook recovery**

Notification: Your Account will be Disabled!

Account FACEBOOK you have already been reported by others about the abuse of account, this is a violation of our agreement and may result in your account is disabled. Please verify your email account to unblock and help us do more for security and convenience for everyone.

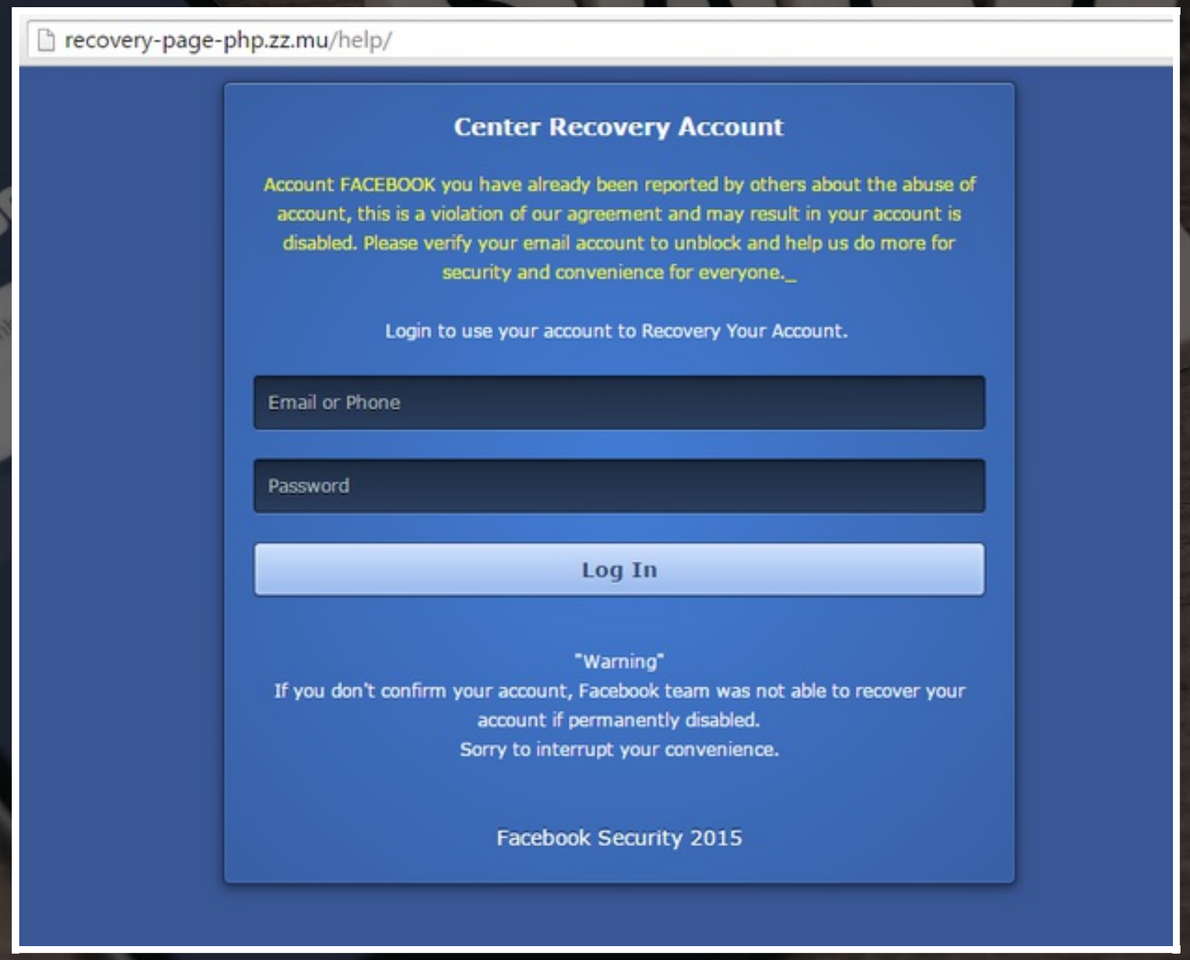
Immediately do recover your Facebook account, by clicking on the link below:
http://j.mp/1HLoHXd?help-facebook-recovery

"Attention"
If you ignore this message, we can not recover your account and your account will be permanently disabled.
Sorry to interrupt your convenience.

The Facebook Team
© Facebook, Inc. 7811 Menlo Park, California, CA, 94043, US

Don't mess with the Facebook police

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



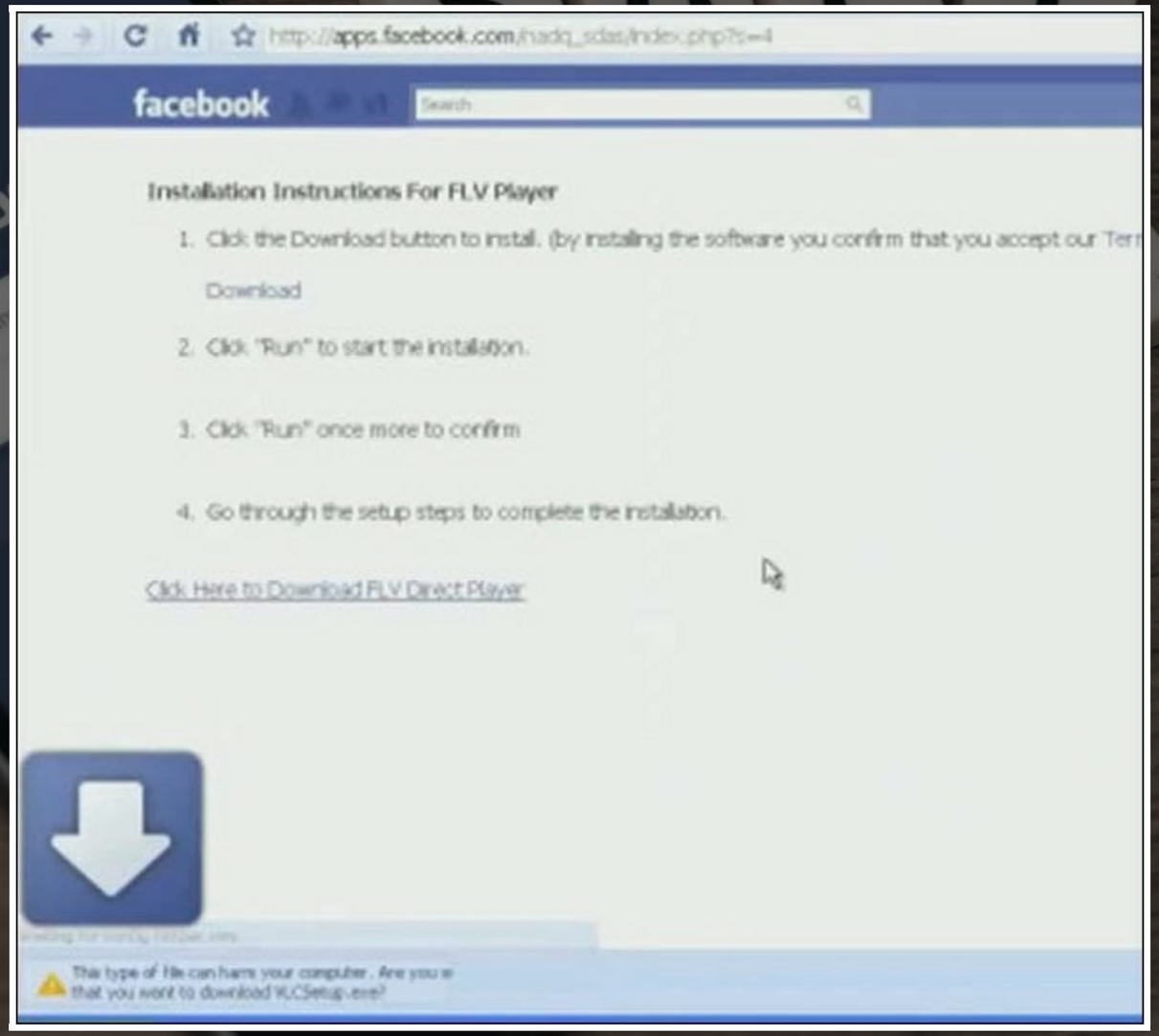
He complied again?!

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

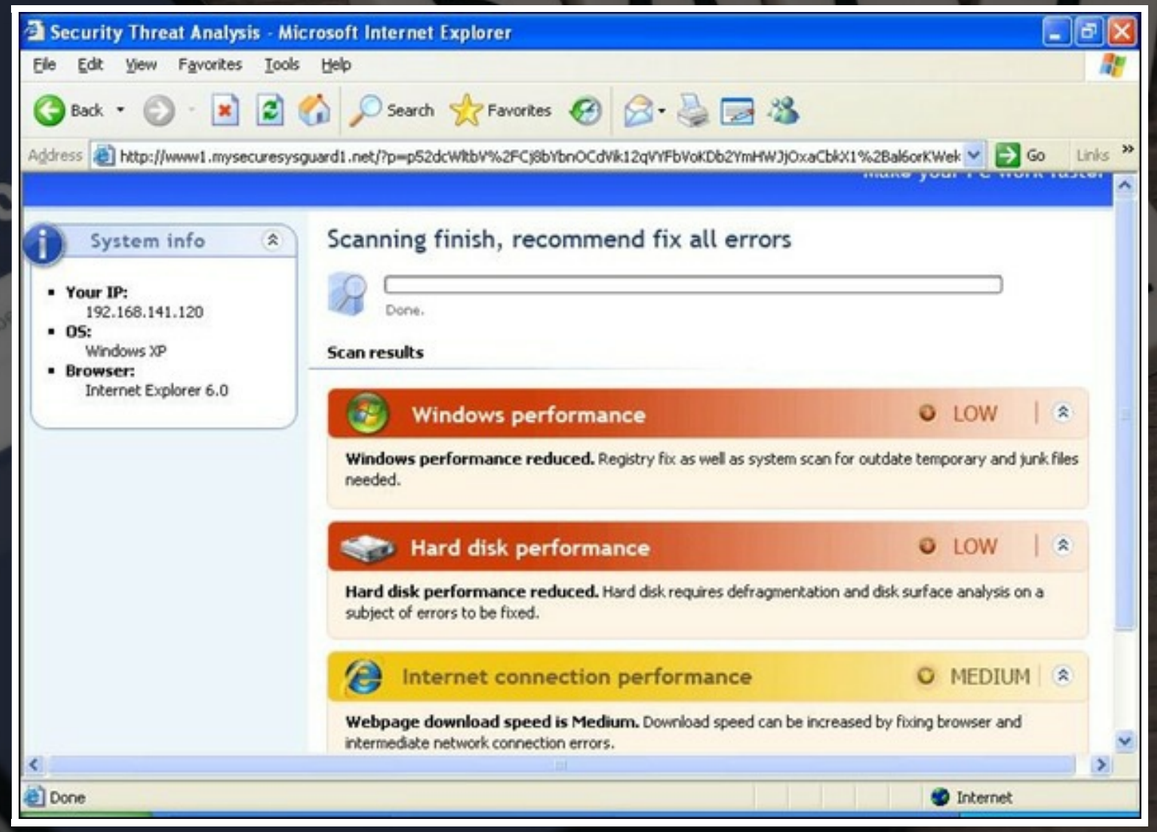
*“Cover up that bosom, which I can't endure to look on.”*

# Again, please give me your password

# Also, please download this totally fake video player plugin



# #IronyAward, you have a virus!

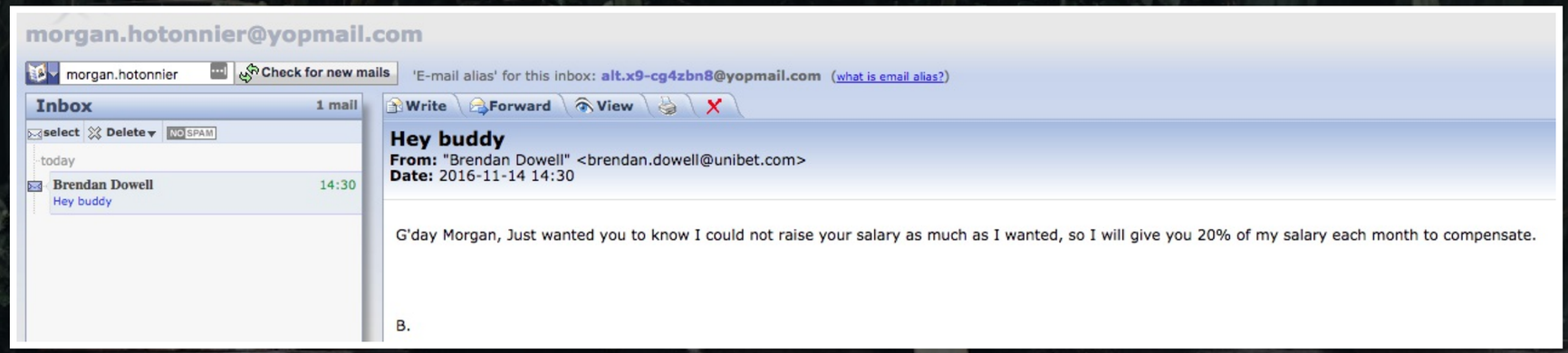



Just pay for my fake antivirus and everything will go away

# SPOOFING

The most common phishing technique

# Spoofing email is doable

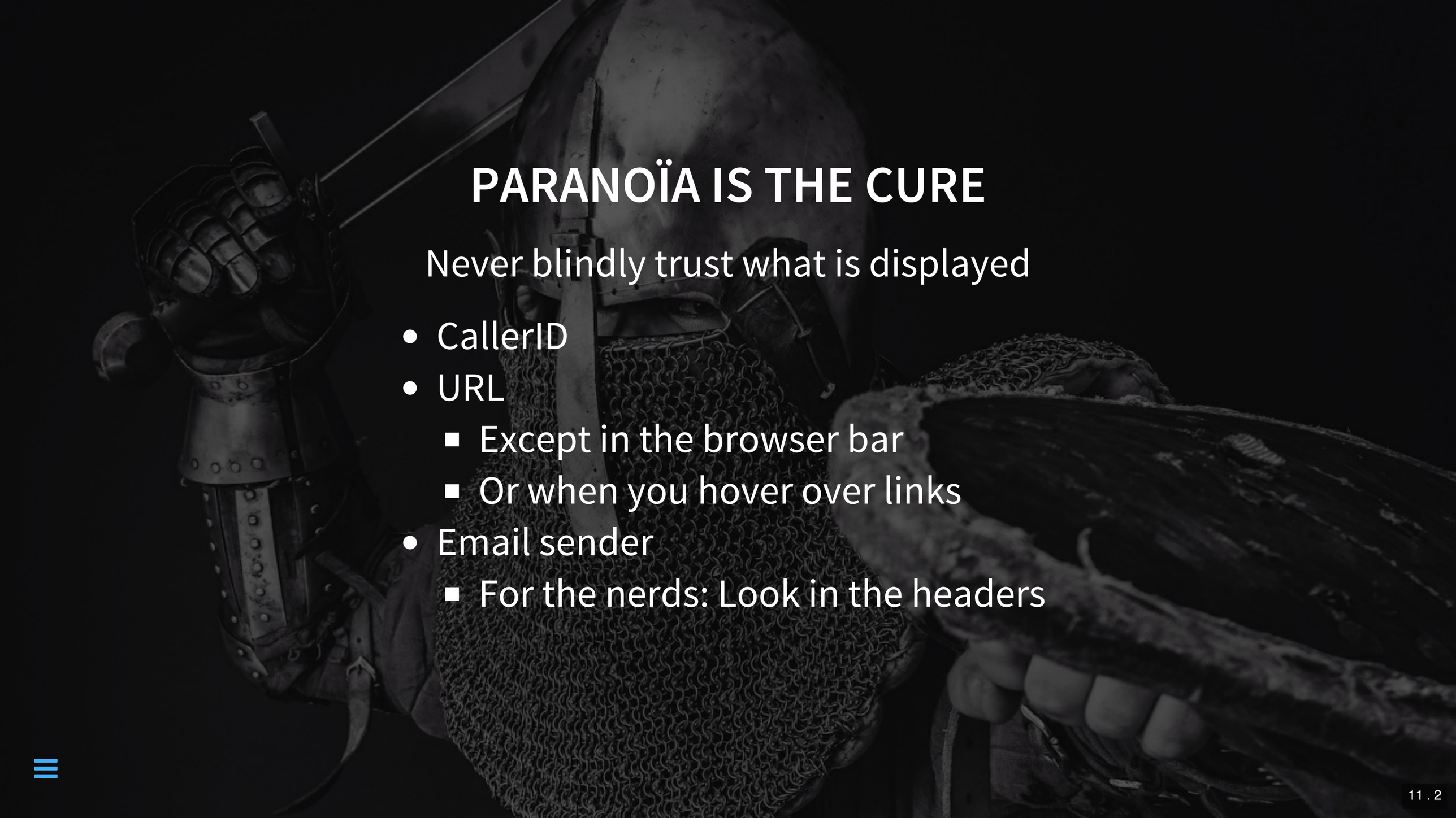


Spoofing link is easy too

*Let's go to google.com*

# SPOOFING CALLERID? EASY PEASY


HOW TO DEFEND YOURSELF?



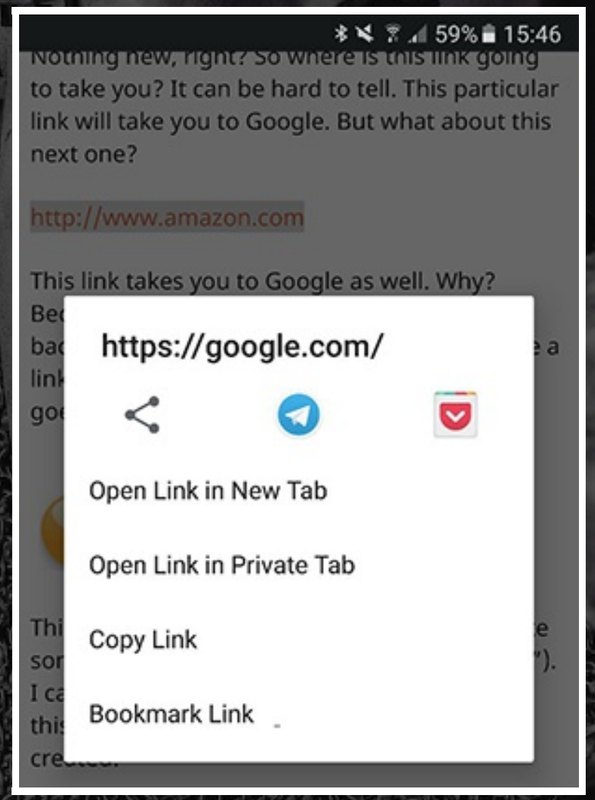
# PARANOÏA IS THE CURE

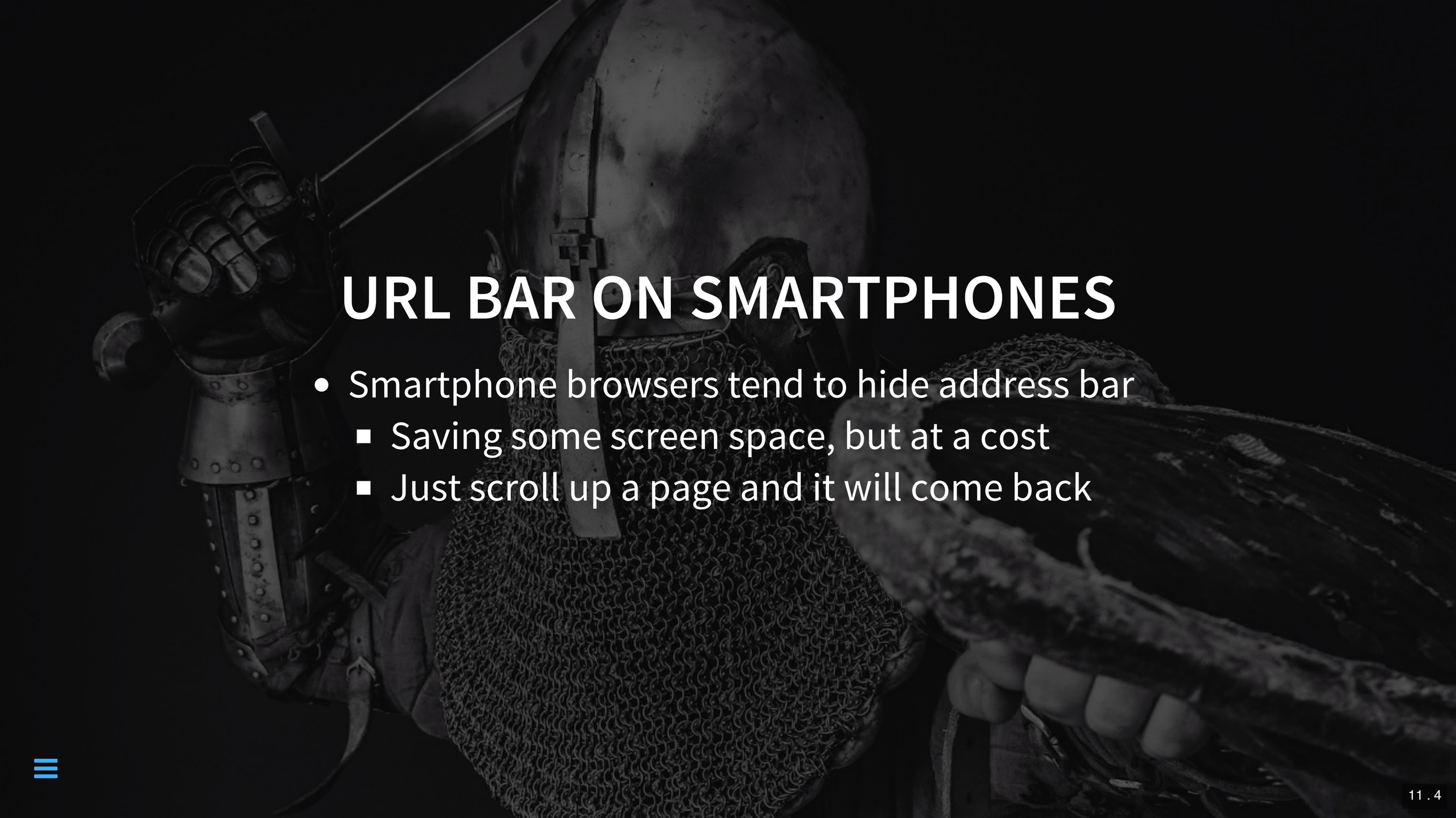
Never blindly trust what is displayed

- 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

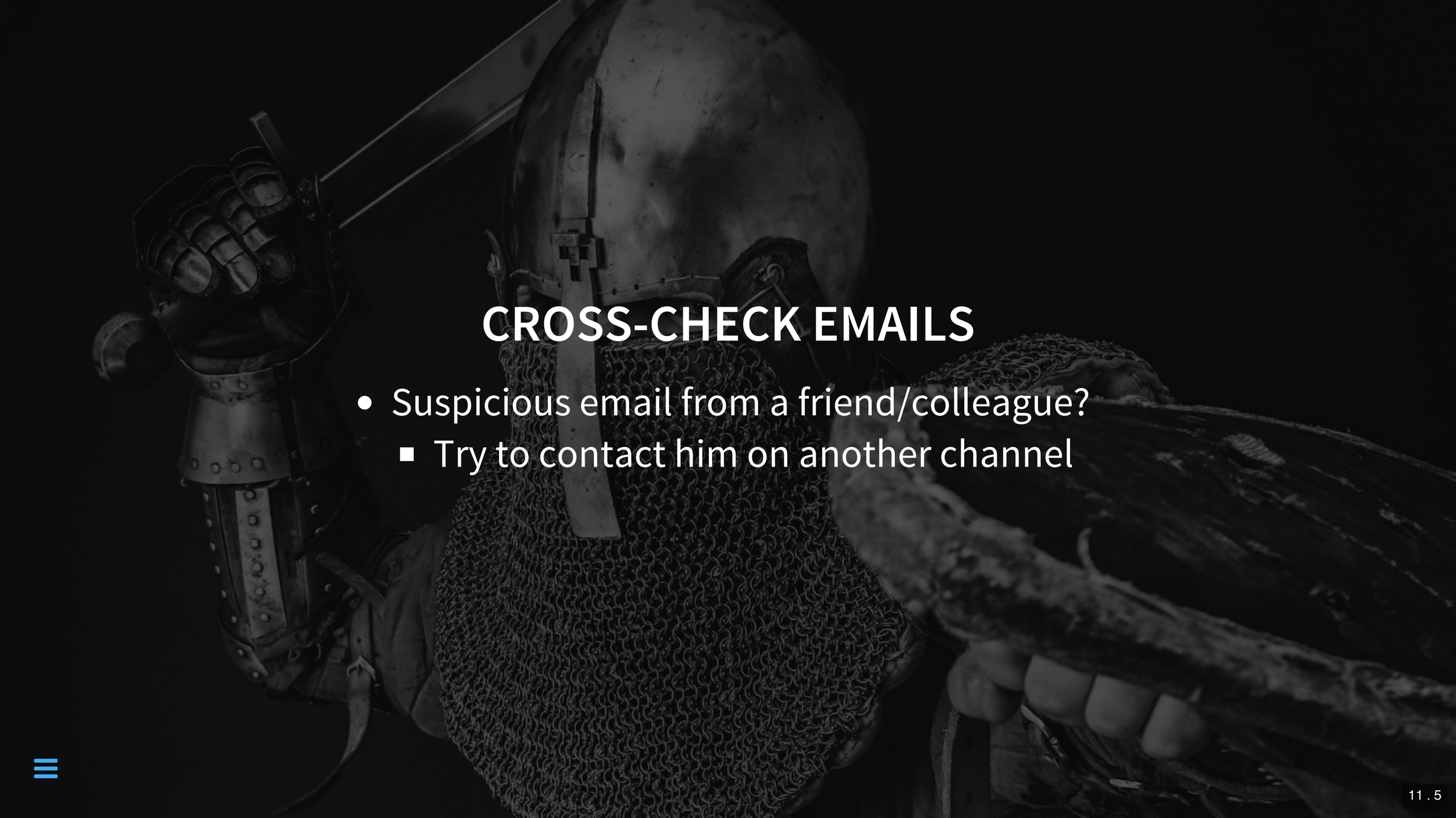
- Long press on links to show the real destination





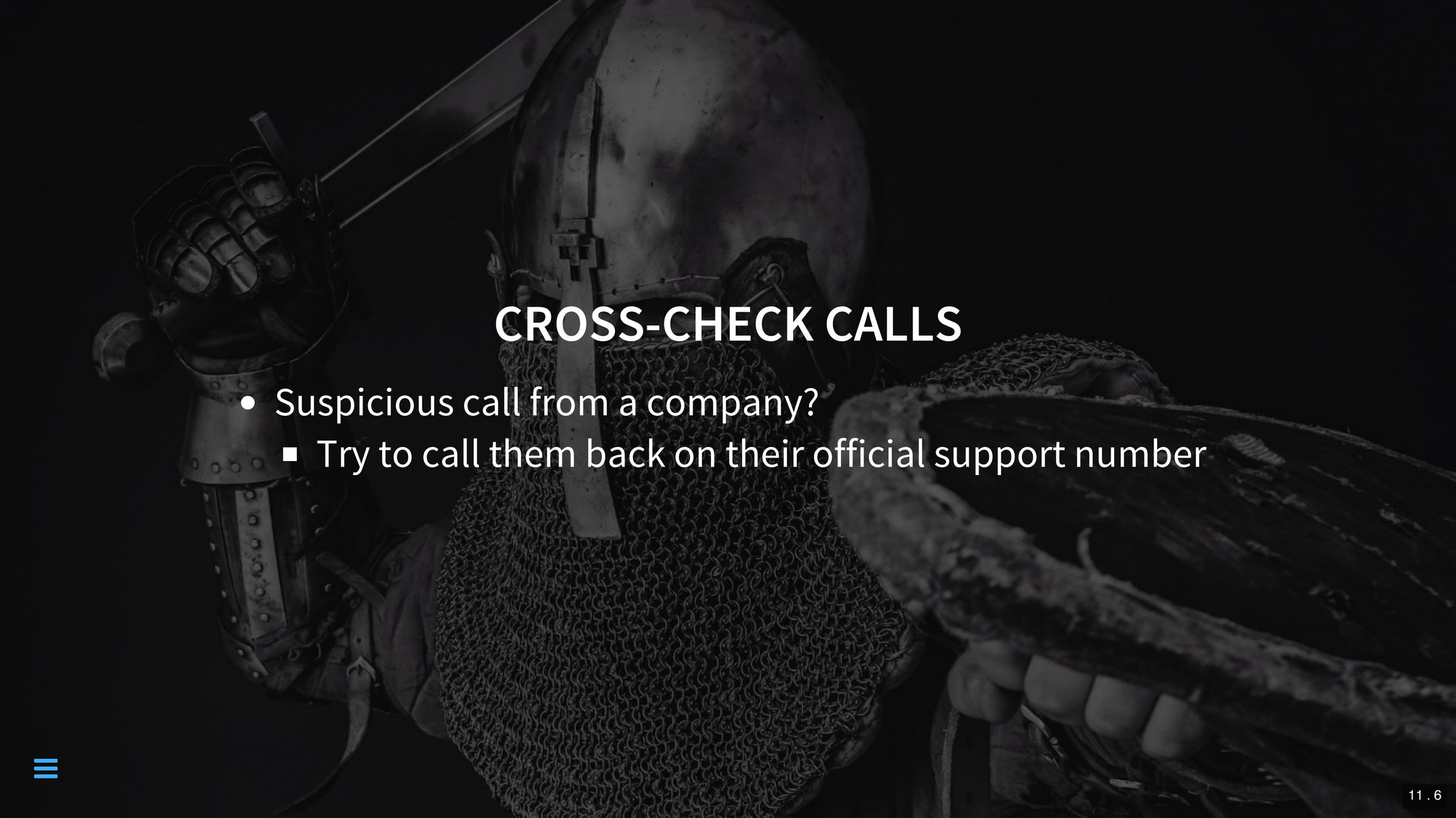
# URL BAR ON SMARTPHONES

- 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



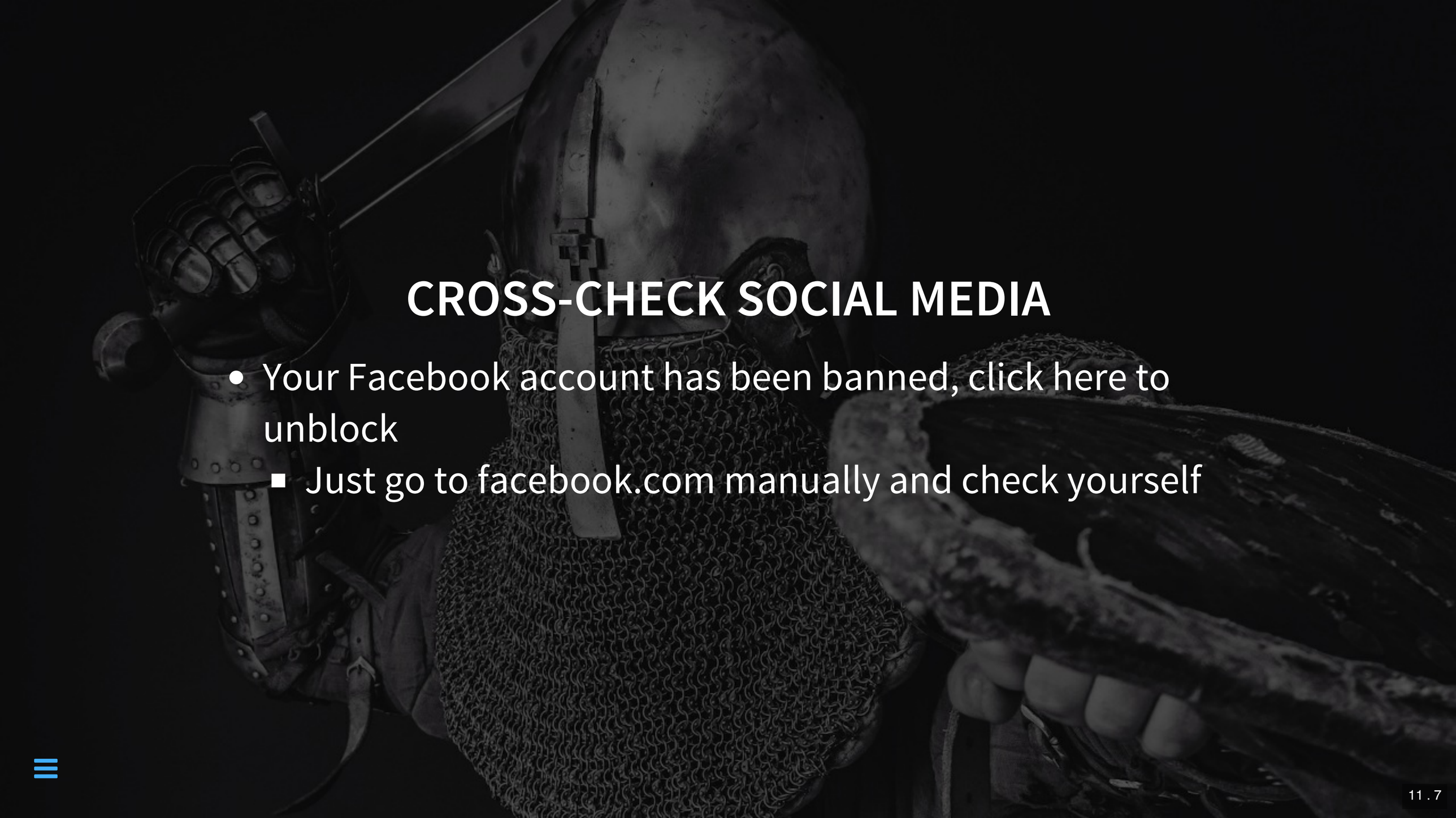
# CROSS-CHECK EMAILS

- 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

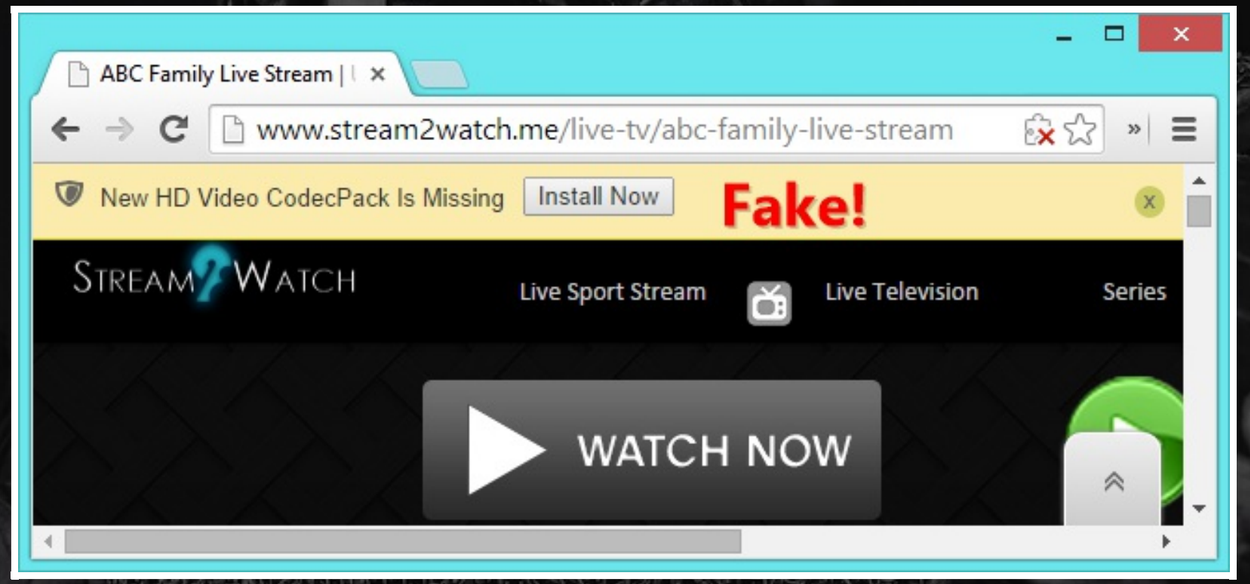


# CROSS-CHECK SOCIAL MEDIA

- 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 explicitely look for




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

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

## UPCOMING: ADVANCED PHISHING TECHNIQUES


ANY QUESTIONS?