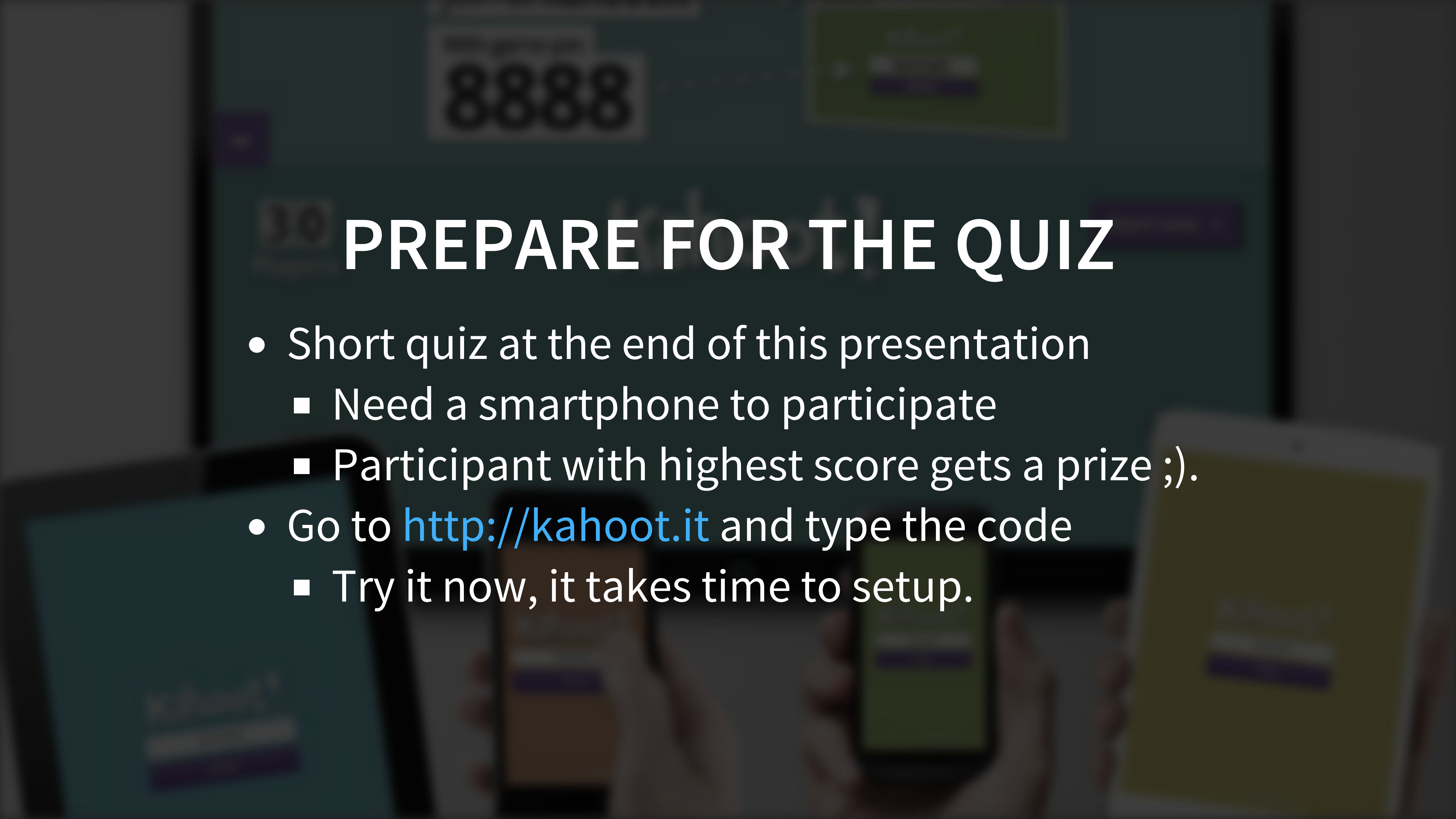
5 THINGS YOU THOUGHT YOU KNEW ABOUT PHISHING

SECURITY BOOST #01

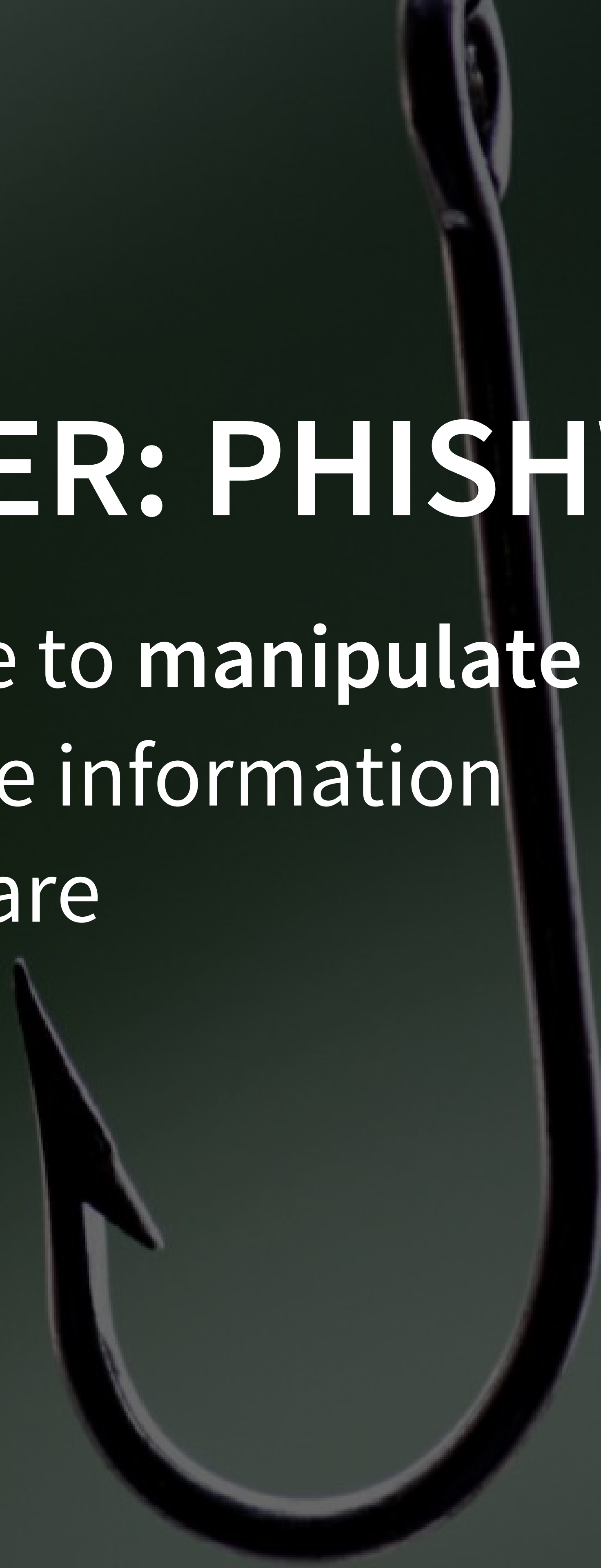
Morgan Hotonnier - Group Security

QUIZ INCOMING!



PREPARE FOR THE QUIZ

- Short quiz at the end of this presentation
  - Need a smartphone to participate
  - Participant with highest score gets a prize ;).
- Go to http://kahoot.it and type the code
  - Try it now, it takes time to setup.



BASIC REMINDER: PHISHWHAT?

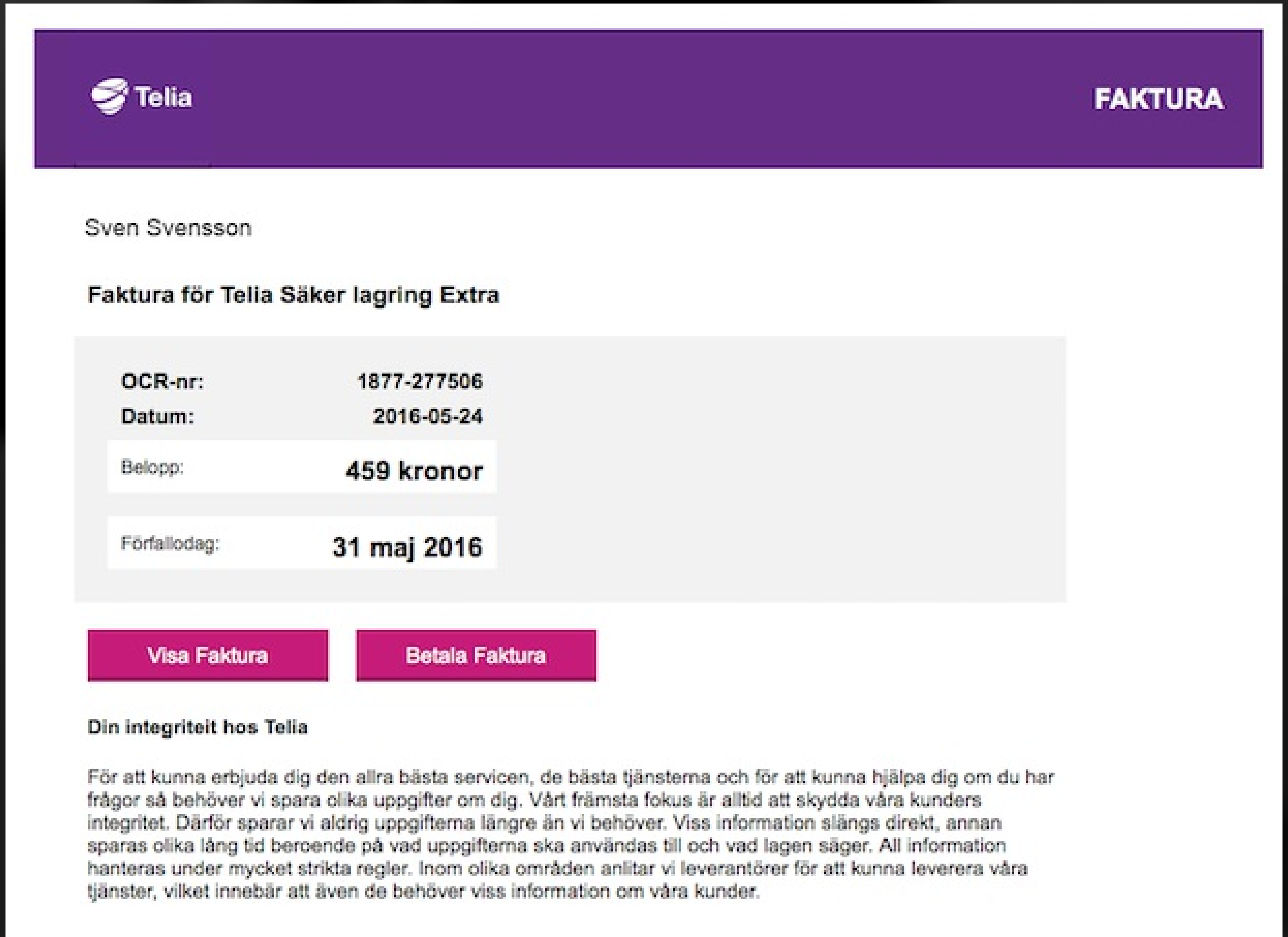
- Phishing: Technique to **manipulate** you into
  - revealing sensitive information
  - installing a malware
  - sending money
  - all of the above

PHISHING "LEVELS"

- Classic (generic)
- **Spear phishing**
- **Whaling**

SPEAR PHISHING

- Tailored to specific individuals or groups
- Uses details from social medias, previous hacks...



Sven Svensson

Faktura för Telia Säker lagring Extra

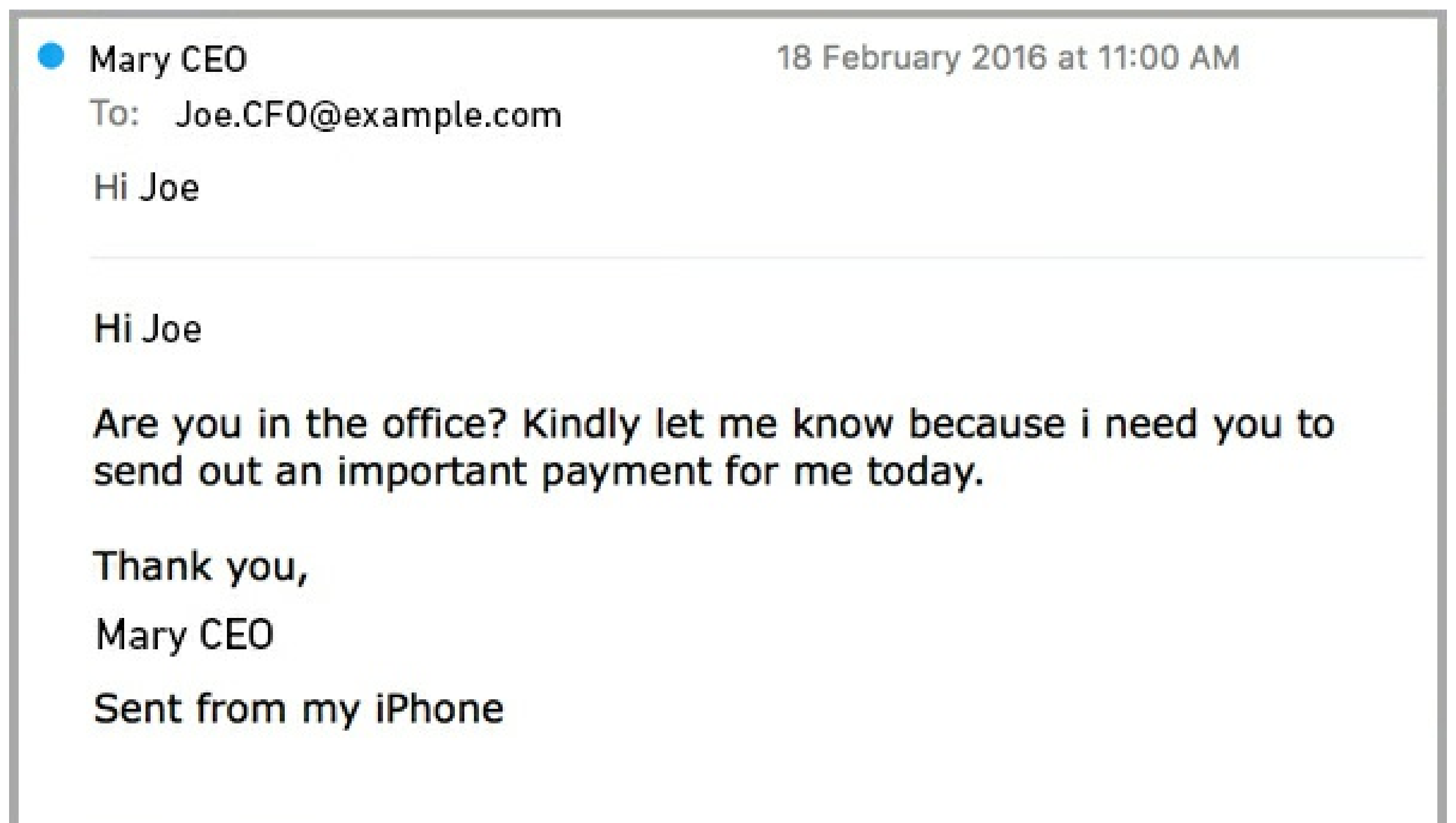
OCR-nr:	1877-277506
Datum:	2016-05-24
Belopp:	459 kronor
Förfallodag:	31 maj 2016

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

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



Mary CEO 18 February 2016 at 11:00 AM

To: Joe.CFO@example.com

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,

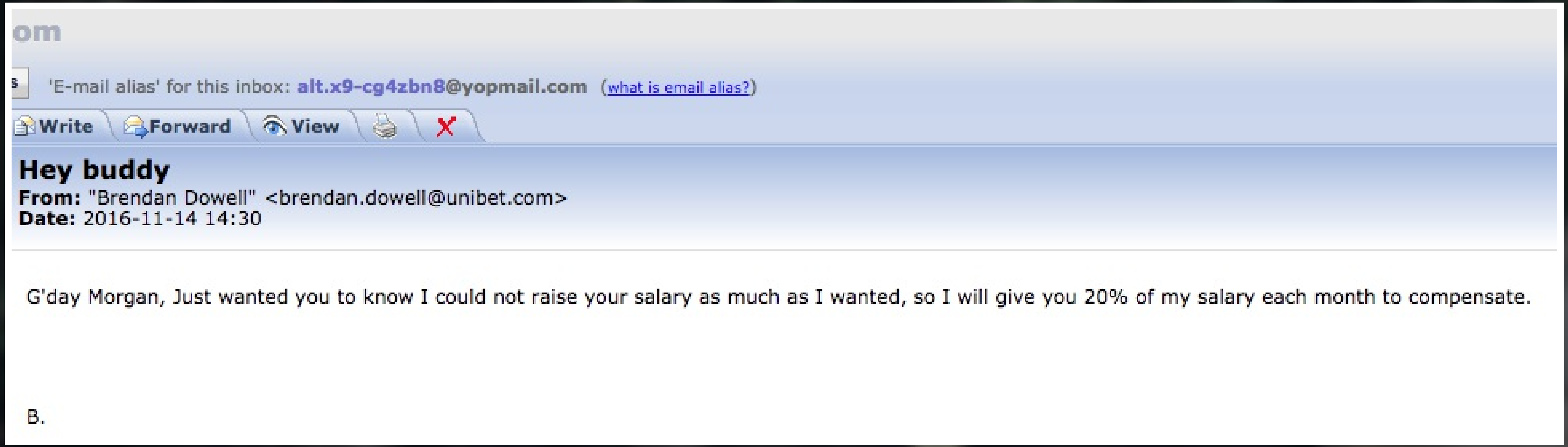
Mary CEO

Sent from my iPhone

TOP FALSE ASSUMPTIONS

1. THE EMAIL SENDER IS THE RIGHT ONE, I'M SAFE!

Spoofing email is doable



'E-mail alias' for this inbox: **alt.x9-cg4zbn8@yopmail.com** (what is email alias?)

Hey buddy
From: "Brendan Dowell" <brendan.dowell@unibet.com>
Date: 2016-11-14 14:30

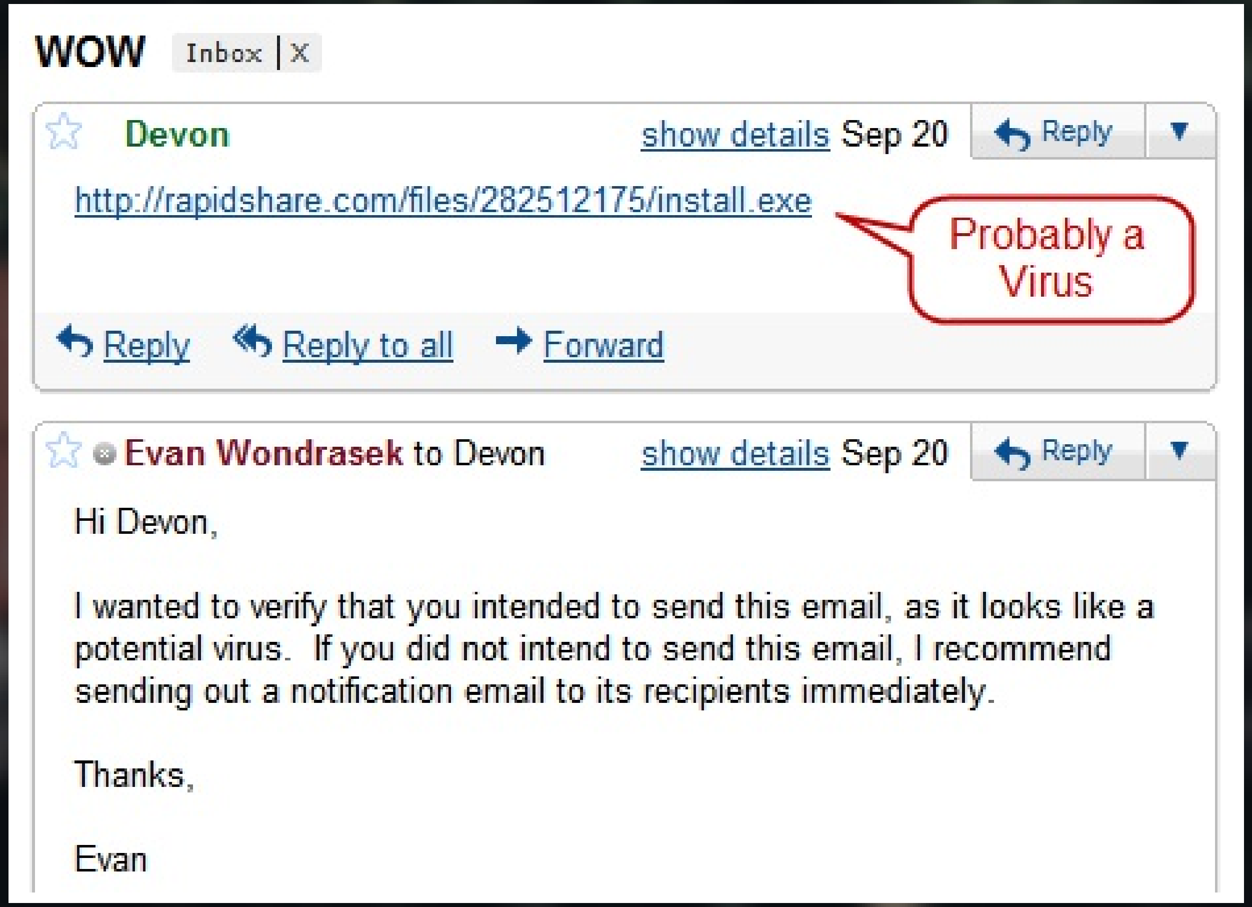
G'day Morgan, Just wanted you to know I could not raise your salary as much as I wanted, so I will give you 20% of my salary each month to compensate.

B.

Anti-spam solutions usually catch it...usually.

EMAIL HIJACK

If your friend got hacked



WOW

Devon — show details Sep 20

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

Evan Wondrasek to Devon — show details Sep 20

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

attacker doesn't even need to spoof anything

WHEN IN DOUBT, CROSS-CHECK

- Preferably on another channel
  - Ex: doubt on an email sent by a friend? Ask them by chat/phone

2. PHISHING IS ONLY DONE OVER EMAIL!

IT'S NOT JUST ABOUT EMAILS!

- Vishing
- Smishing
- Social media

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

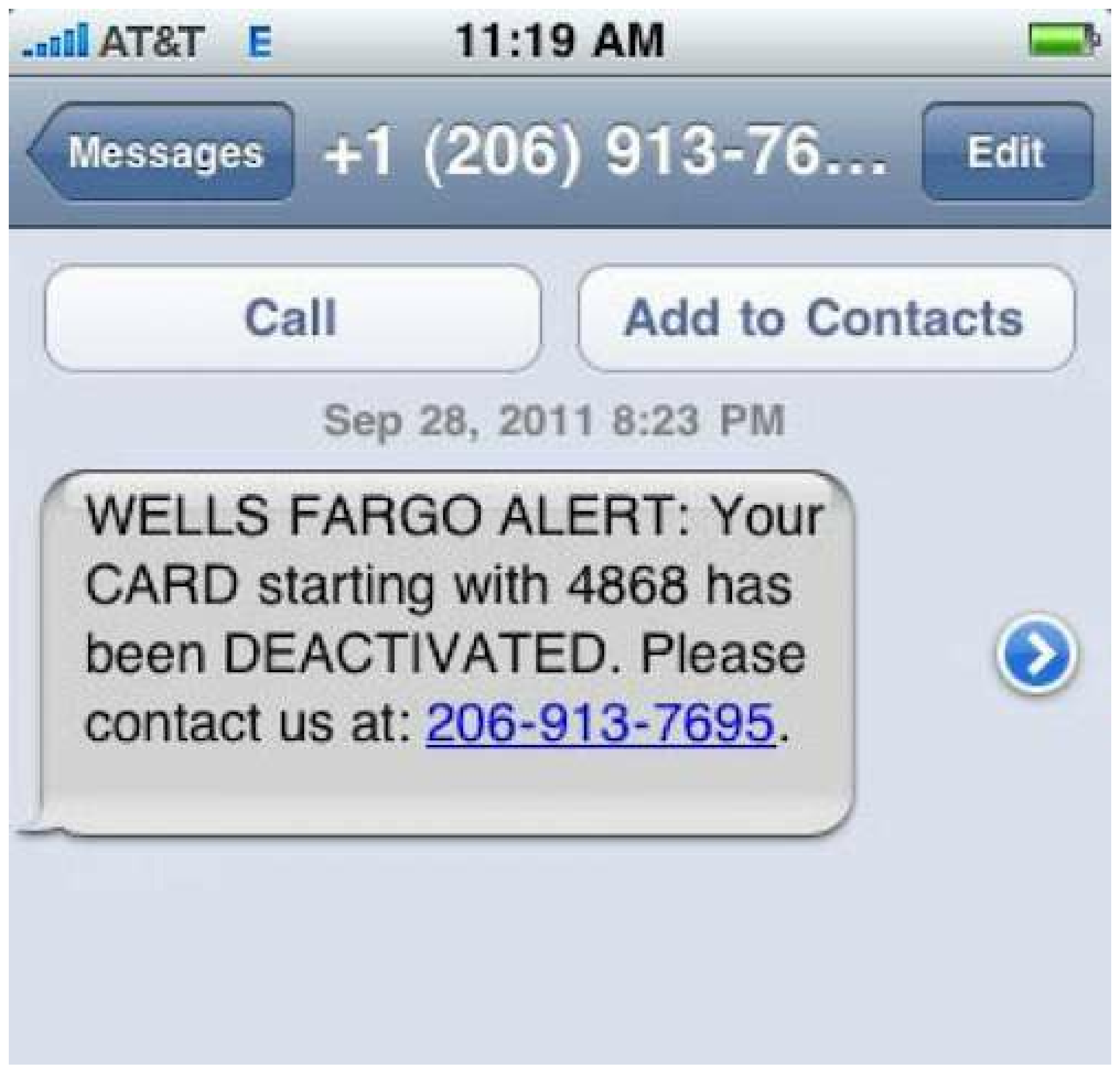
Vishers are posing as **IRS Agents**

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

IRS reports from January 2016 show that since October 2013:

SMISHING

- Phishing over SMS

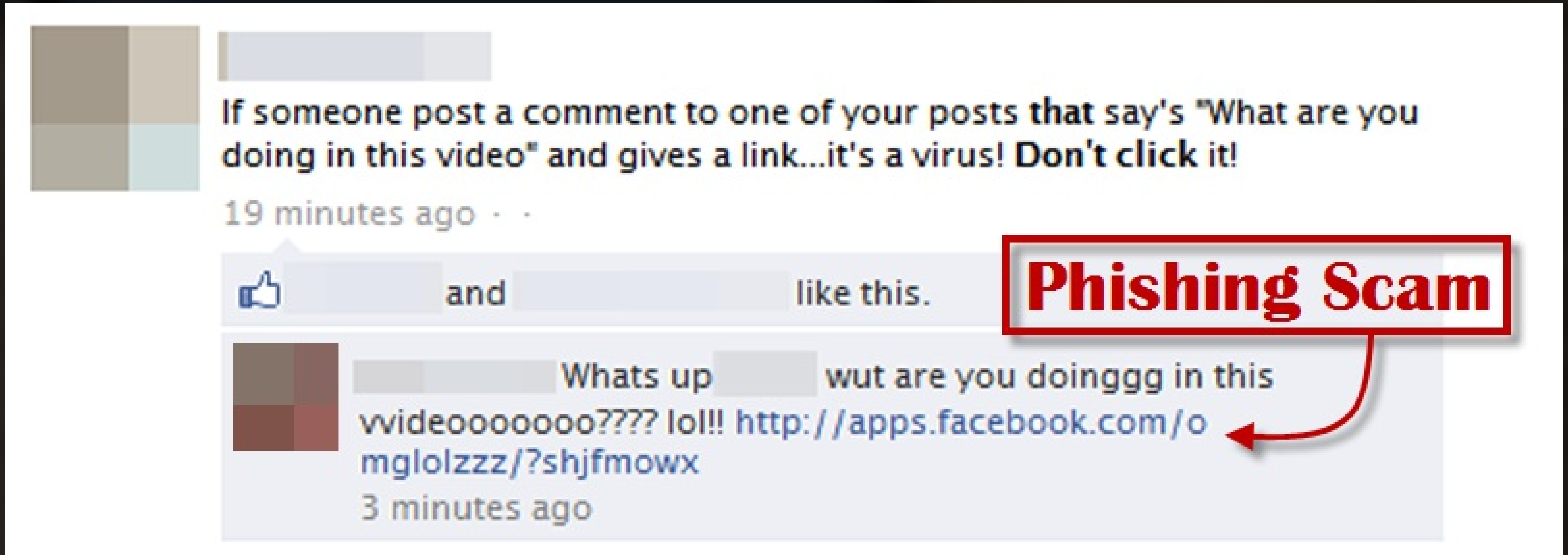


Sep 28, 2011 8:23 PM

WELLS FARGO ALERT: Your CARD starting with 4868 has been DEACTIVATED. Please contact us at: 206-913-7695.

SOCIAL NETWORK PHISHING

- Masquerading as the social Network
- Use "infected" friends to make you click on malicious links
- Catphishing to lure you into giving out personal details



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.

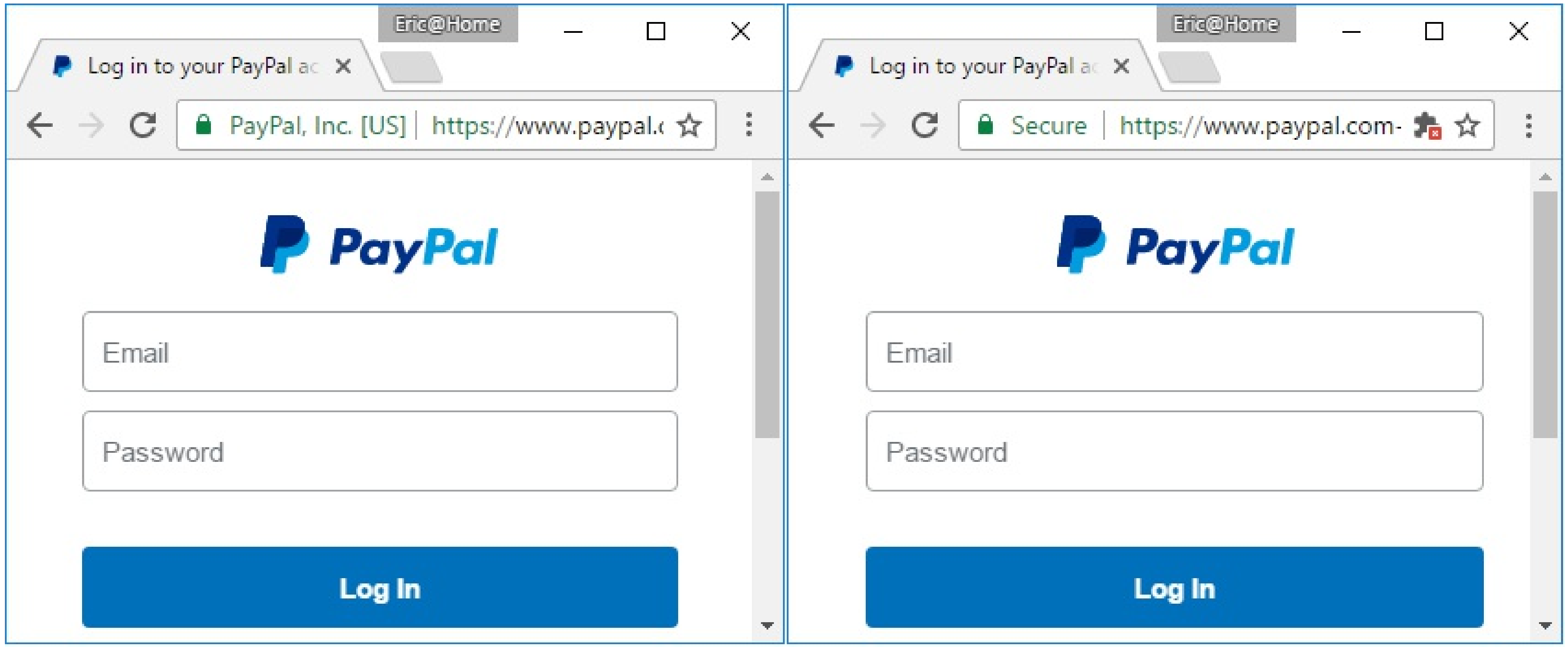
Whats up wut are you doinggg in this vvideoooooooo???? lol!! http://apps.facebook.com/omglolzzz/?shjfmowx

3 minutes ago

3. THE WEBSITE HAS THE GREEN PADLOCK, I'M SAFE!

THE GREEN PADLOCK

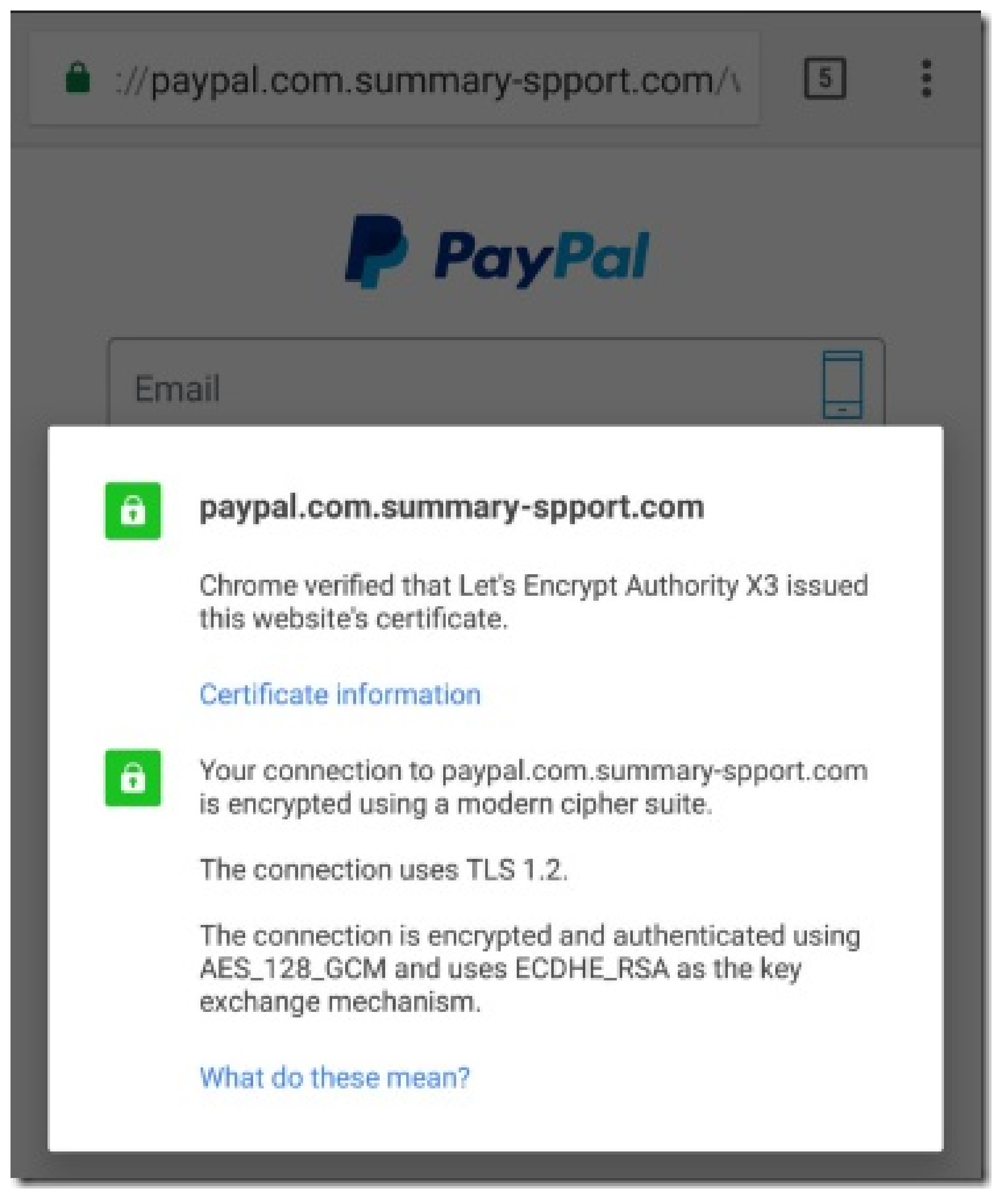
What do you think of those websites?



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

THE GREEN PADLOCK

...woops



paypal.com.summary-spport.com

Chrome verified that Let's Encrypt Authority X3 issued this website's certificate.

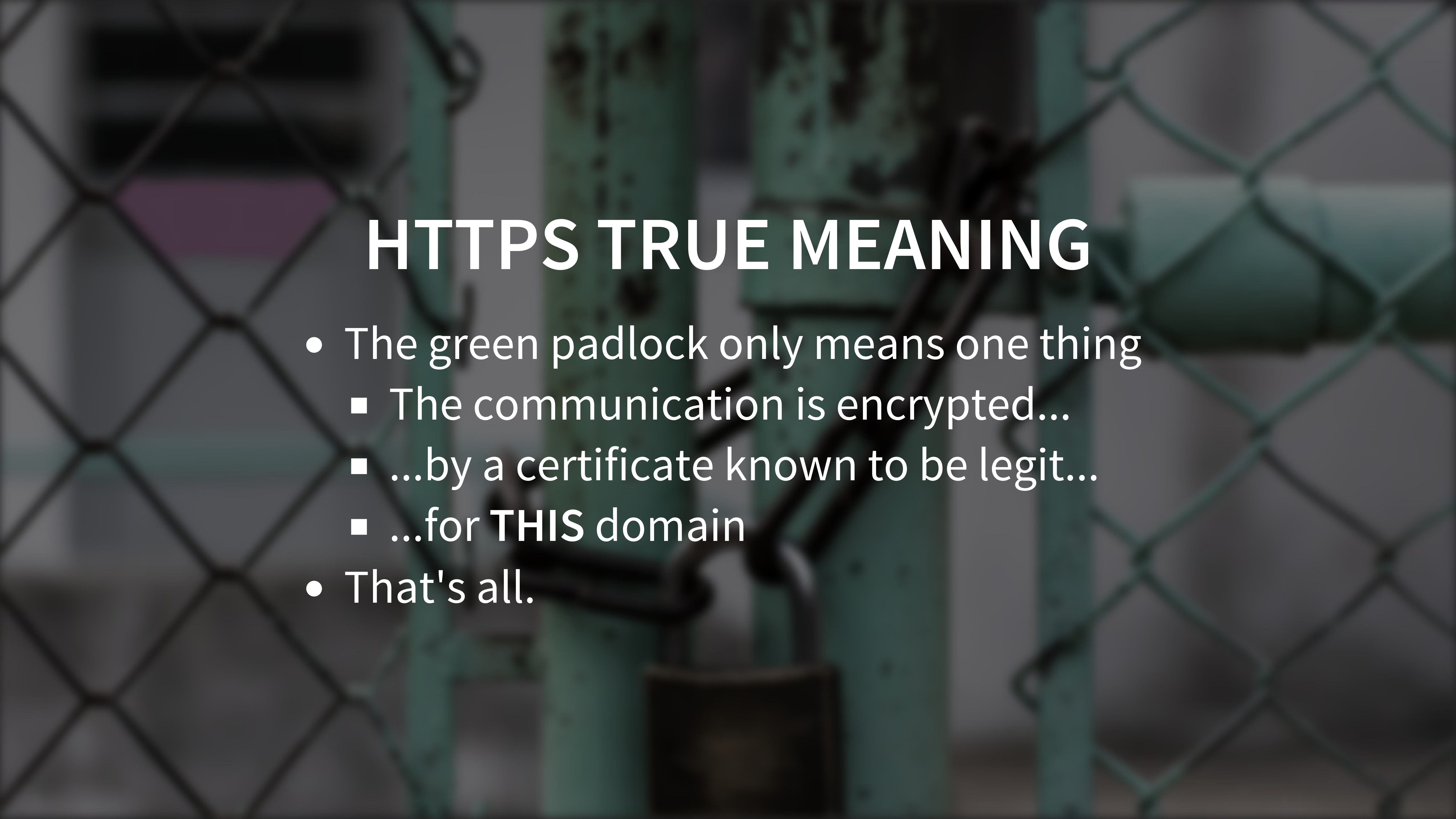
Certificate information

Your connection to paypal.com.summary-spport.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

What do these mean?



HTTPS TRUE MEANING

- The green padlock only means one thing
  - The communication is encrypted...
  - ...by a certificate known to be legit...
  - ...for **THIS** domain
- That's all.

4. IF THE ADDRESS IS THE RIGHT ONE, THEN I'M SAFE!

TYPOSQUATTING

Please visit rnicrosoft.com for more details

Sorry, I meant mircosoft.com

Damn! I meant micrpsoft.com

HOMOGRAPHS

Wikipedia != Wikipedia

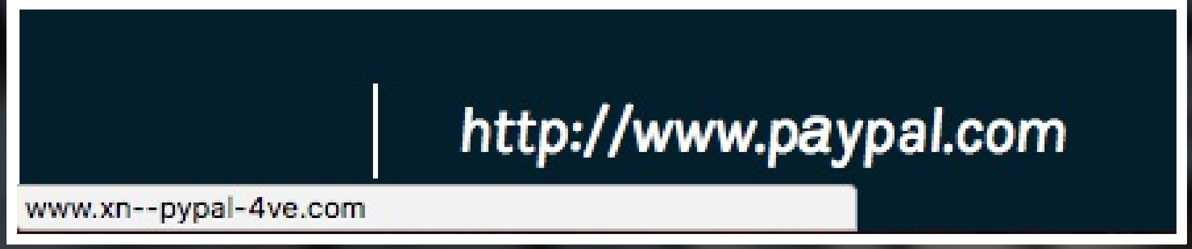
HOMOGRAPHS

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/



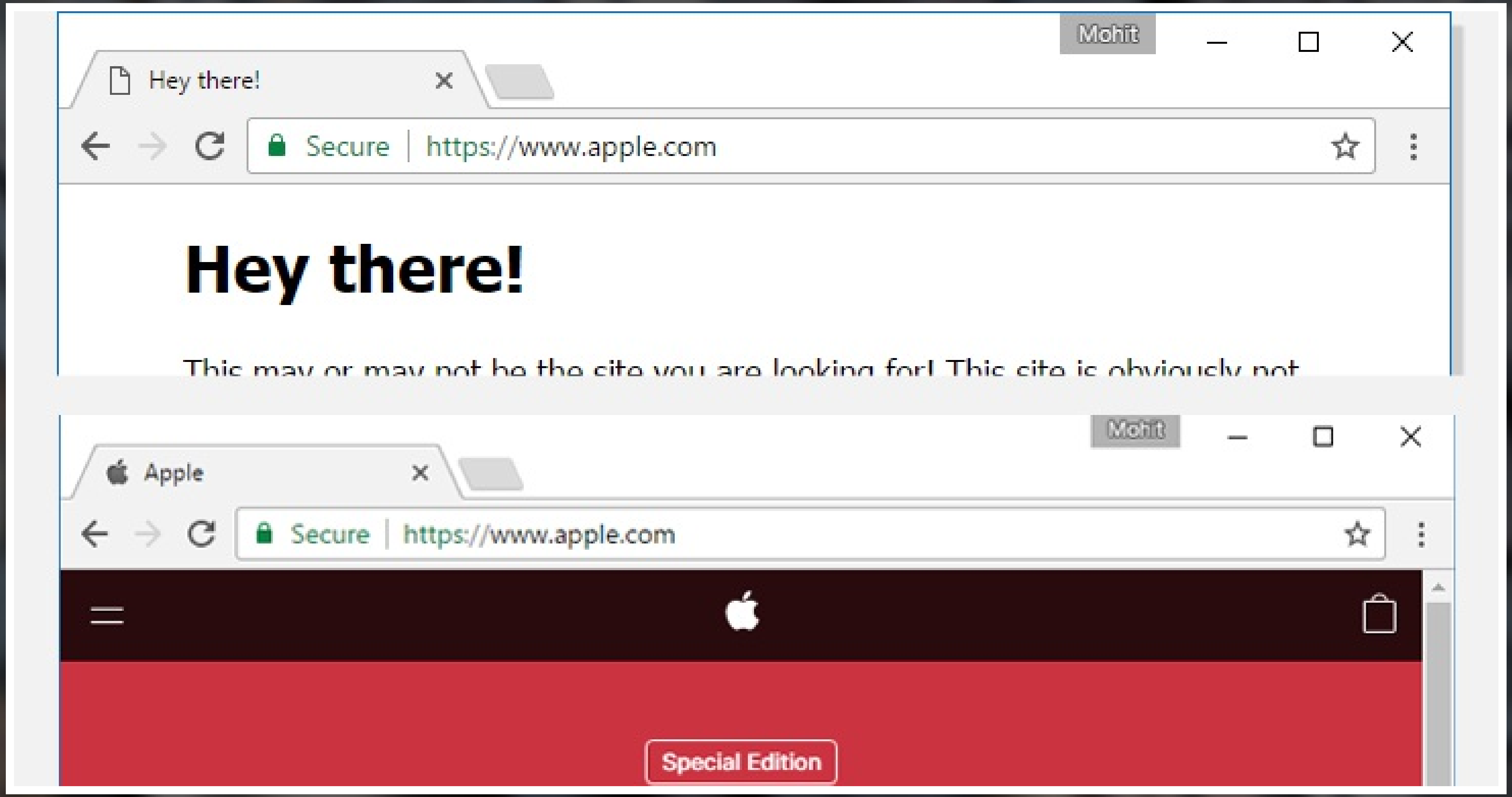
http://www.paypal.com

www.xn--pypal-4ve.com

...but

PUNYCODE IS NOT PERFECT

- Won't trigger if full domain uses foreign alphabet
  - The result can be pretty scary



Hey there!

This may or may not be the site you are looking for! This site is obviously not

WE'RE DOOMED!

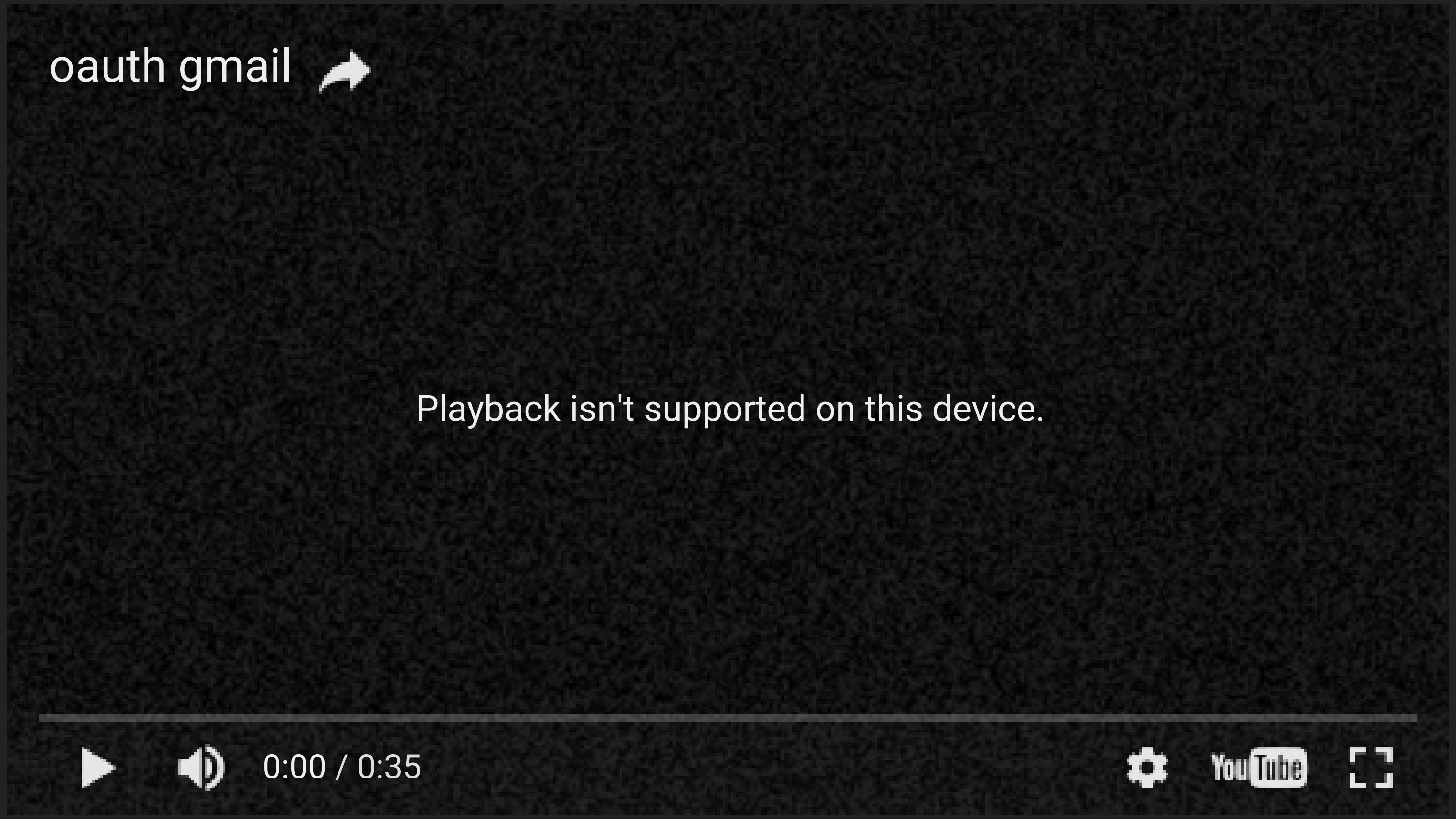
- It's pretty rare though..
- Password managers to the rescue!

5. I'M USING 2FA, I'M PHISHING FREE!

2FA IS GREAT, NOT BULLET PROOF

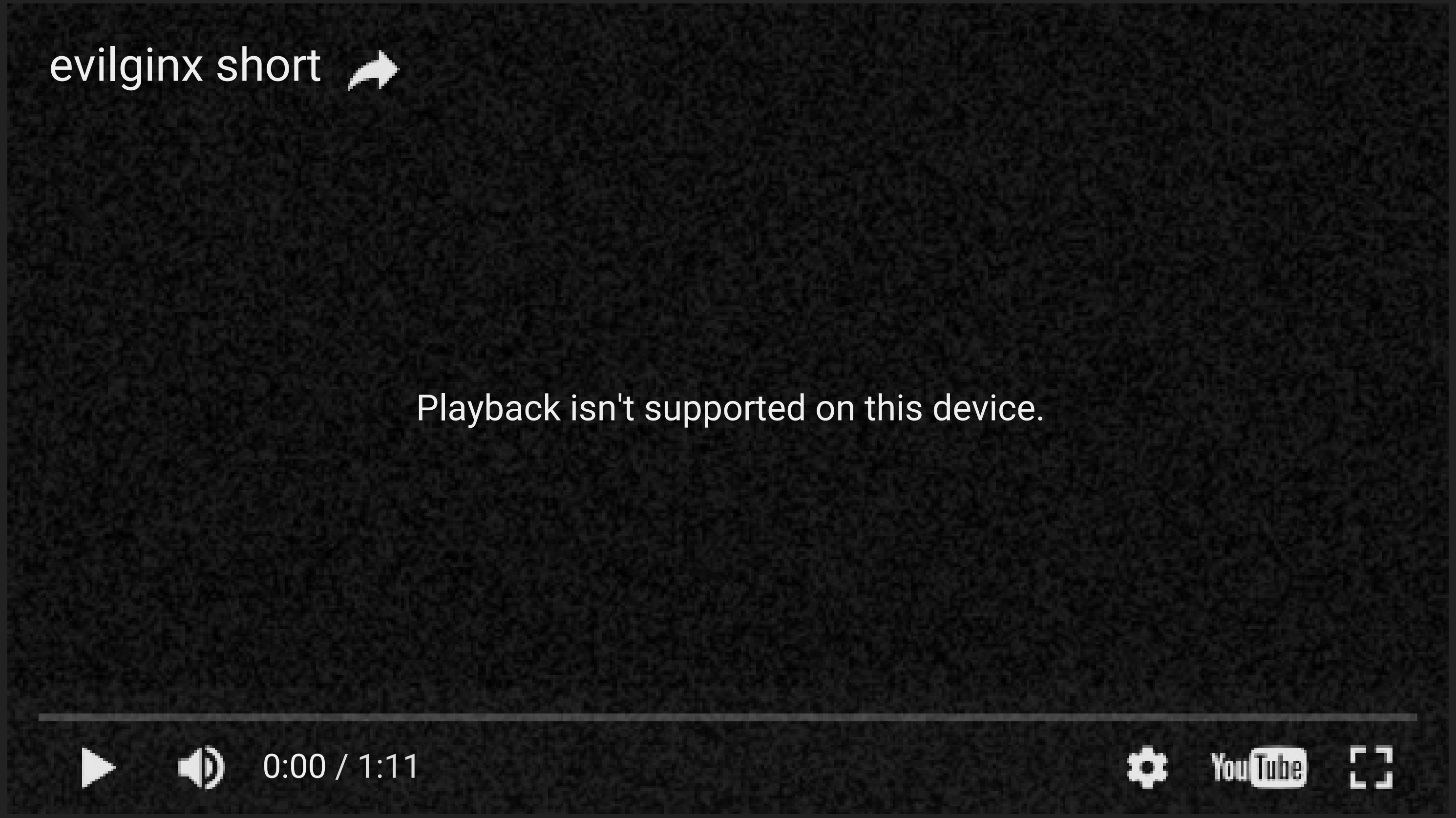
- 2FA can be bypassed
  - Website vulnerability
  - Social engineering
  - OAuth

OAUTH PHISHING EXAMPLE : GOOGLE DOCS



Playback isn't supported on this device.

BYPASSING 2FA : EVILGINX



evilginx short

Playback isn't supported on this device.

OK, THAT'S ENOUGH FOR TODAY

ANY QUESTIONS?

QUIZ TIME!

http://kahoot.it