



Share
Gerry Grant



Cyber Services

- ▶ Security Assessments
- ▶ Footprinting
- ▶ Social Engineering
- ▶ Training and Awareness
- ▶ Cyber Essentials advice

Ethical Hacking

- ▶ BSc Ethical Hacking
- ▶ Abertay University, Dundee
- ▶ Established 2006
- ▶ “It takes a thief to catch a thief”
- ▶ abertay.ac.uk/studying/udg/ethhac
- ▶ Shortlisted for DigiLeaders award 2017



“SECURITY IS A PROCESS, NOT A
PRODUCT”

Bruce Schneier

“I DON'T NEED TO RUN FASTER
THAN THE BEAR: I ONLY NEED TO
RUN FASTER THAN YOU.”

Updates

A critical pain in the ass

Updates matter

- ▶ Low effort but high reward
- ▶ Windows 10, 8.1, 7 get security updates
 - ▶ Windows XP and Vista don't get any updates
 - ▶ Google "Windows lifecycle factsheet"
- ▶ OS X 10.13 (High Sierra), 10.12 (Sierra), 10.11 (El Capitan) get security updates
 - ▶ Apple supports the current & two previous updates

Updates matter - Mobile

- ▶ iOS 11.1 (New emojis!!)
 - ▶ Version: Settings > General > About > Version
 - ▶ Update: Settings > General > Software Update
- ▶ Android 7 Nougat
 - ▶ Version: Settings > About Phone > Android Version
 - ▶ Update: Settings > About Phone > System Updates

Passphrases

Size matters!

Never give them away!

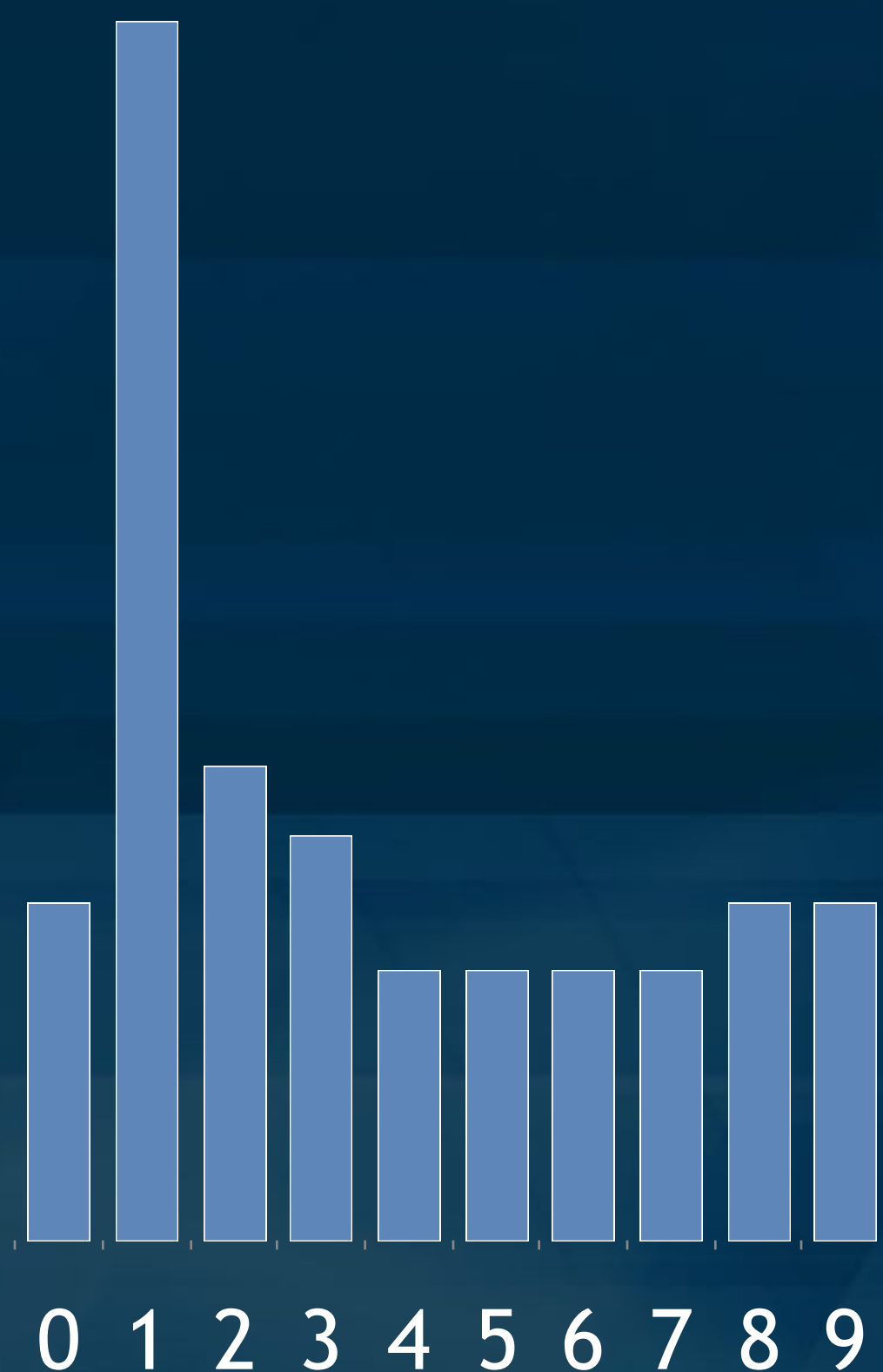


The worst passwords

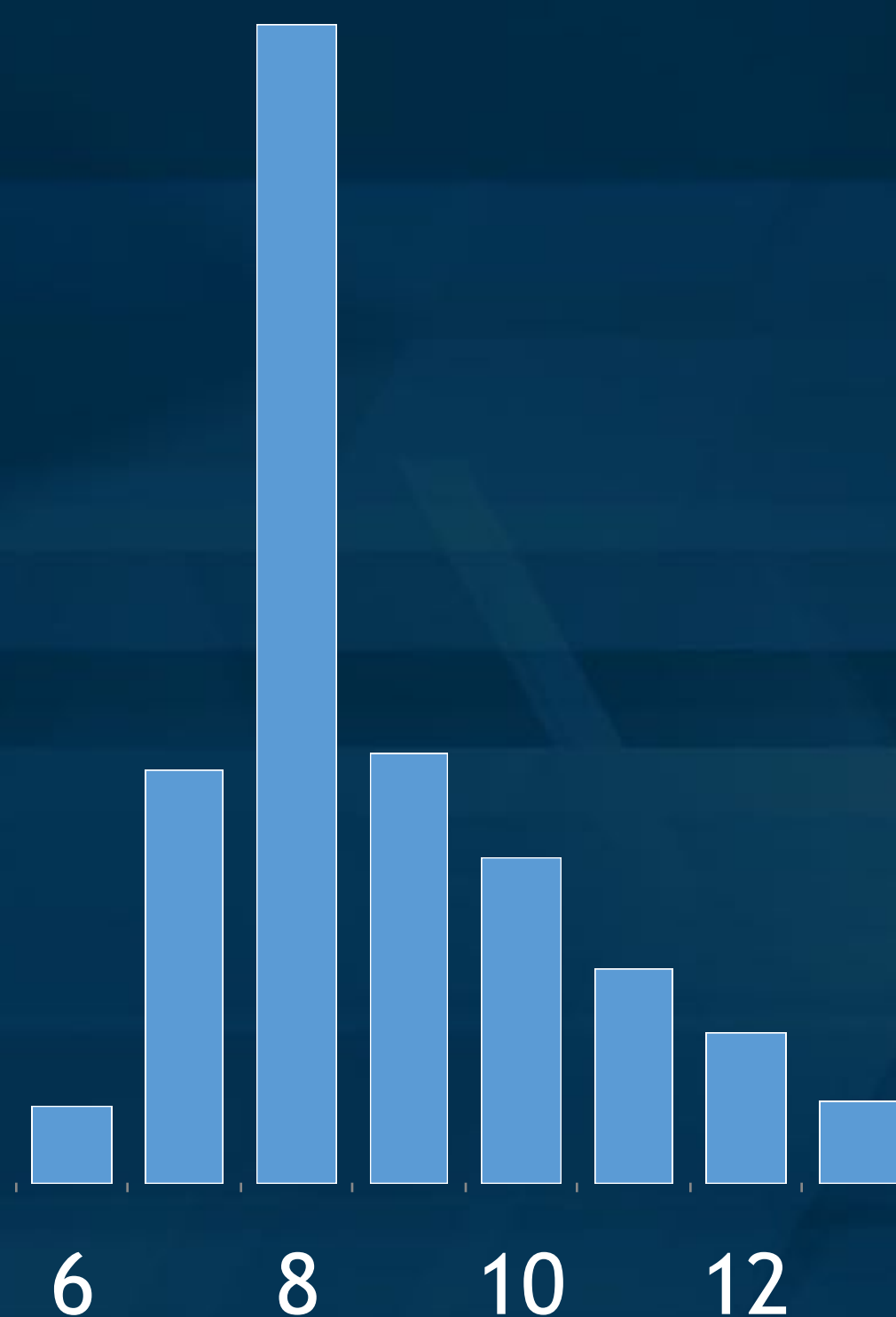
- ▶ 123456
- ▶ password
- ▶ 12345678
- ▶ 1234
- ▶ master
- ▶ 12345
- ▶ dragon
- ▶ qwerty
- ▶ 696969
- ▶ mustang
- ▶ letmein
- ▶ baseball
- ▶ michael
- ▶ football

Statistical analysis of passwords

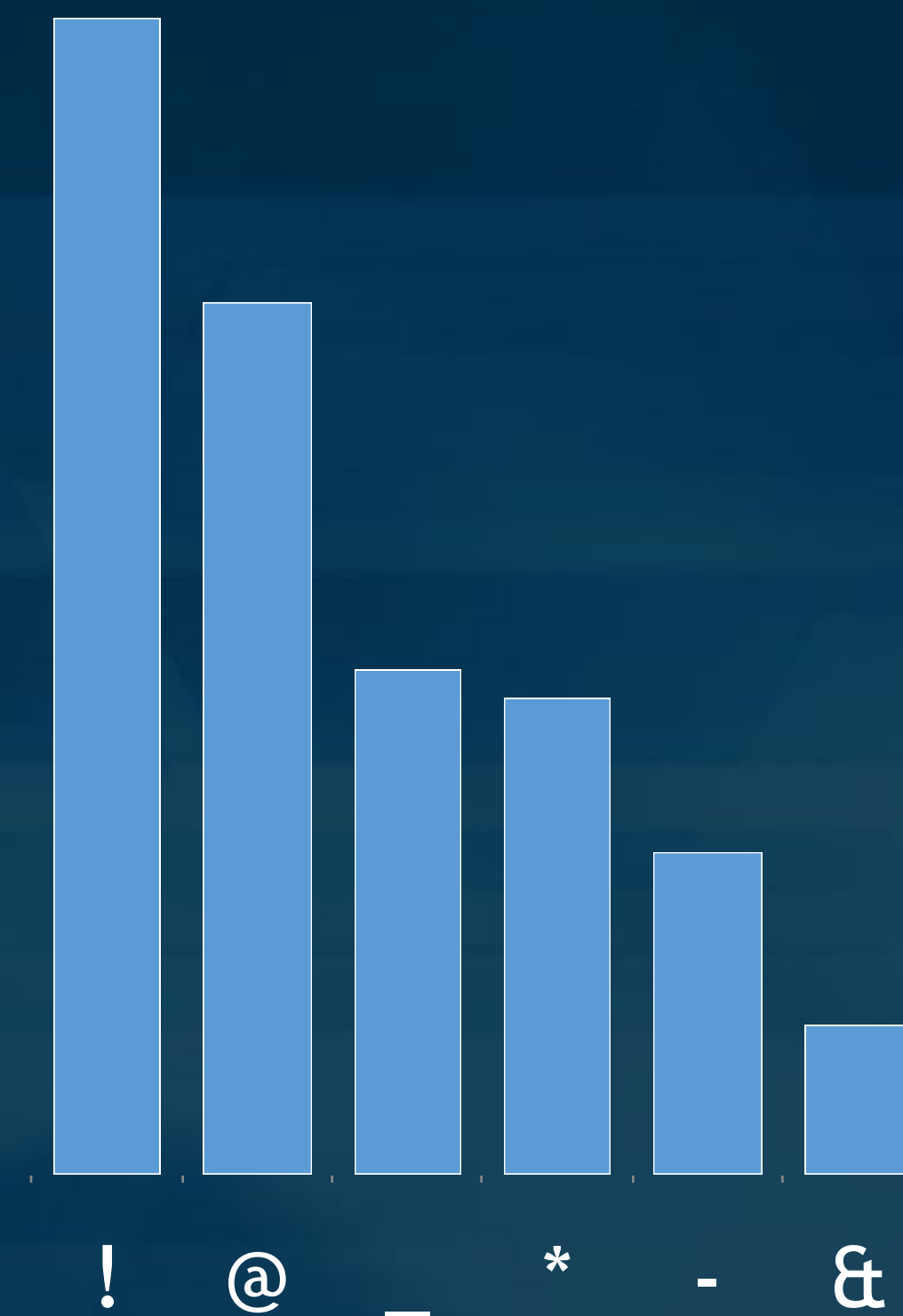
Numbers Used



Length



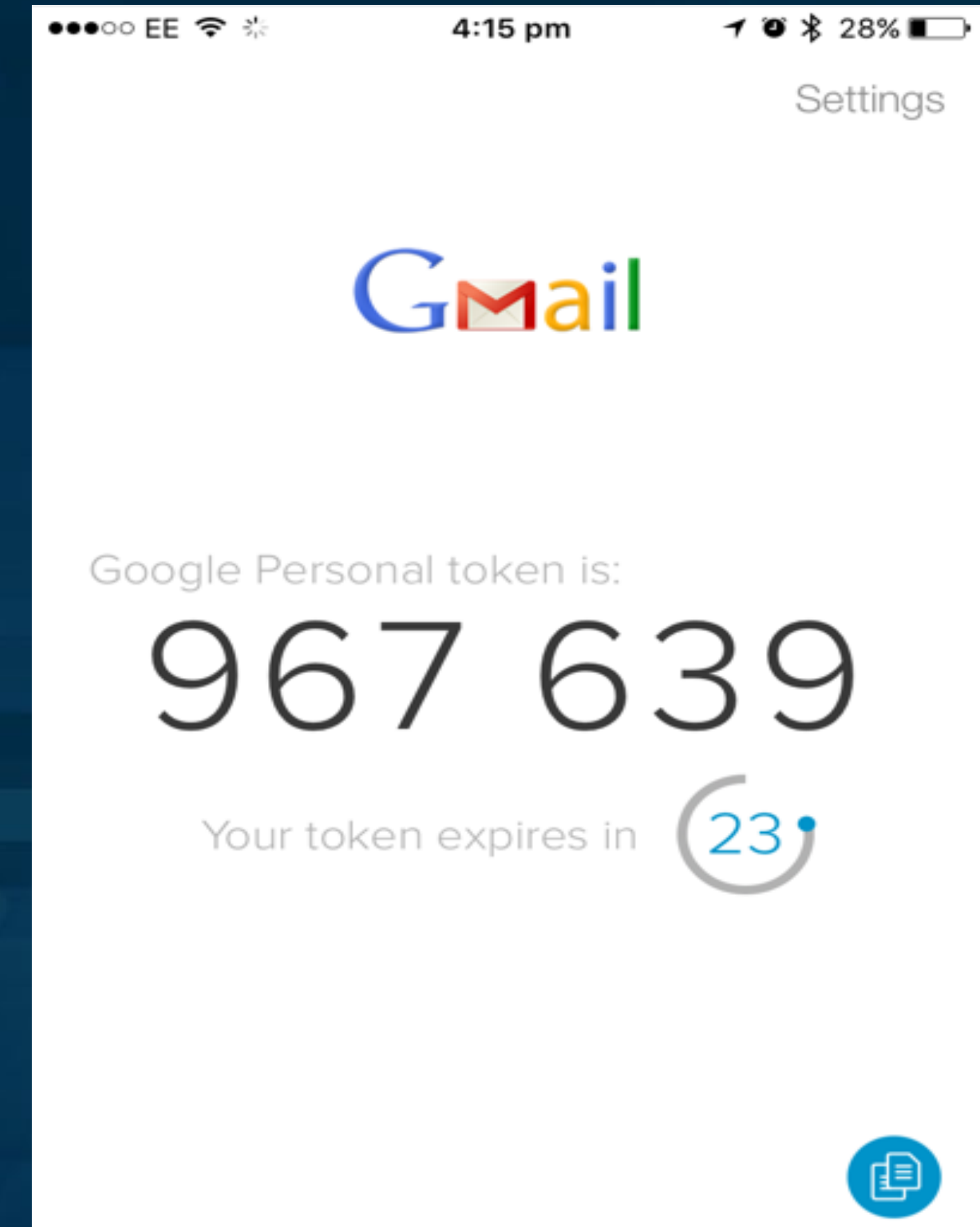
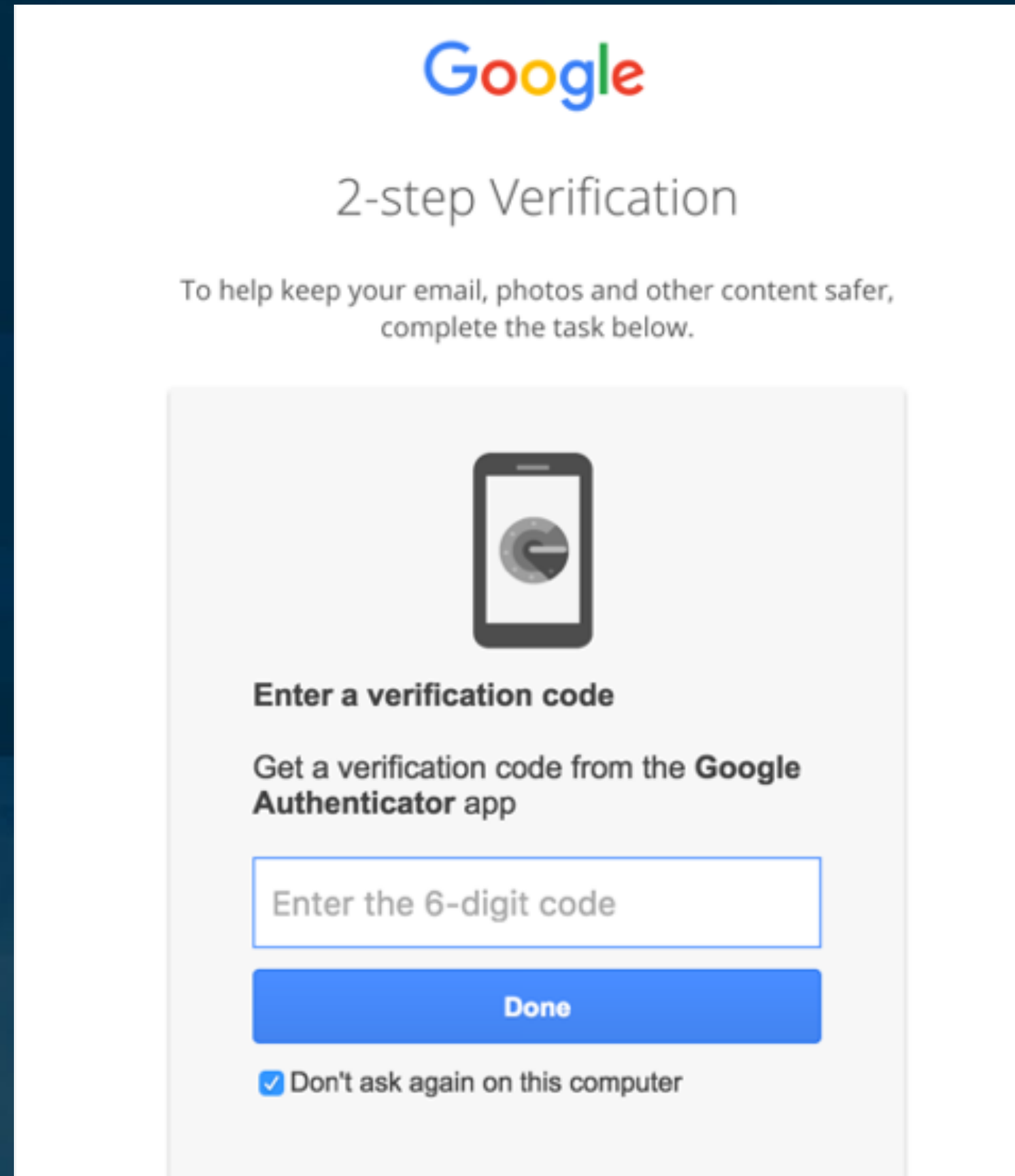
Symbols Used



Password managers

- ▶ Lastpass
 - ▶ All platforms
 - ▶ Cloud based
- ▶ 1Password
 - ▶ All platforms but works well with Apple
 - ▶ Sync devices

Two factor authentication

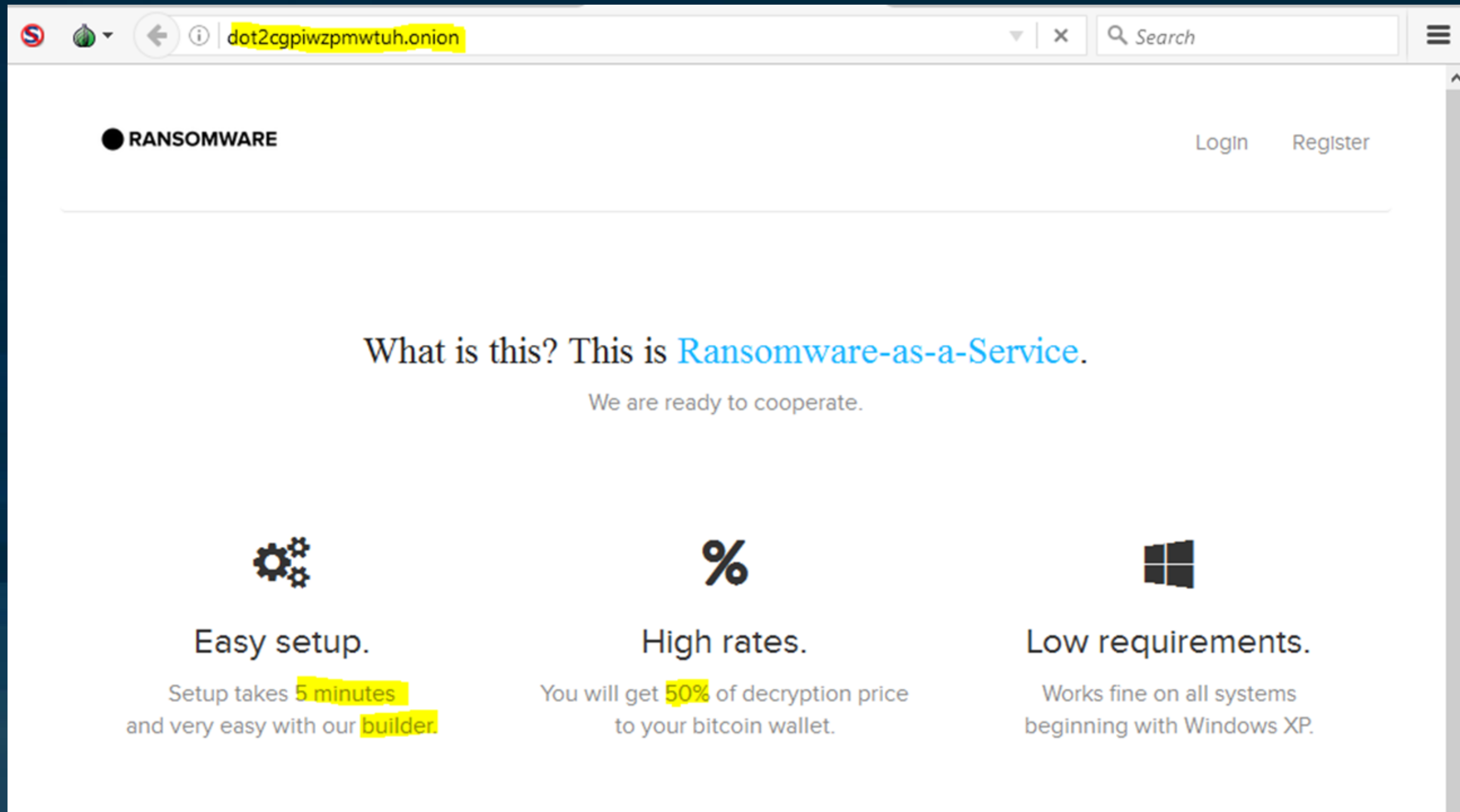


Ransomware

We have a solution

Ransomware

- ▶ Encrypts your files
- ▶ Demands a ransom, usually only a couple of hundred pounds
- ▶ You **MIGHT** get your files back
- ▶ **DO NOT** pay the ransom
- ▶ Report to the police on 101



4 WTF is this?? and what is Bitcoin???

Could you check video on Instruction field?

A I got hit with this virus on the 3rd, now today it looks like the files changed. Are you also stopper@india.com, or is that a second ransomware?

We are only Spora Ransomware, no other ransomwares we can help

Gifted free decode for 798182B07B5530. Please, make a review (with screenshots, payment details, decryption process) on site: <http://bit.ly/2ky4Eb2>

And few others that you will find. Please, make a truthful review as it was. Thank you

7 ok, now i will make some screenshots for proofs. And copy link to site. Thanks.

E Both of my computers have been infected by this. I was able to piece together the price for the first one in bitcoins but my other computer just showed up as being infected too. I will pay the full restore fee, but I dont think I could get the bitcoins in only 3 days, especially starting from scratch.

No problem. We disabled deadline for you. Pay asap, please. After this, left a review on <http://bit.ly/2ky4Eb2> and we will send you back some bitcoins

A Thank have p
Last u
depend
my 3
one w

Please that we

nomoreransom.org

NO MORE RANSOM!

★ English ▼

[Crypto Sheriff](#) [Ransomware: Q&A](#) [Prevention Advice](#) [Decryption Tools](#) [Report a Crime](#) [Partners](#) [About the Project](#)

**NEED HELP unlocking your digital life
without paying your attackers*?**

YES **NO**

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!



Fabian Wosar

@fwosar



Follow



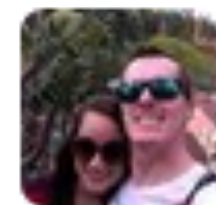
Companies ask me if I recommend ransomware insurance. I have ransomware insurance. It's called having a backup. You should try that, too.

RETWEETS

199

LIKES

312



5:51 PM - 23 Jan 2017

“The condition of a backup is unknown until a restore is attempted.”

Social Media

Facebook, Twitter, LinkedIn, Instagram



Gerry Grant
@Gerrytonic

Proud daddy, happy husband, just graduated in Ethical Hacking. Working for @SBRC_Scotland. All opinions my own. I was on the tele once. Just once mind.

📍 Scotland, United Kingdom

469 Following 869 Followers

Tweets Tweets & replies Media Likes

You Retweeted

Barrier Networks @BarrierNet... · 21h ✓
Think twice before providing sensitive information. Scams like this one are obvious to some but many people do fall for them #cybersecurity

SECURITY CHECK
Is there your card in the hackers database?



Ae-ae-ron Cameron
@AaronCameron6 Follows you

Student Ethical Hacker at Abertay uni. Work at Scottish Business Resilience Centre. 'If fifty million people say a foolish thing, it is still a foolish thing.'

229 Following 155 Followers

Tweets Tweets & replies Media Likes

Ae-ae-ron Cameron @... · 30/10/2017 ✓
#SSEspotlight #chrisgreig cmon boys 🙌🙌

Ae-ae-ron Cameron Retweeted

Lewis Capaldi @Lewi... · 20/10/2017 ✓
Cheers sen! 🙌🙌 @NiallOfficial

Niall Horan @NiallOfficial



Treven Lagerman

42
connections

All-Source Intelligence Analyst at United States Army

US Military Posts in Europe | Military

Current Mission Essential, US Army

Previous US Army, Afghanistan Theater All-Source Intelligence, All-Source

Education University of Maryland University College

Summary

Seven years experience as an Intelligence Analyst. Excelled as an All-Source Analyst/Supervisor; supported both Geospatial Analysis and Signals Intelligence missions throughout my career. Currently deployed in support of Operation Enduring Freedom supporting missions in Kuwait, United Arab Emirates, Qatar, and Jordan. An expert on enemy combatant activities and atmospherics in US Central Command's Area of Responsibility. Extensive experience with Distributed Common Ground System-Army (DCGS-A), ACE Block II, Multi-Intelligence Analysis and Archive System (MAAS), and Portable Airborne Interrogator Transponder System (PAITS). Current Top Secret - Sensitive Compartmentalized Information security clearance; additionally read-on to SI, TK, H, G, NATO, NATO COSMIC, NATO ATOMAL, NITRO ZEUS in support of cooperation between the Cooperation Council for the Arab States of the Gulf (GCC). Possess both Official and Tourist US passports.



Phishing

Email —> link —> fake website —> malware/credential stealing

Phishing - Normal

- ▶ Economies of scale
- ▶ Not targeted
- ▶ Gullibility filter

Spear Phishing

- ▶ Highly targeted, using previous research
- ▶ Find areas of weakness and opportunity
- ▶ Make the target click the link
- ▶ This will result in compromise
- ▶ Everyone gets caught by this...

CEO Fraud

- ▶ “Please transfer lots of money to this account, it’s urgent. Love your CFO”
- ▶ Difficult to get your money back
- ▶ Verify!

Malicious Websites

Email → link → fake website → malware/credential stealing

Trust, but verify

Our Mantra

Wi-fi

A second front door






How wi-fi works



How wi-fi works



How wi-fi works

- ▶  sends ProbeRequest (“BT-HomeHub are you there?”)
- ▶  Router receives ProbeRequest
- ▶  Router initiates connection with phone 
- ▶  Receives ProbeRequest

Some Links

- ▶ Chrome security usability: youtu.be/XfFjde0UPbY
- ▶ Very strong passwords: theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/
- ▶ LastPass: lastpass.com
- ▶ 1Password: 1password.com
- ▶ Which sites use Two Factor Auth: twofactorauth.org
- ▶ Guides to setting up 2FA: turnon2fa.com
- ▶ Google Chrome: google.com/chrome