KnowBe4
Human error. Conquered.

Fight the Phish

Roger A. Grimes
KnowBe4
Data-Driven Defense Evangelist
e:rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

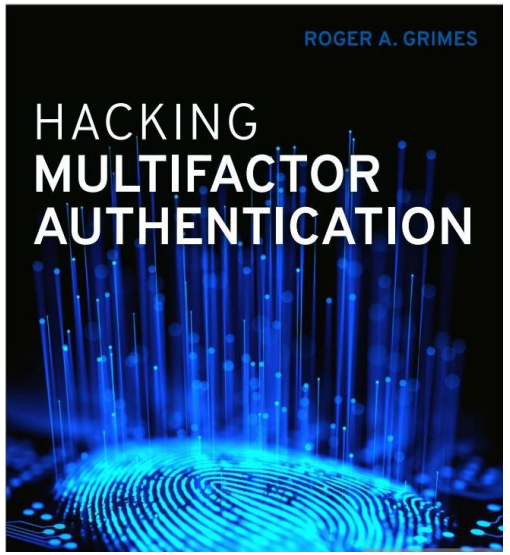
About Roger

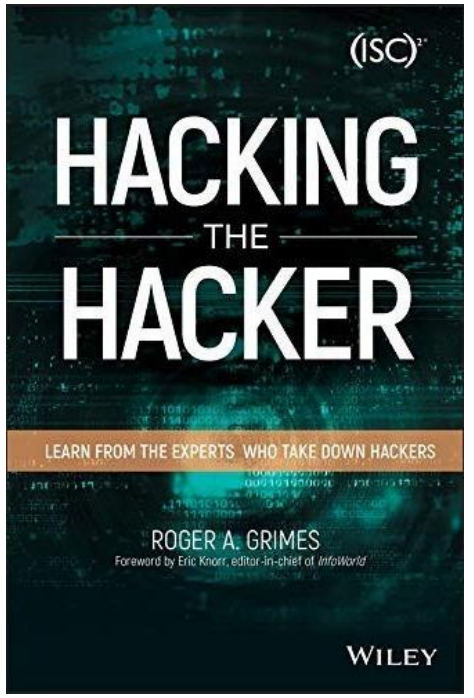
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,100 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

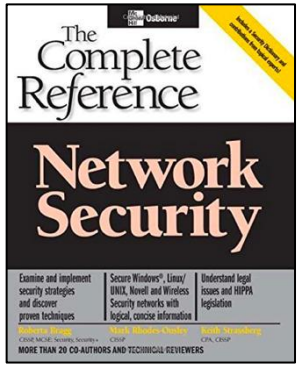
Certification exams passed include:

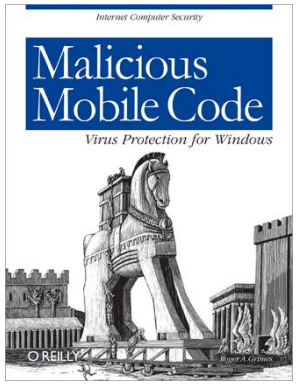
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

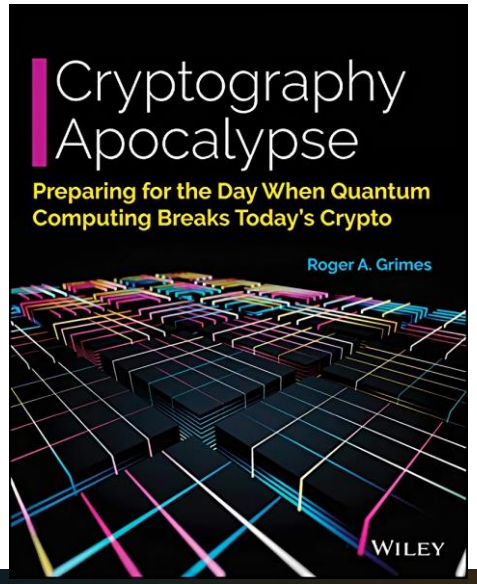
Roger's Books

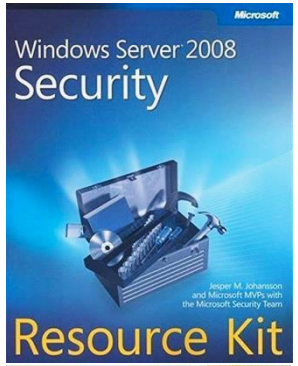


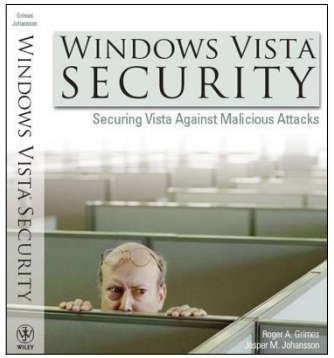


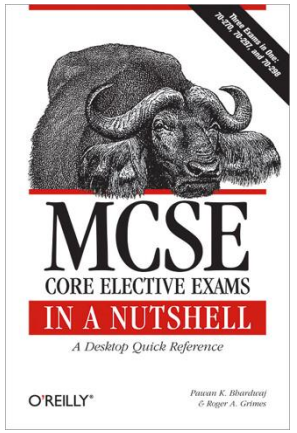


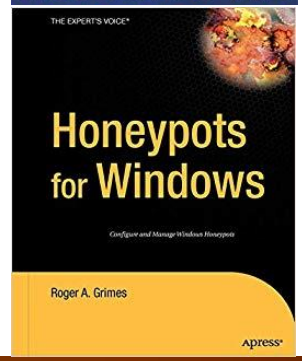












About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Agenda

- Why is Fighting Phishing Important?
- What is Phishing?
- Security Awareness Training Best Practices

Agenda

- Why is Fighting Phishing Important?
- What is Phishing?
- Security Awareness Training Best Practices

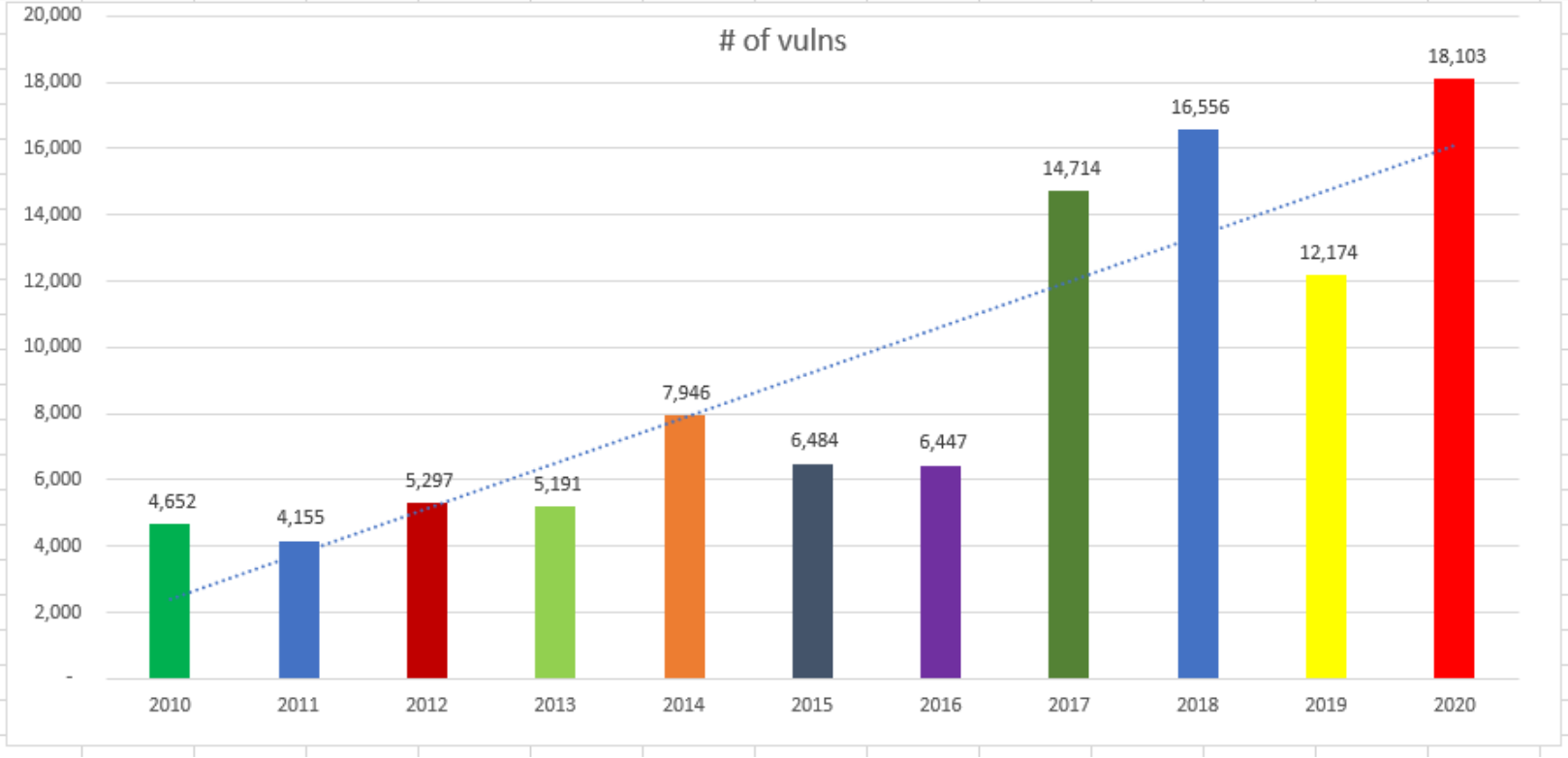
Problem – Overwhelming Number of Vulnerabilities

# of Vulnerabilities

- Avg: 4K-18K+ new threats/year
- 11-50/day, day after day

Number of Vulnerabilities

Year	# of vulns
2010	4,652
2011	4,155
2012	5,297
2013	5,191
2014	7,946
2015	6,484
2016	6,447
2017	14,714
2018	16,556
2019	12,174
2020	18,103

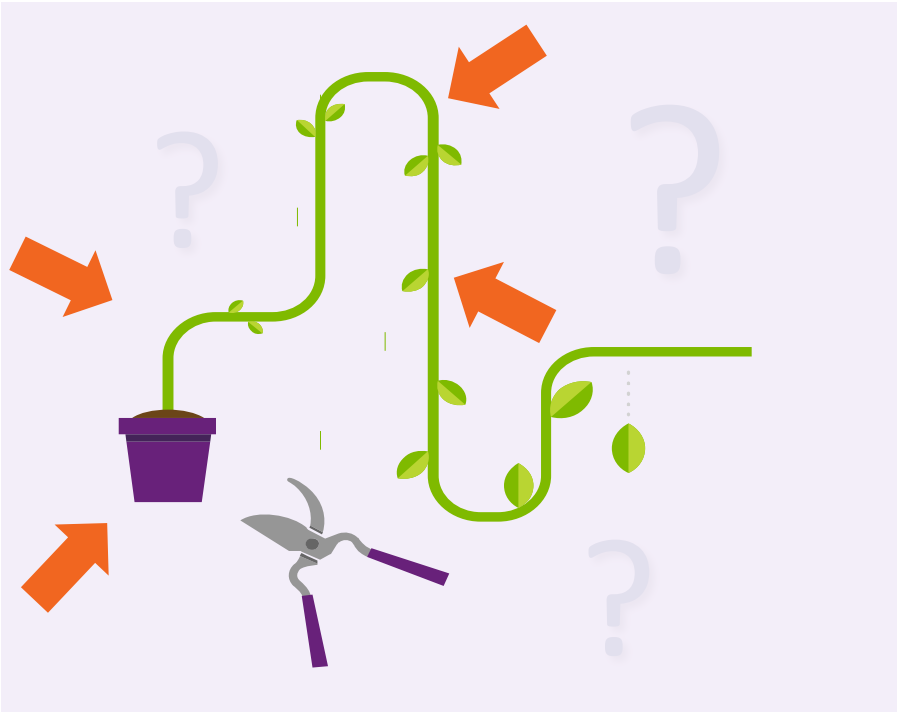


And this is just (known public) vulnerabilities, doesn't include hackers and a hundred million malware programs

How All Hackers and Malware Break In

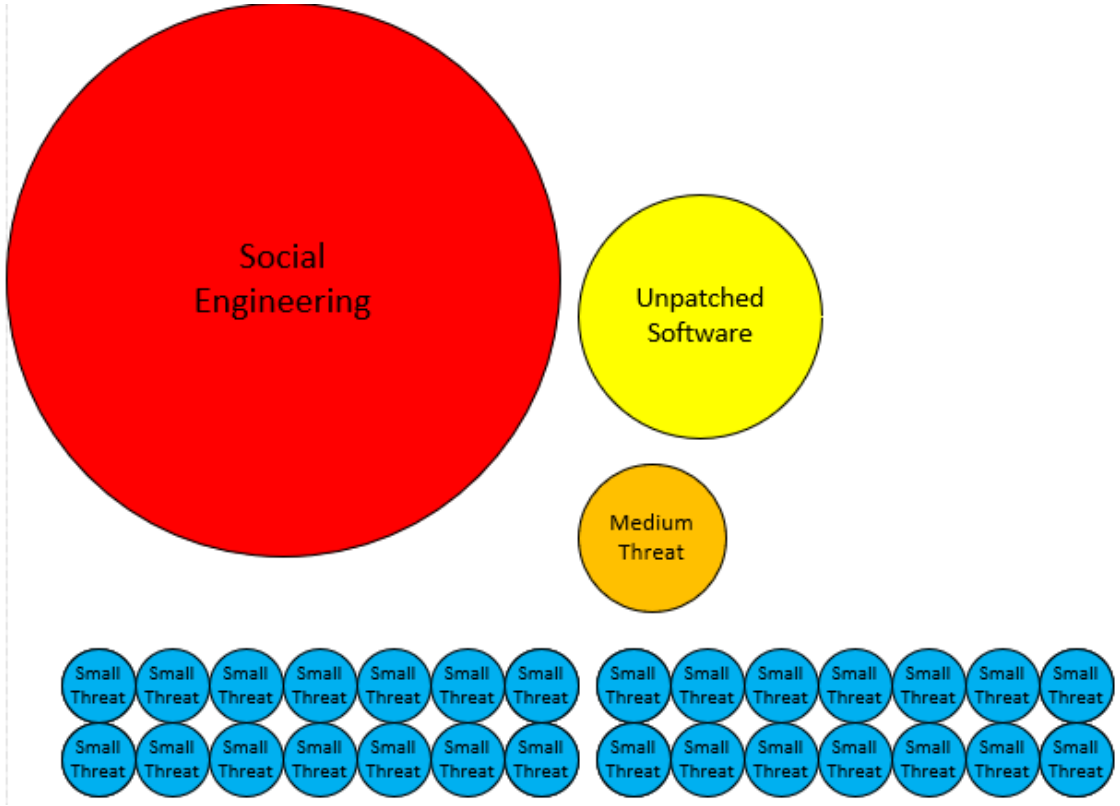
Here Are the 10 Root Exploit Methods:

- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue
- Physical Attack



Biggest Initial Breach Root Causes for Most Attacks

- Social Engineering
- Unpatched Software



Social engineering is responsible for majority of malicious data breaches

https://blog.knowbe4.com/phishing-remains-the-most-common-form-of-attack
https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense

Agenda

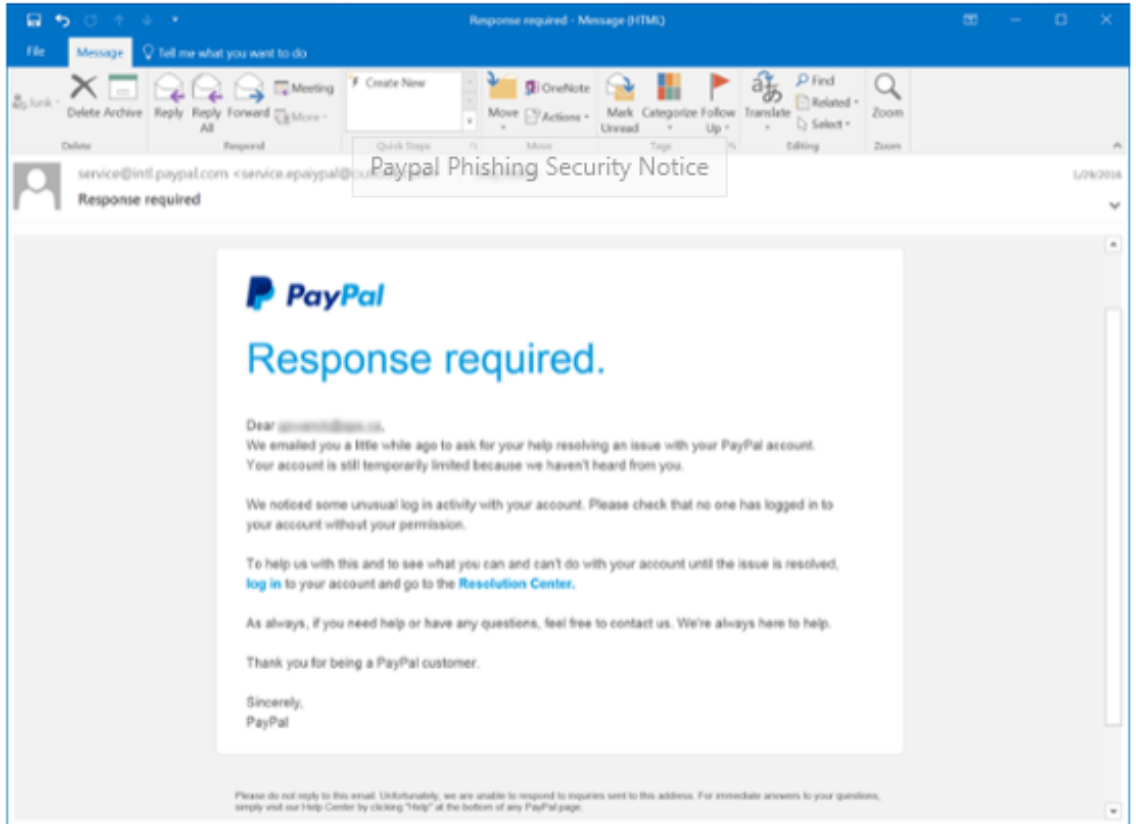
- Why is Fighting Phishing Important?
- What is Phishing?
- Security Awareness Training Best Practices

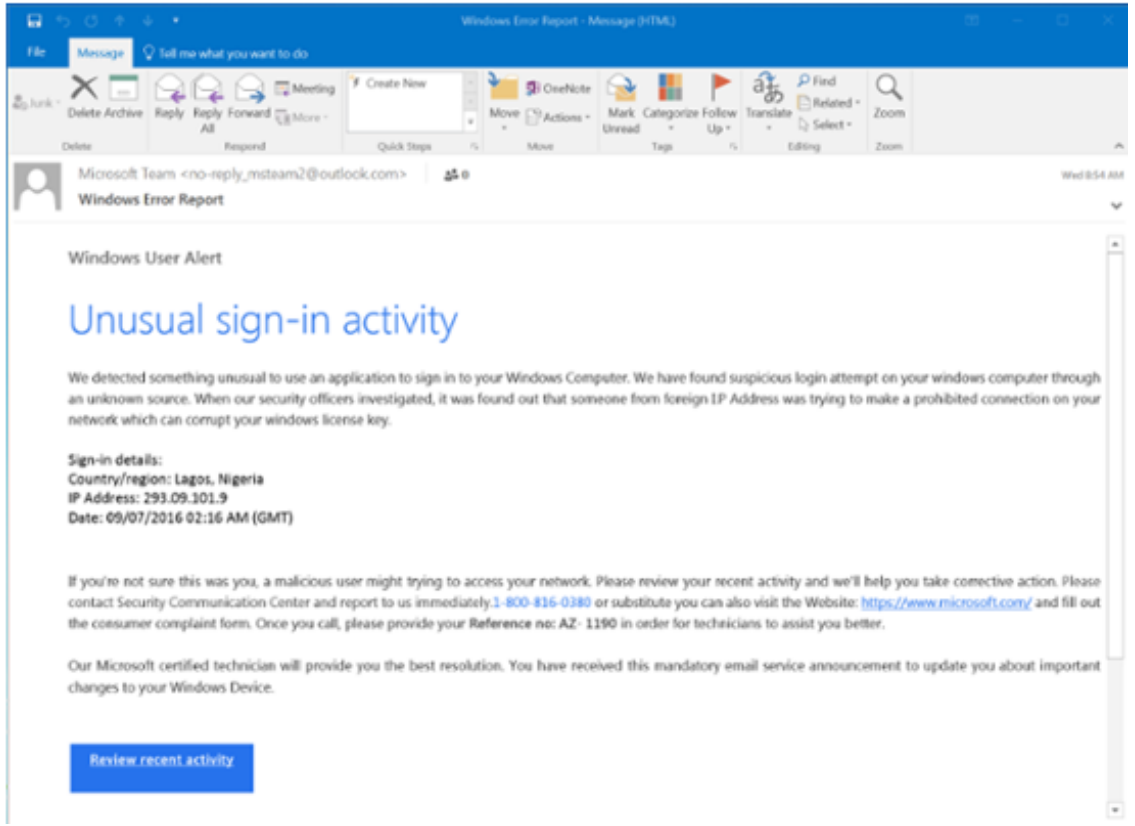
What is Phishing?

- The process of maliciously masquerading as a trusted entity to acquire unauthorized information or to created a desired action that is contrary to the victim's or their company's self-interests
- Simply put - a "con", criminal-intent
- Often done using in-person, email, IM, SMS, phone, etc.
- AKA phishing, spearphishing, spamming, vishing, etc.
- Emails/messages/SMS/Voice calls claiming to be from friends, co-workers, popular social web sites, banks, auction sites, or IT administrators are commonly used to lure the unsuspecting public.

What is Phishing?

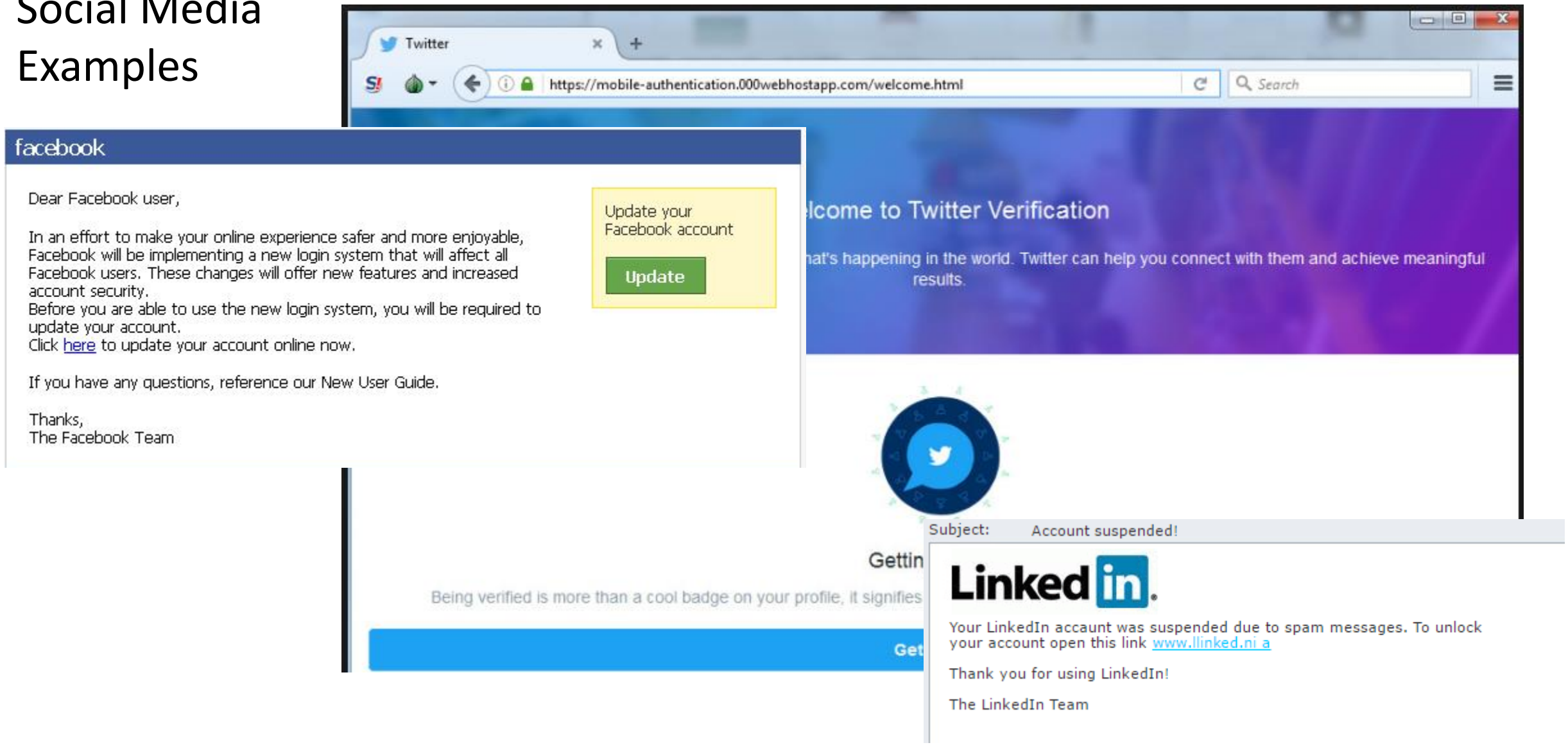
Email Examples





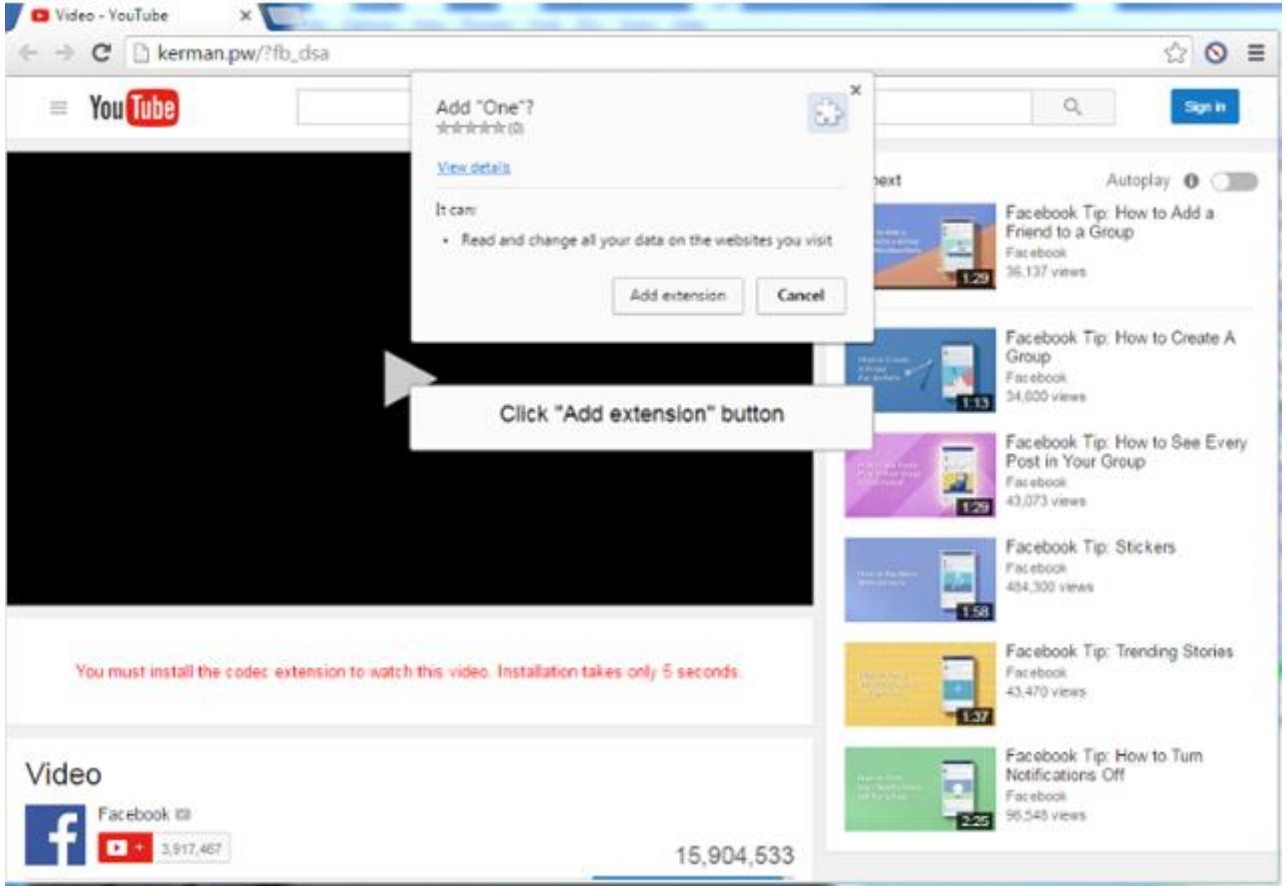
What is Phishing?

Social Media Examples



What is Phishing?

More Social Media Examples



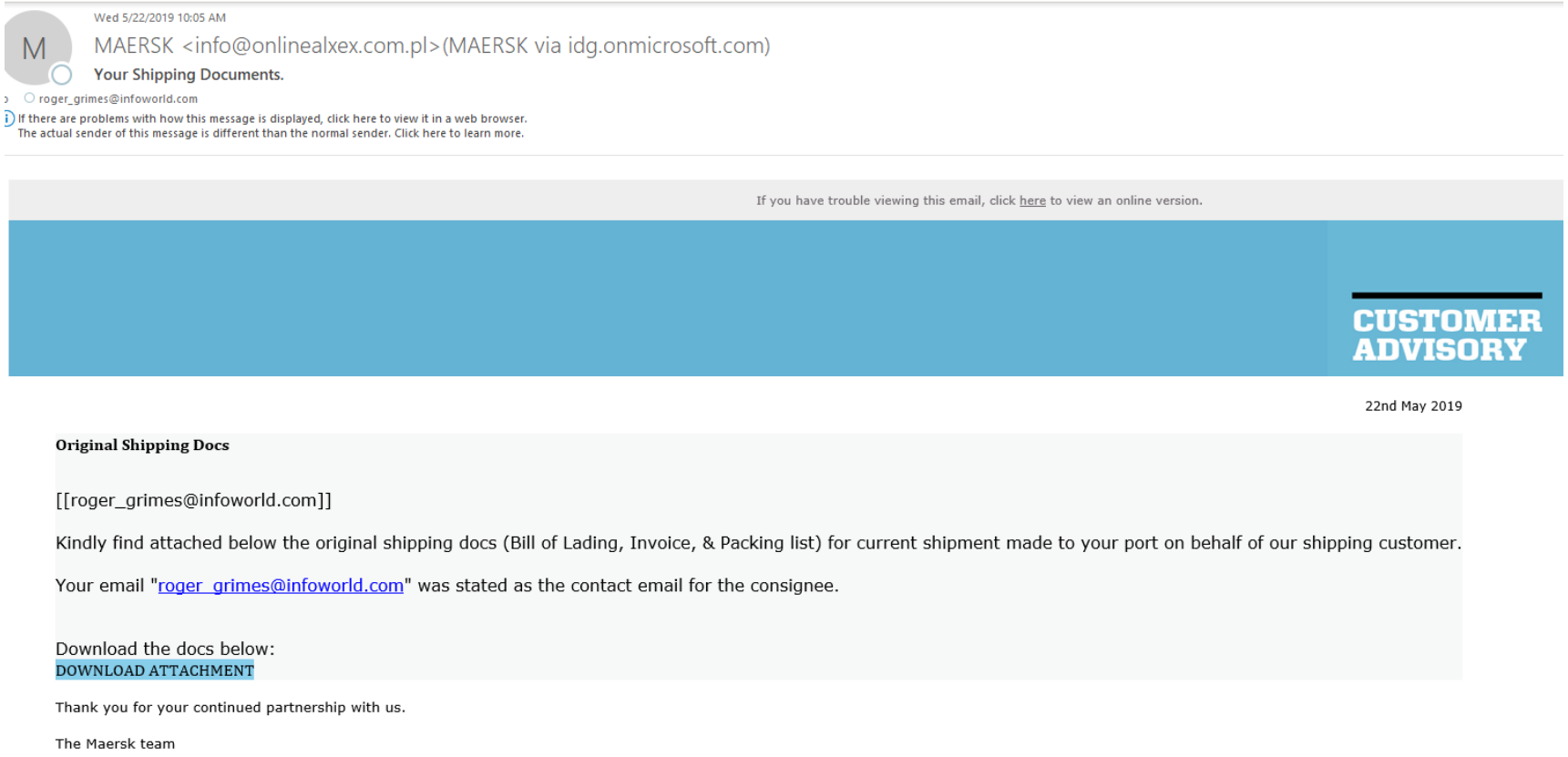
Business Email Compromise Scams

Spammer/Attacker/Phisher:

- Creates email purporting to be from boss, co-worker, invoicing company, etc.
- Can use fake email address or come from real person's email account
- Asks user to go out buy gift cards, send money, send W2s, pay invoice, change normal wiring instructions, etc.
- Almost always includes "stressor event"
  - (e.g. "I needed this yesterday or the deal is dead.", "Bill will be sent to collections!")
- Often indicates that sender will be out of reach and to do action now
- Defense: Can be defeated by creating a organizational policy which requires all unexpected requests for money, bill payments, etc. to be verified verbally

What is Phishing?

Fake Invoice Example



Wed 5/22/2019 10:05 AM

M

MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)

Your Shipping Documents.

roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.

If you have trouble viewing this email, click here to view an online version.

CUSTOMER ADVISORY

22nd May 2019

Original Shipping Docs

[[roger_grimes@infoworld.com]]

Kindly find attached below the original shipping docs (Bill of Lading, Invoice, & Packing list) for current shipment made to your port on behalf of our shipping customer.

Your email "roger_grimes@infoworld.com" was stated as the contact email for the consignee.

Download the docs below:
DOWNLOAD ATTACHMENT

Thank you for your continued partnership with us.

The Maersk team

Business Email Compromise Scams

Spammer/Attacker/Phisher:

- Creates email purporting to be from boss, co-worker, invoicing company, etc.
- Can
- Ask
- norr

Facebook and Google were victims of a $100 million dollar phishing scam:

Fortune

Ubiquiti Networks is one of the latest companies to admit it's had the multimillion dollar wool pulled over its eyes. The San Jose, Calif.-based networking equipment company disclosed it lost $46.7 million through such a scam in its fourth quarter financial filing.

dead.", "Bill will be sent to collections!")

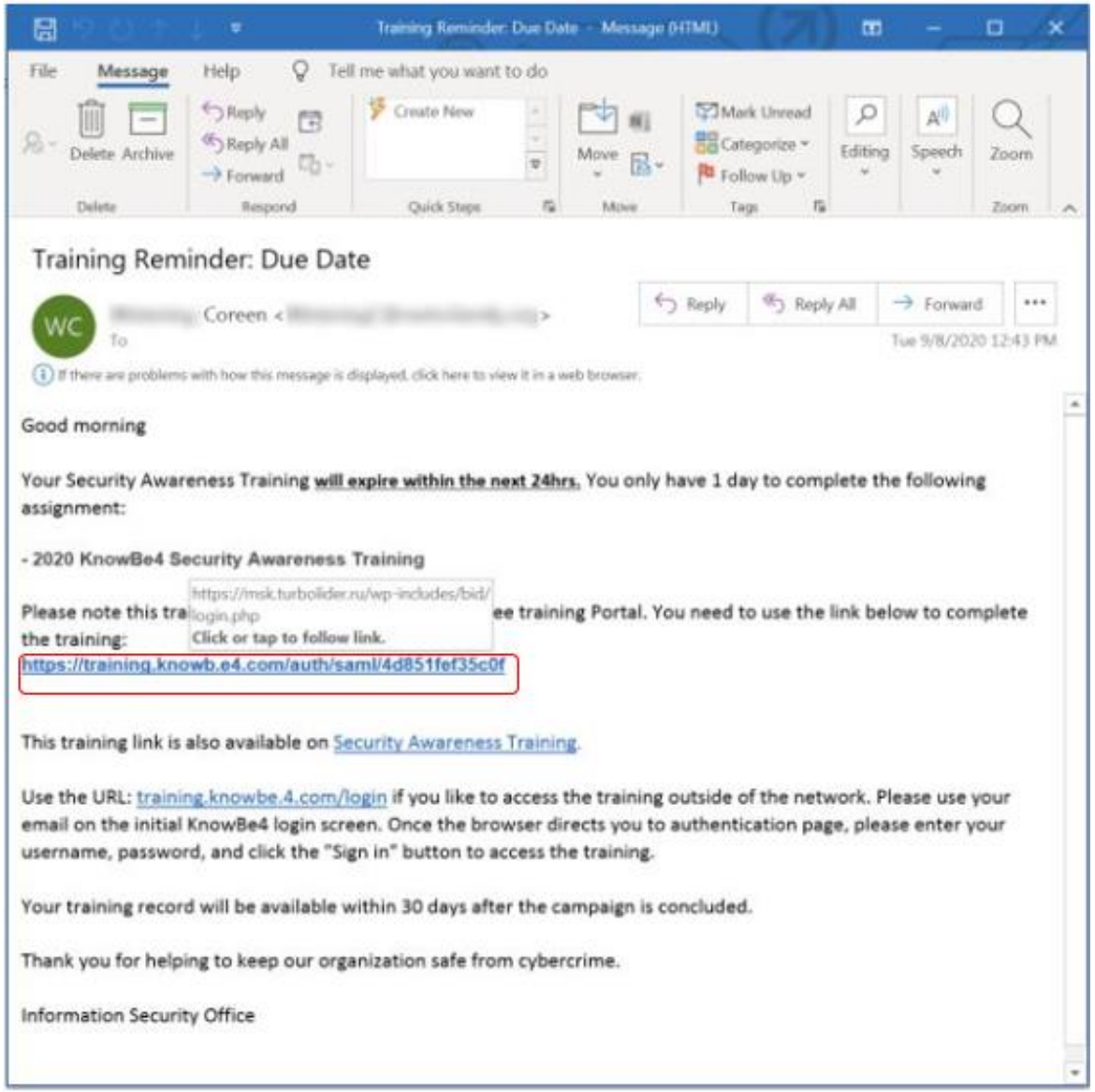
VIENNA (Reuters) - The head of Austrian aerospace parts maker FACC has been fired after the company was hit by a cyber fraud that cost it 42 million euros ($47 million).

- Defense: Can be defeate

unexpected requests for money, bill payments, etc. to be verified verbally

What is Phishing?

Sneaky Rogue URLs



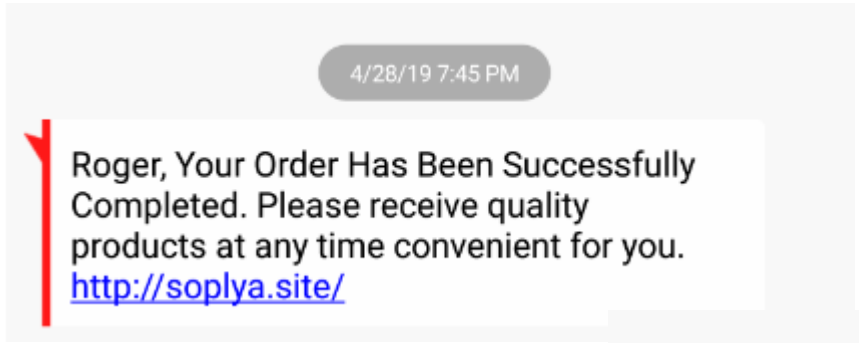
COVID-Related Phishing?

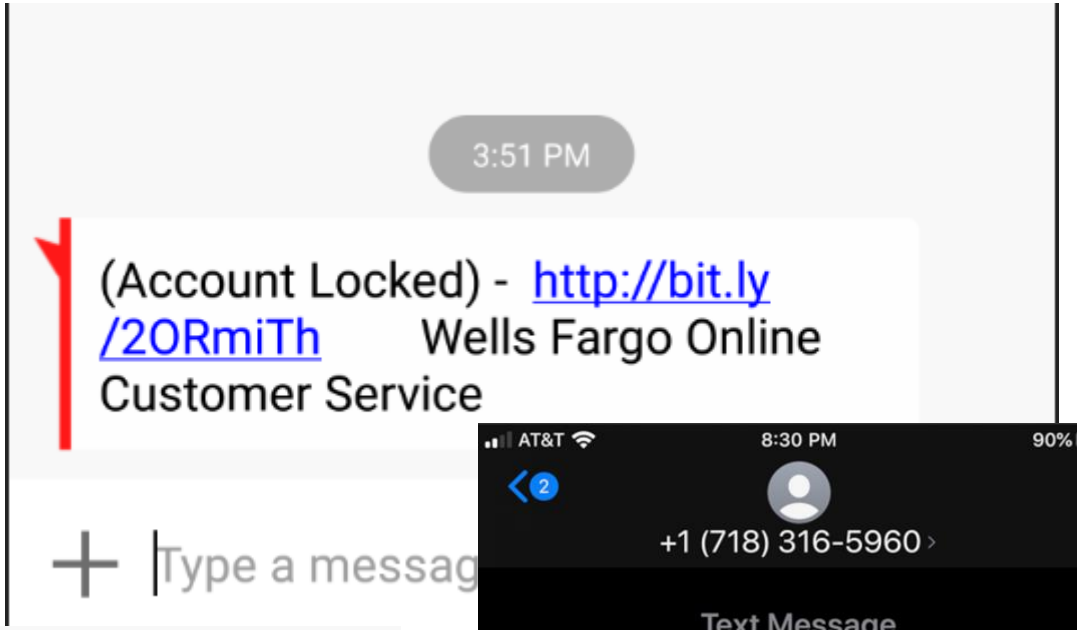
6000% Increase in Phishing Attacks Leveraging COVID-19, Healthcare Industry Often The Target

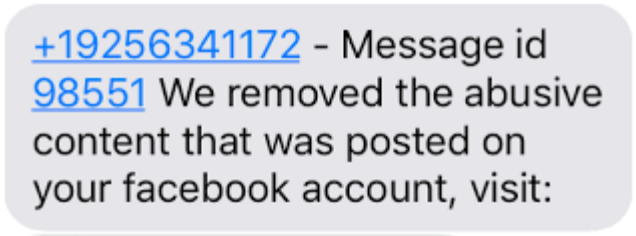
What is Smishing?

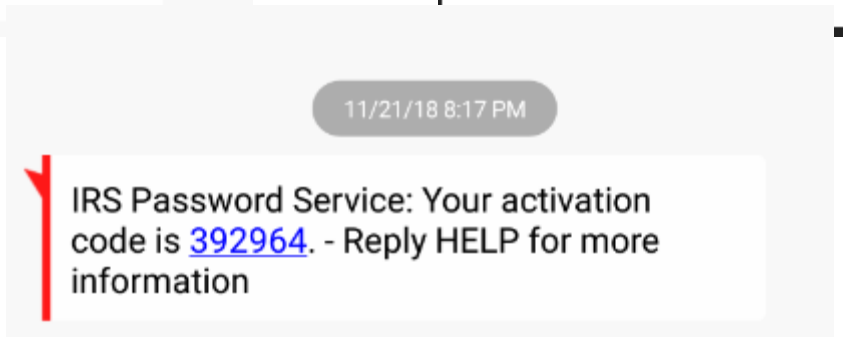
Smishing Examples

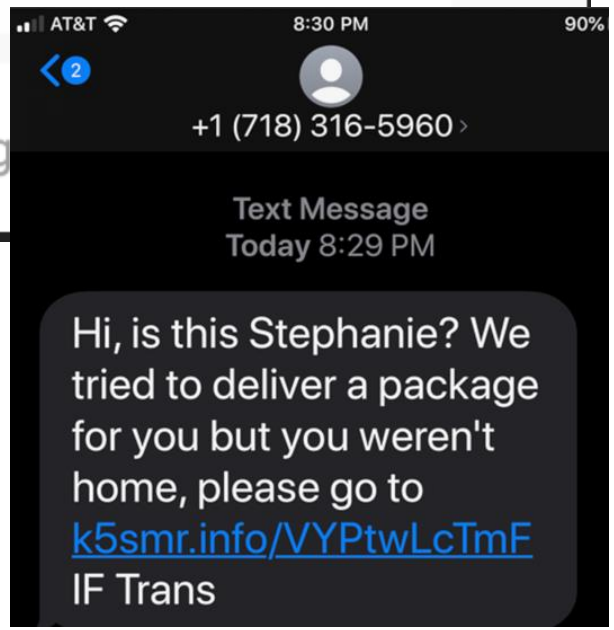
- Malicious SMS message
- Becoming very common











Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery Hack

- There is an inherent problem in that SMS message origination cannot be easily authenticated within SMS itself
- Anyone can claim to be anyone

To pull off hacker must have:

- You email address and associated phone number

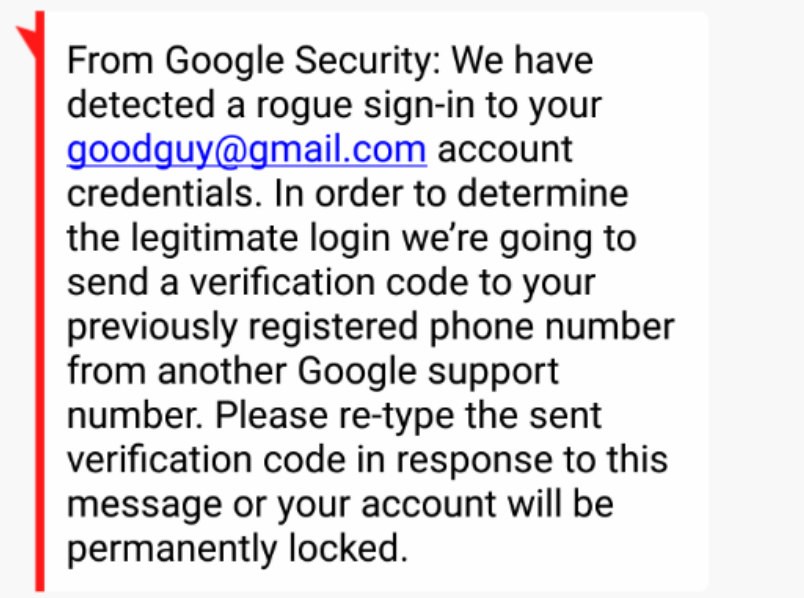
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

1. Hacker sends you a text pretending to be from your email provider asking for your forthcoming SMS PIN reset code



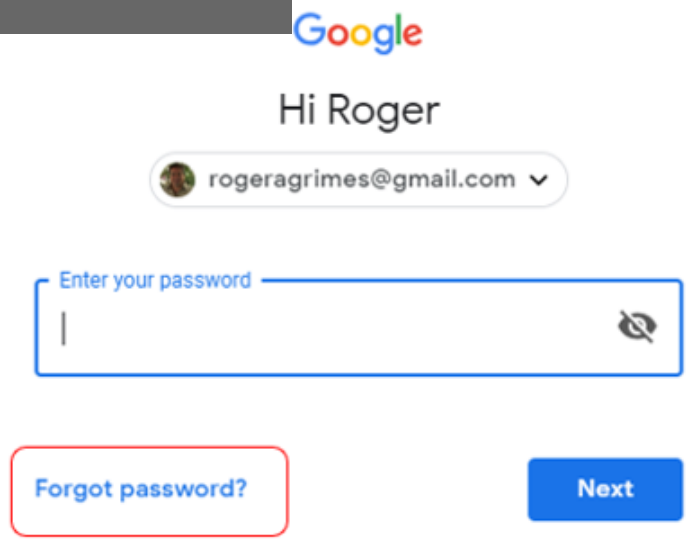
Rogue Recoveries

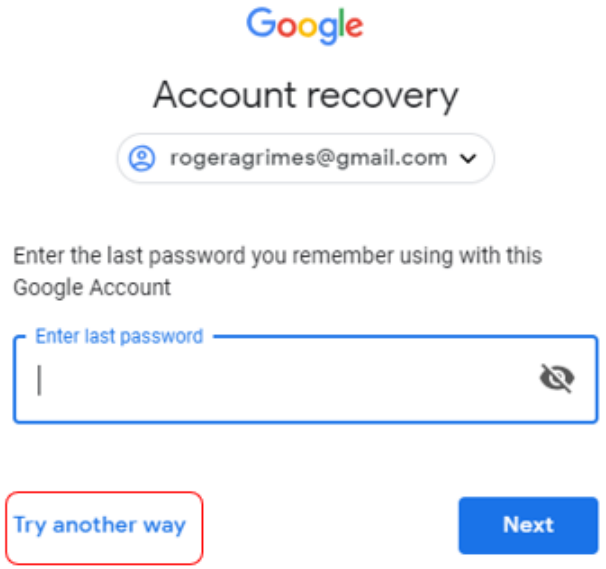
SMS Rogue Recovery

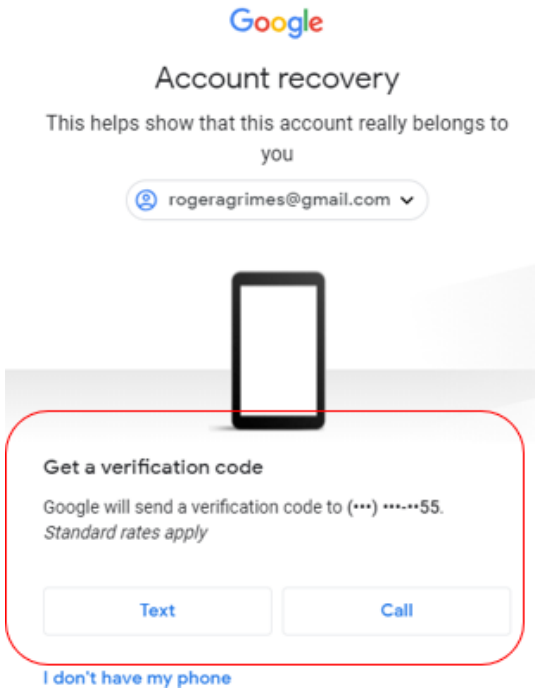
Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recoverv







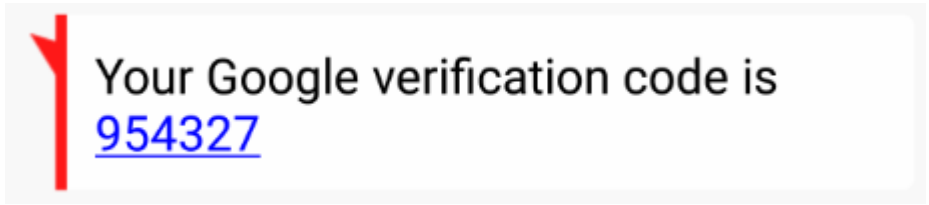
Rogue Recoveries

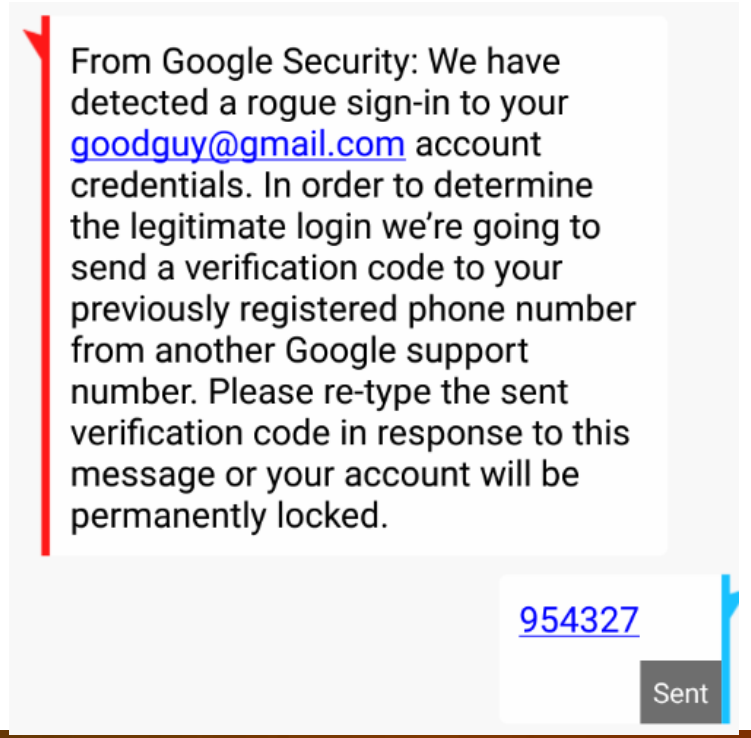
SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

3. You get text from vendor with your reset code, which you then send to other number

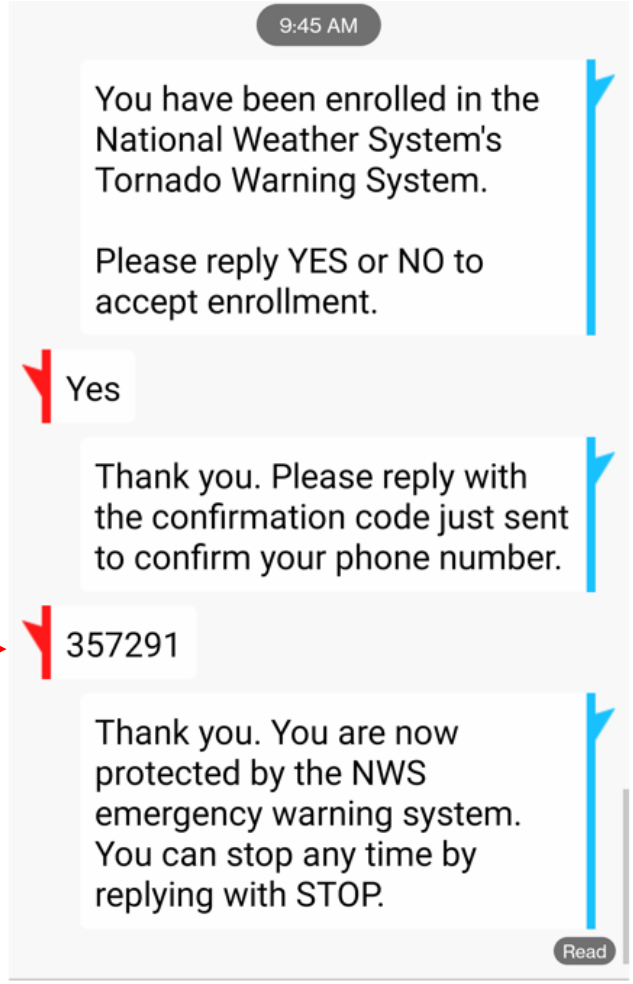




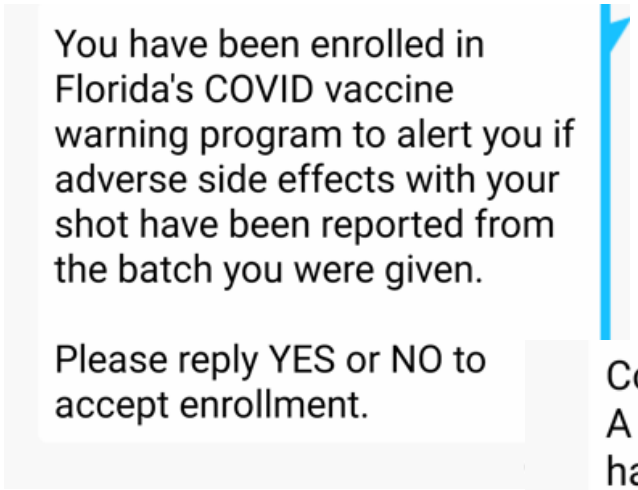
Rogue Recoveries

SMS Rogue Recovery

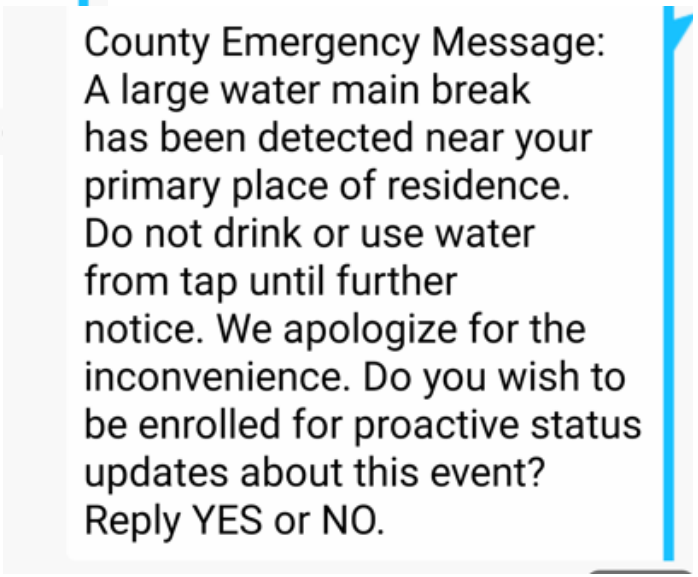
Hacking Into Your Email Using Recovery Methods



Code from their email, bank account, or stock account being reset



We can do this all day



What is Vishing?

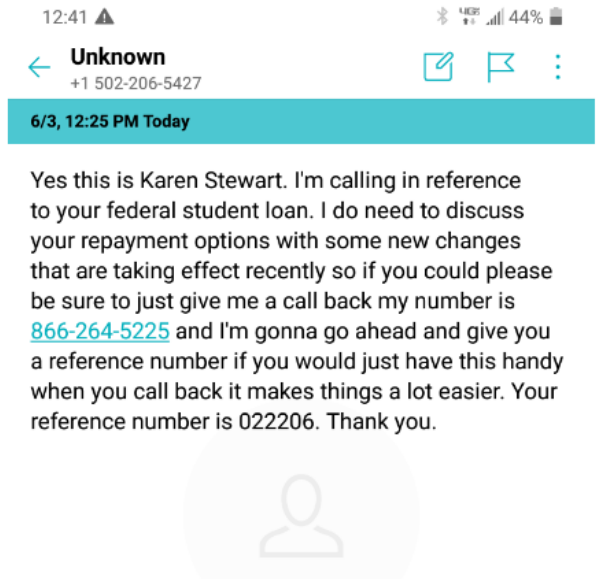
Voice Phone Phishing

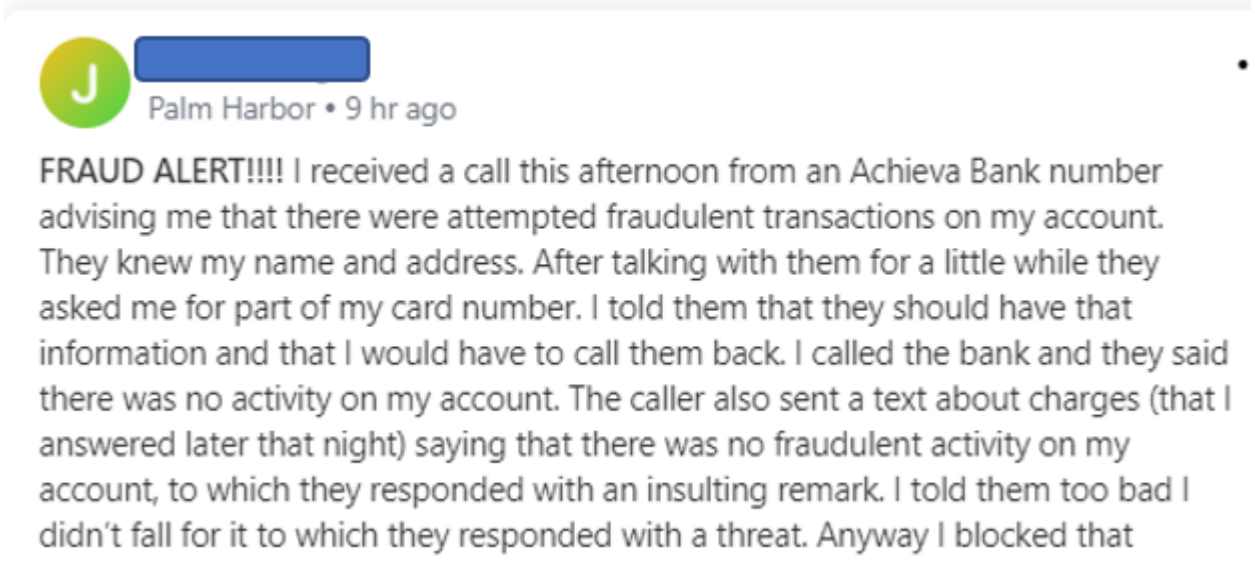
- Malicious person calls pretending to be from a trusted company
- Ex: Microsoft Tech Support has detected a virus on your computer
- Ex: Paypal person claims they have detected fraud on your account and need your help to stop quickly stop it
- Often has relevant, correct information about you and your legitimate related account
- Malicious person is often using your help to break into your PC or real account, as you're helping them over the phone

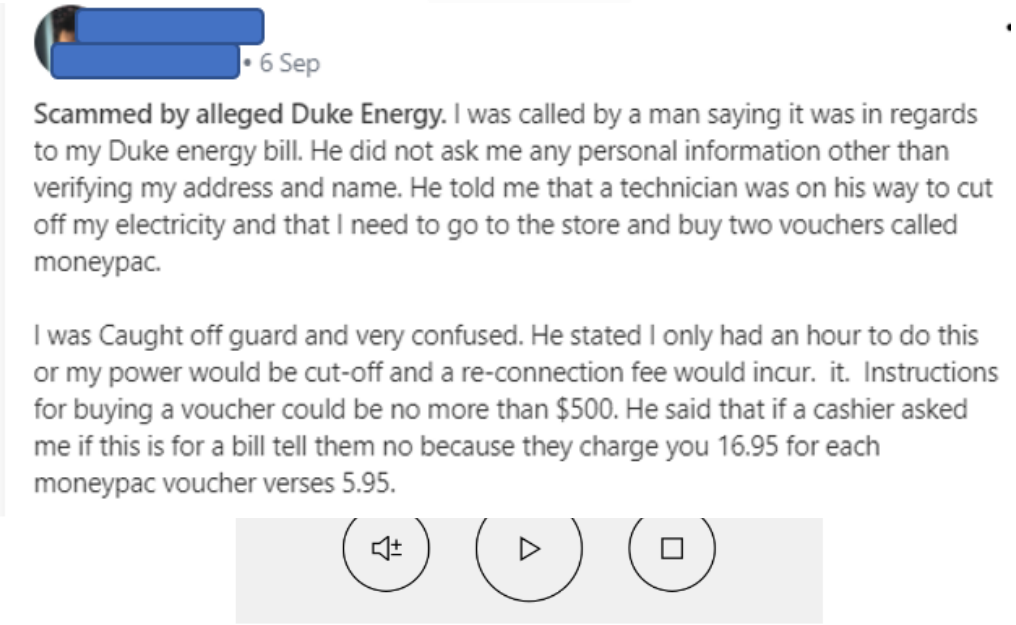
What is Vishing?

Voice Phone Phishing

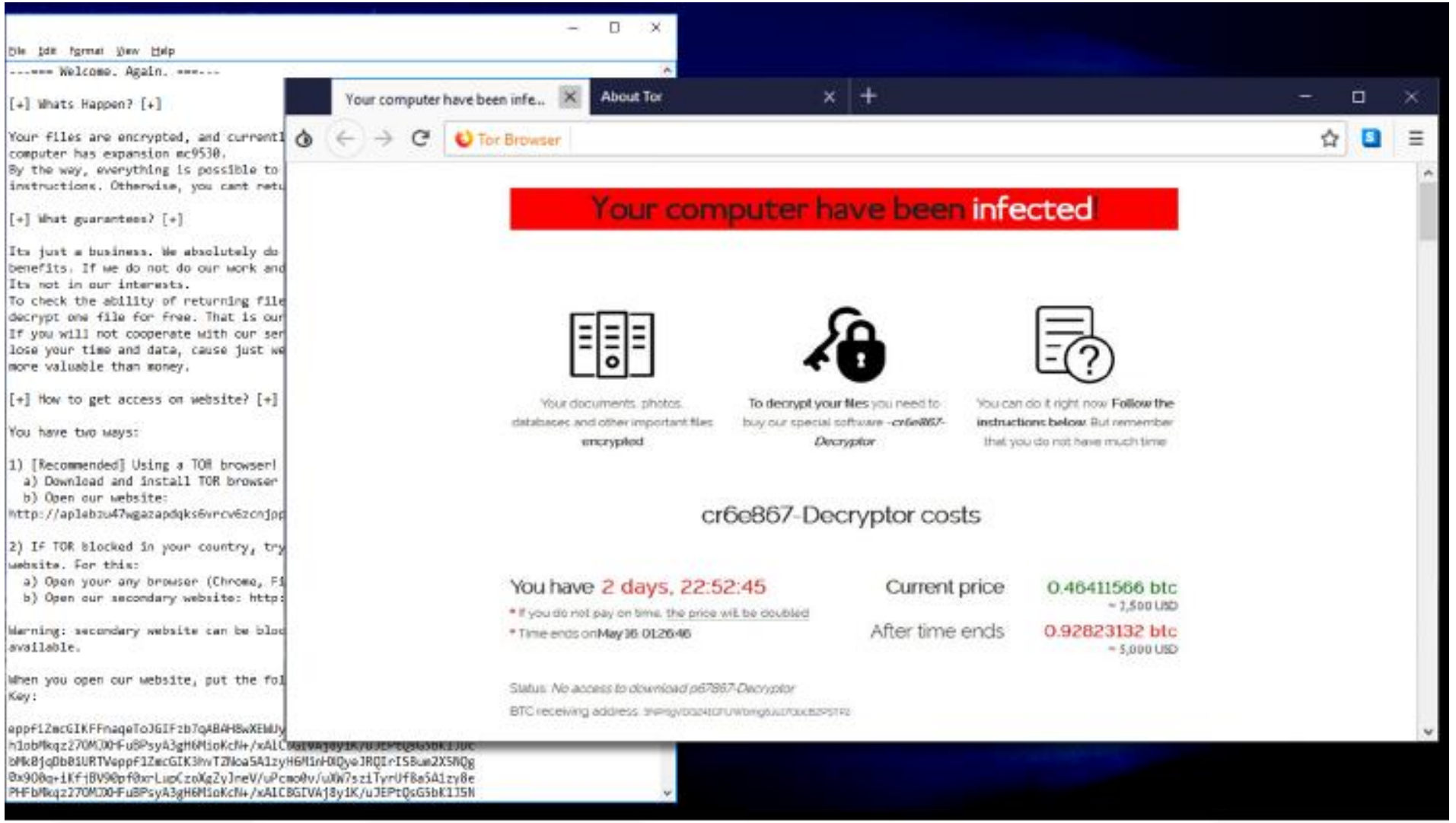
- Malicious person calls pretending to be from a trusted company
- Becoming much more common







Ransomware Example



Nuclear Ransomware

Doesn't Just Encrypt Your Files Anymore

- Steals Intellectual Property/Data
- Steals Credentials
- Threatens Victim's Employees and Customers
- Uses Your Stolen Data to Spear Phish Partners and Customers
- Publicly Shames you

Good luck having a good backup save you!

https://info.knowbe4.com/nuclear-ransomware

Multifactor Authentication (MFA)

Authentication Factors

- Something You Know
  - Password, PIN, Connect the Dots, etc.
- Something You Have
  - USB token, smartcard, RFID transmitter, dongle, etc.
- Something You Are
  - Biometrics, fingerprints, retina scan, smell
- Contextual, behavioral analytics, actions, location, etc.

Multifactor Authentication (MFA)

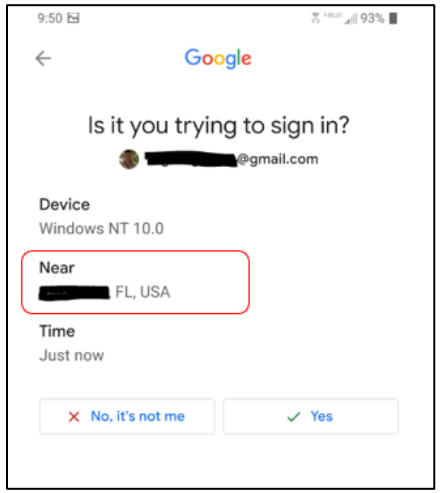
Examples

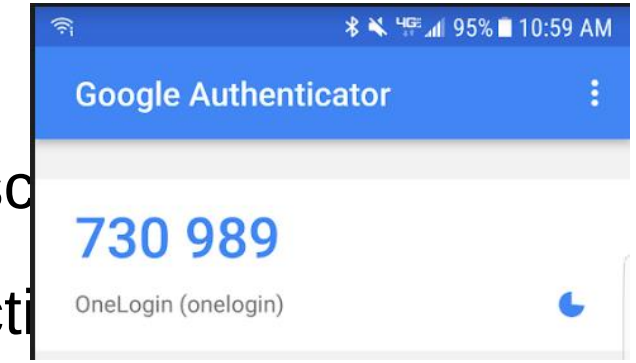
- Something You Know
- 

ne D


- USB token, smartcard, RFID transmitter, dongle, etc.
- Something You


- trics, , retina sc
- C l, behavioral analytics, acti





Multifactor Authentication (MFA) Hack

Network Session Hijacking

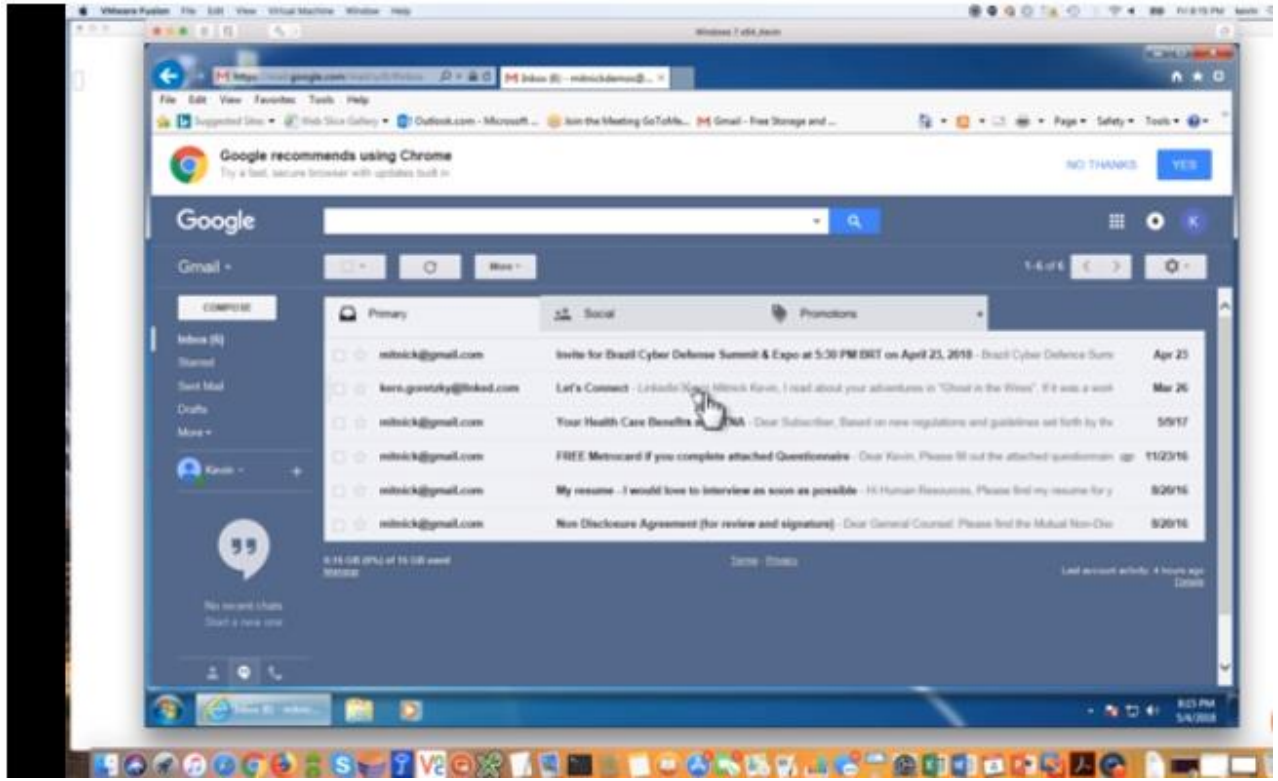
Network Session Hijacking Proxy Theft

1. Bad guy convinces victim to visit rogue (usually a look-alike) web site, which proxies input to real web site
2. Prompts victim to put in MFA credentials
3. Victim puts in credentials, which bad guy relays to real web site
4. Bad guy intercepts victim's resulting access control token
5. Bad guy logs into real site, and drops legitimate user
6. Takes control over user's account
7. Changes anything user could use to take back control

Multifactor Authentication (MFA) Hack

Network Session Hijacking

Kevin Mitnick Hack Demo



https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video

Agenda

- Why is Fighting Phishing So Important?
- Phishing Examples
- Defenses

Phishing Cannot Be Beat by Intelligence

- Anyone can fall victim to social engineering
- “Smart people” are just as likely to fall victim to phishing as anyone else
- Scammers use “stressors” to make people bypass their normal skepticism survival skills
- Whether or not someone clicks on a “phish” or falls victim to a fake phone call, has more to due with awareness of digital crime than anything else
- Once people are aware of social engineering, phishing, and all it’s forms, the less likely they are to fall victim to it

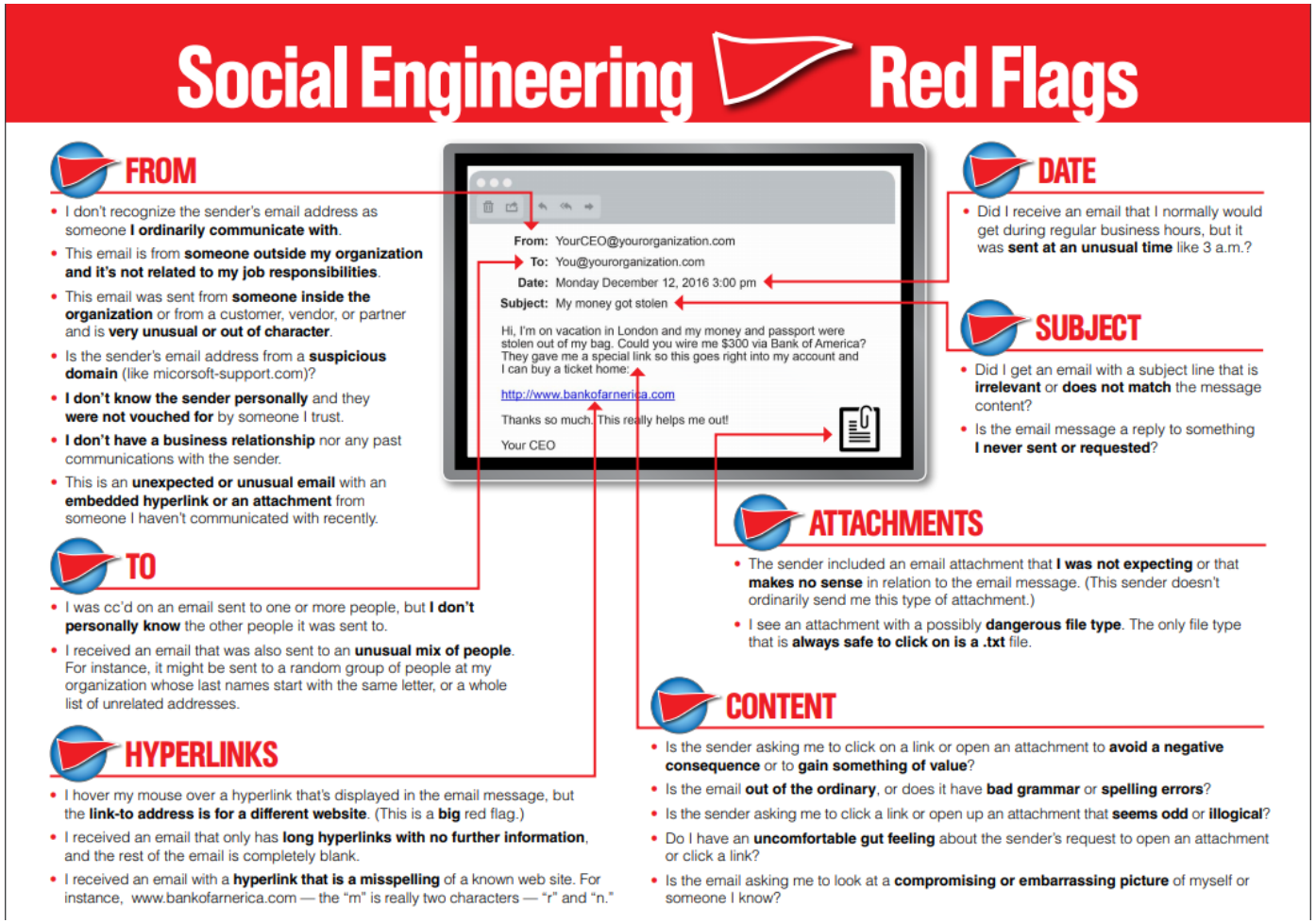
Best Defenses

Top Defenses for Most People

(in order of importance)

- **Fight Social Engineering Best You Can**
- **Patch Your software**
- **Use Multifactor authentication (MFA)/Non-Guessable passwords**
  - Use MFA where you can, where you can't
  - Use different passwords for every website and service
- **Teach Yourself How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls

Learn “Red Flags” of Social Engineering



https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees

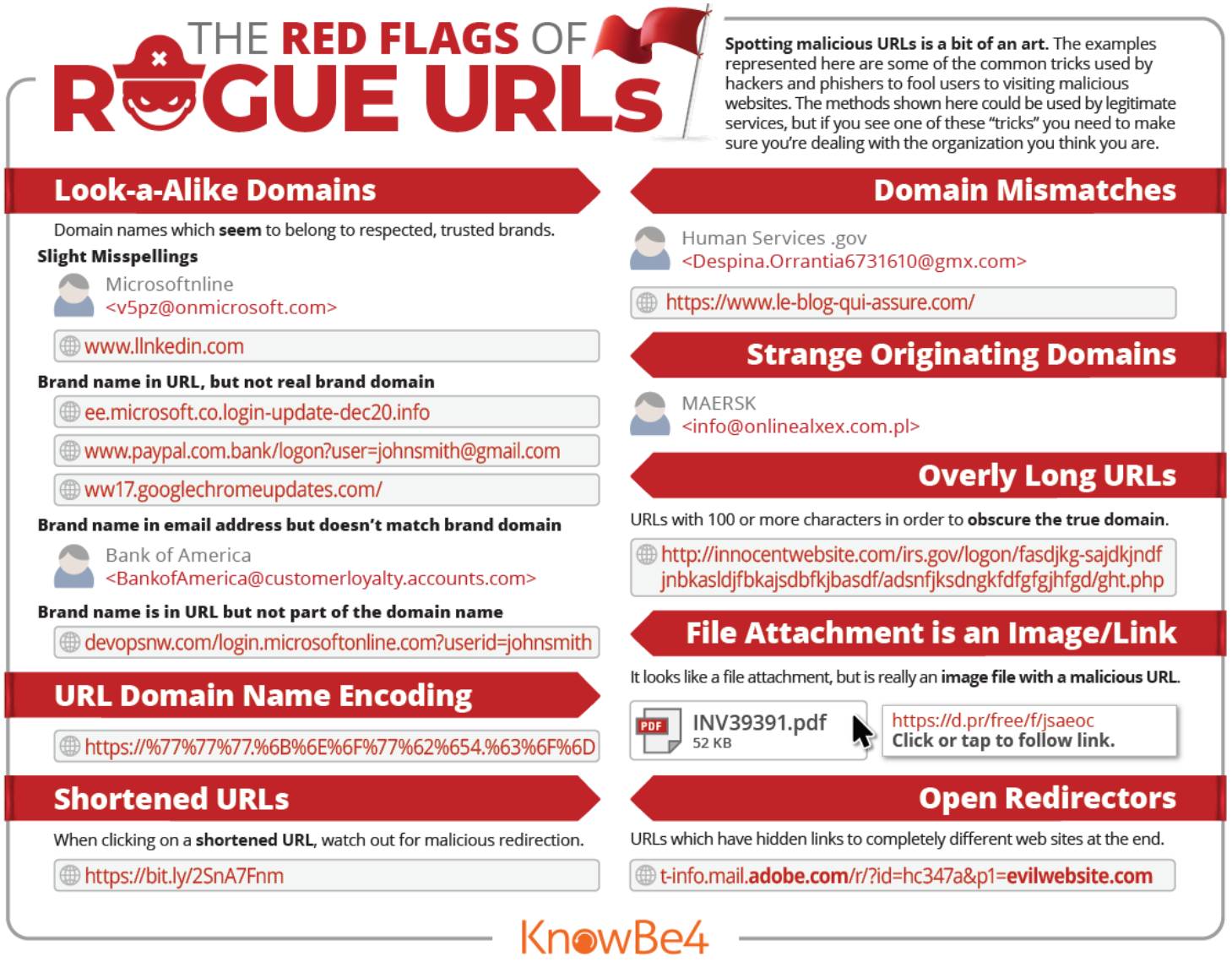
Best Defenses

How to Spot Phishing

(each symptom adds risk)

- **Email/Message/Call Arrives Unexpectedly**
- **It's asking you to do something that person or company has never asked you to do before**
- **Requested action could be harmful**
- **Tries to create a sense of urgency ("stressor") or appeals to profit/greed**
- **Contains a link or file attachment**

- **Solution: When in doubt, call person on known legitimate phone number to confirm request or visit vender website using known legitimate link**



https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

Thank You!

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
LinkedIn: www.linkedin.com/in/rogeragrimes