



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/>

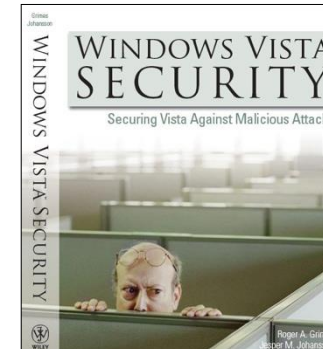
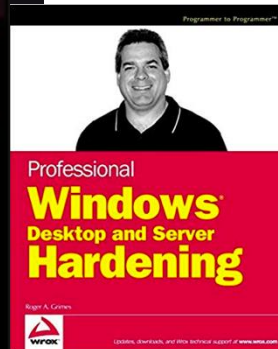
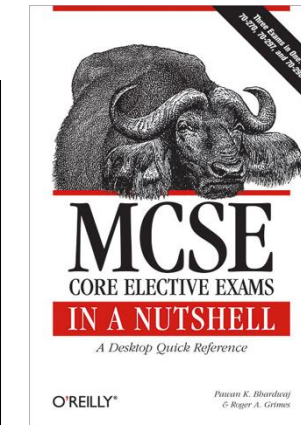
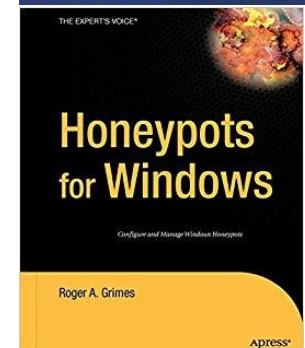
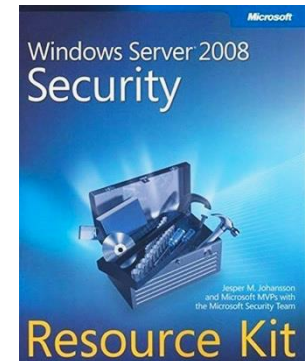
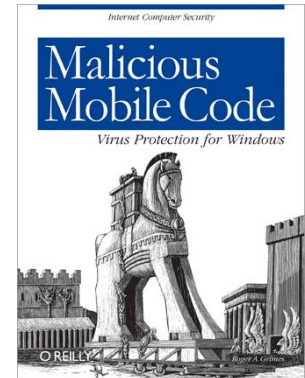
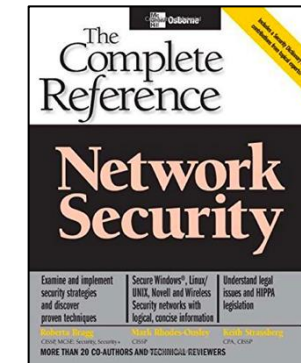
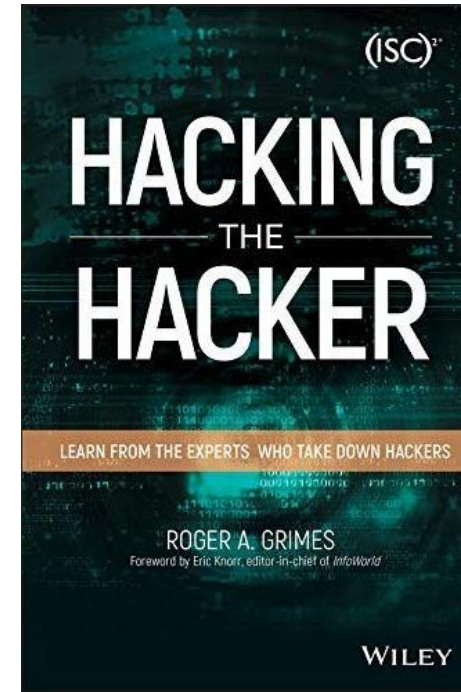
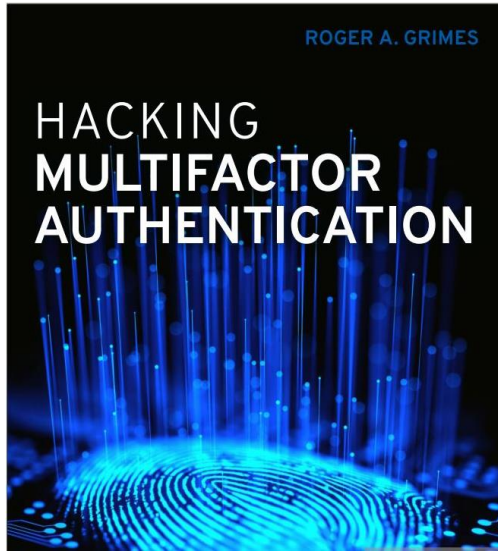
About Roger

- 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

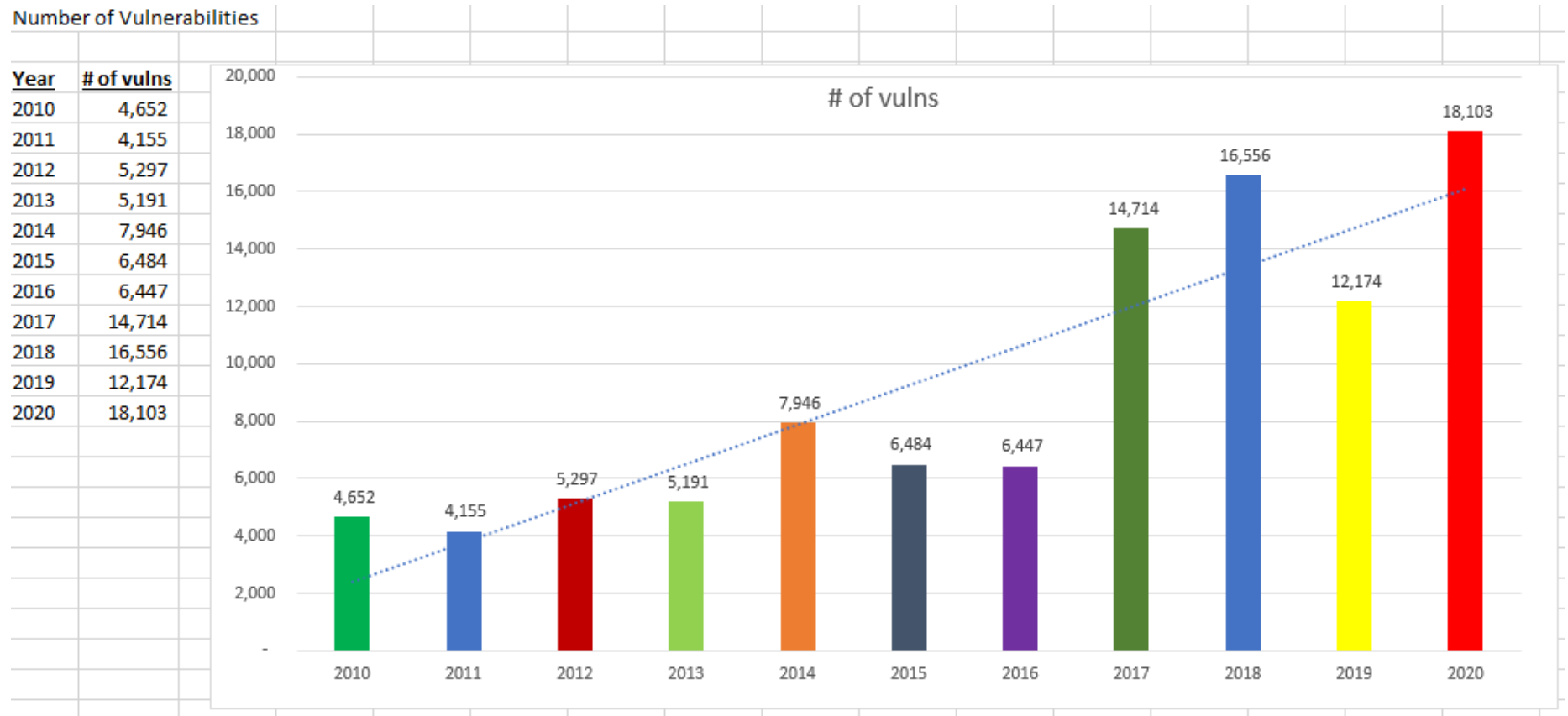
- Why is Fighting Phishing Important?
- What is Phishing?
- Security Awareness Training Best Practices

Problem – Overwhelming Number of Vulnerabilities

of Vulnerabilities

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

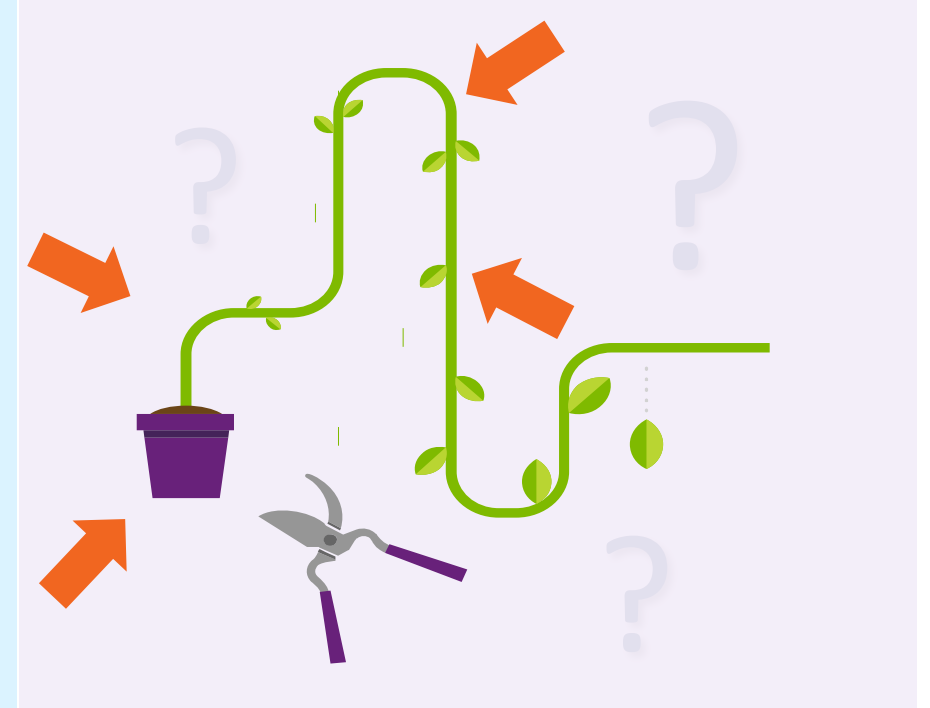
*And this is just
(known public)
vulnerabilities,
doesn't include
hackers and a
hundred million
malware
programs*



How All Hackers and Malware Break In

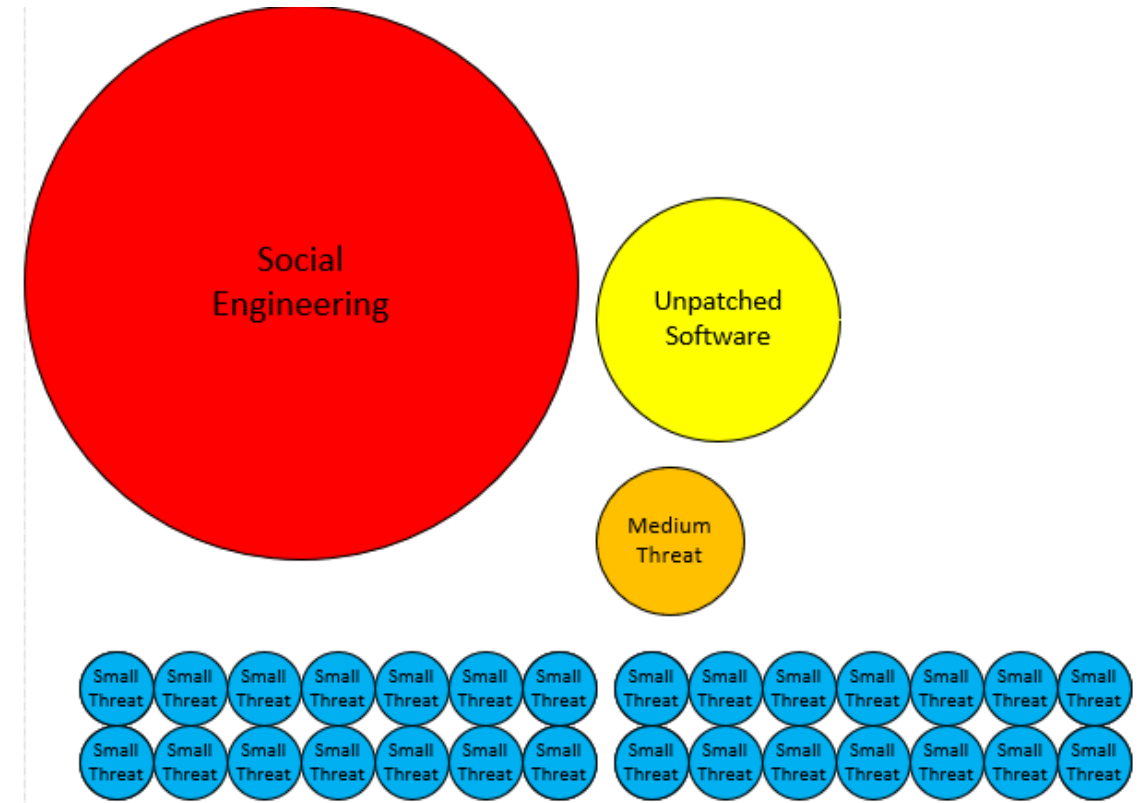
Here Are the 10 Root Exploit Methods:

- 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

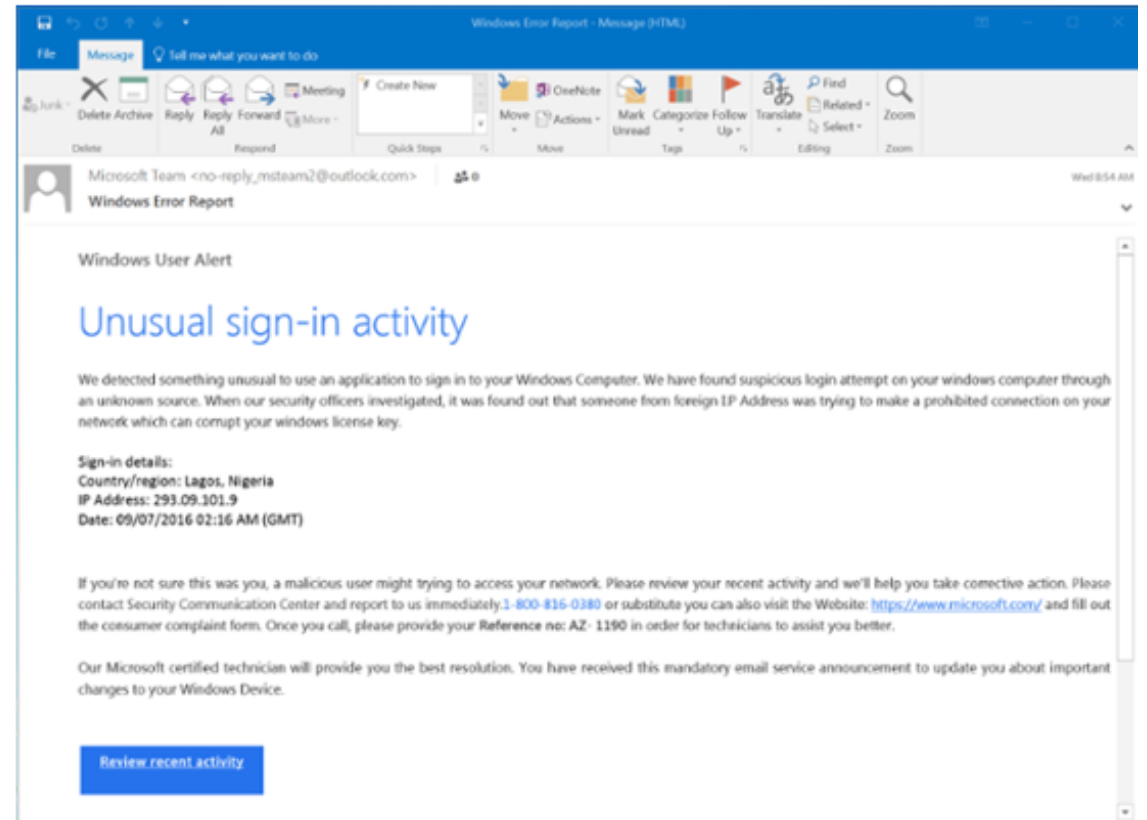
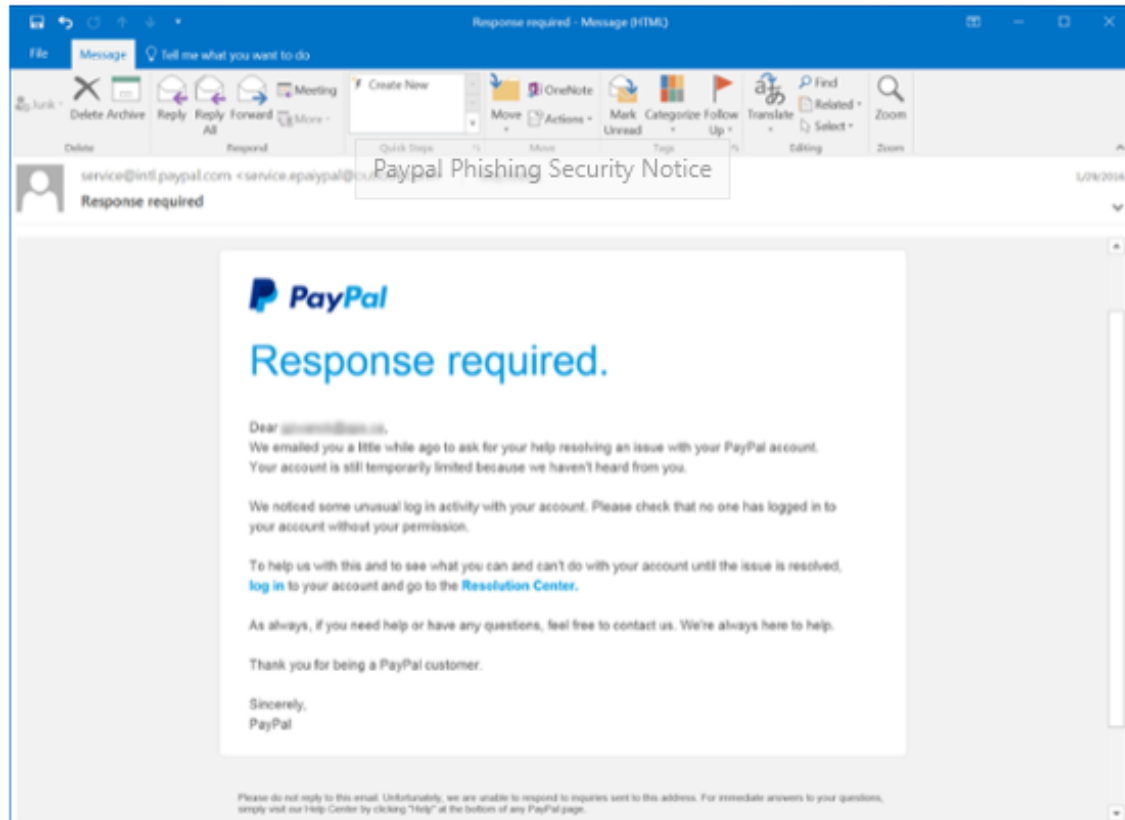
- Why is Fighting Phishing Important?
- What is Phishing?
- Security Awareness Training Best Practices

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.

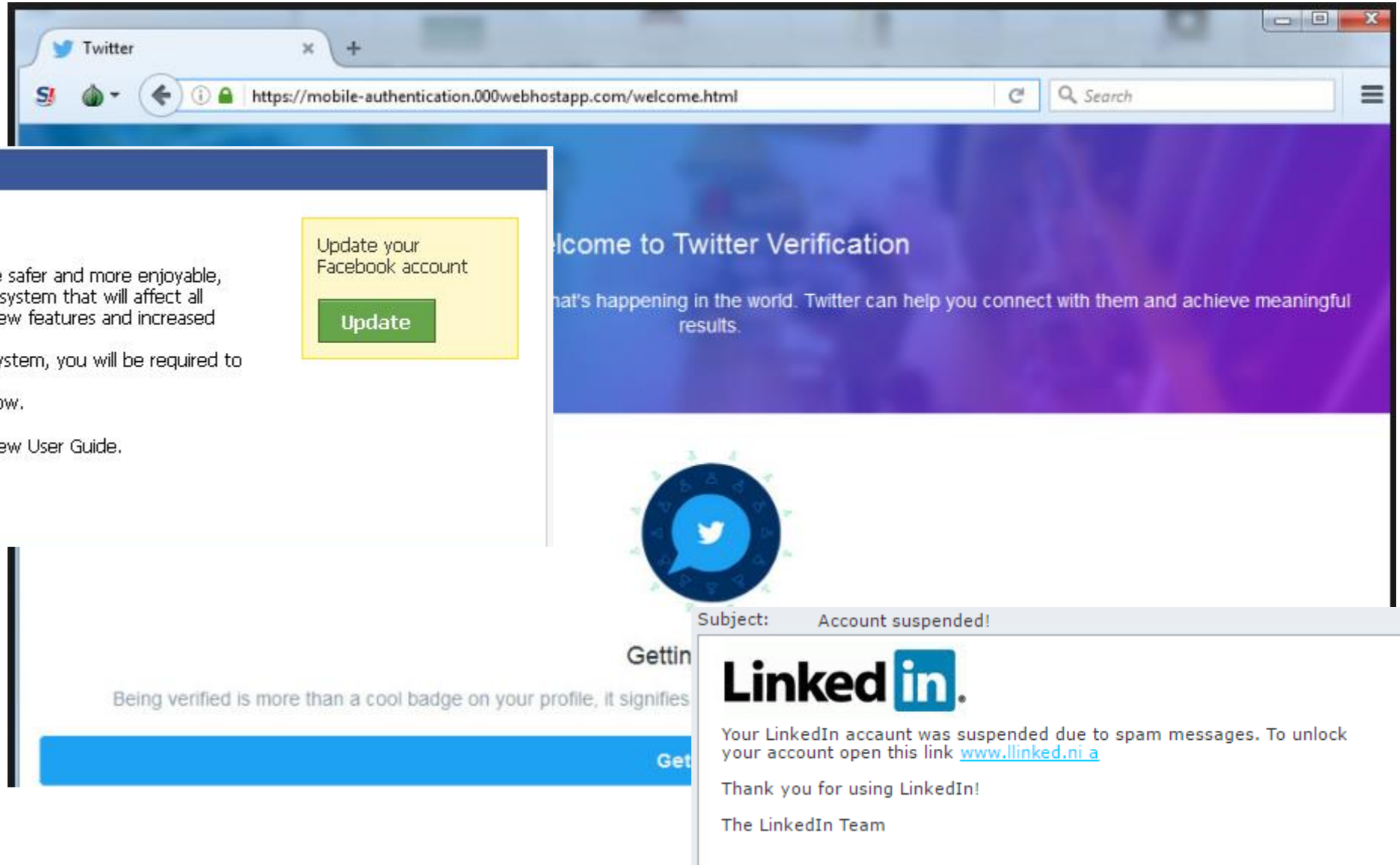
What is Phishing?

Email Examples



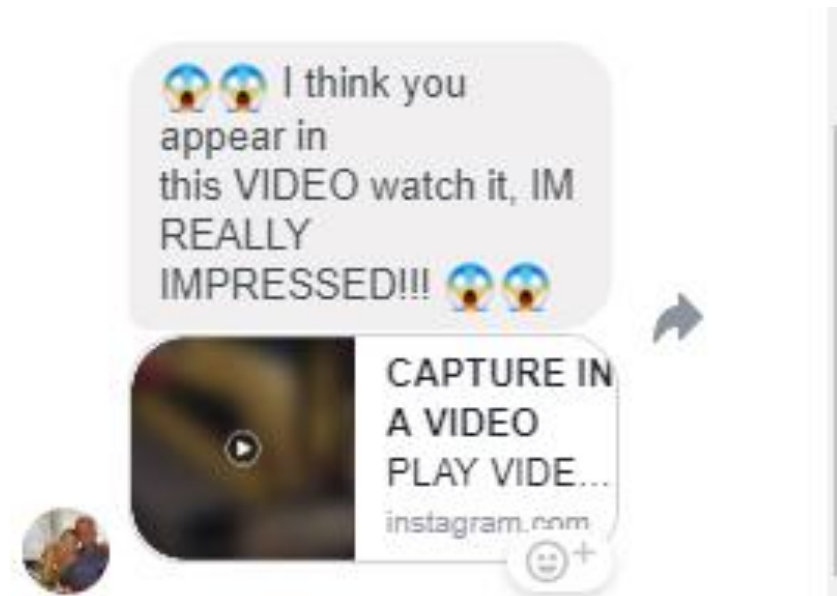
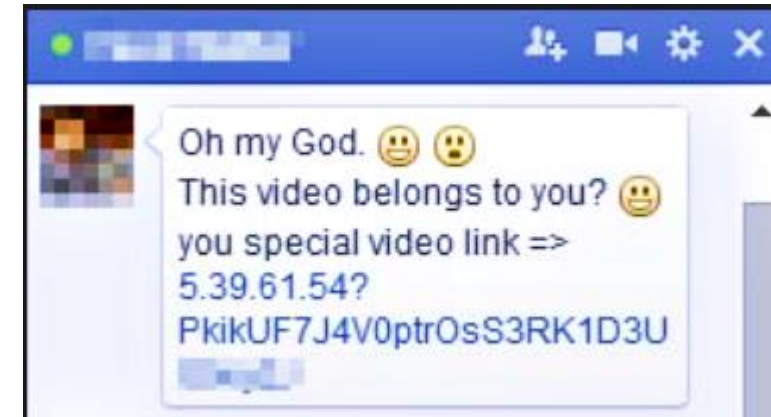
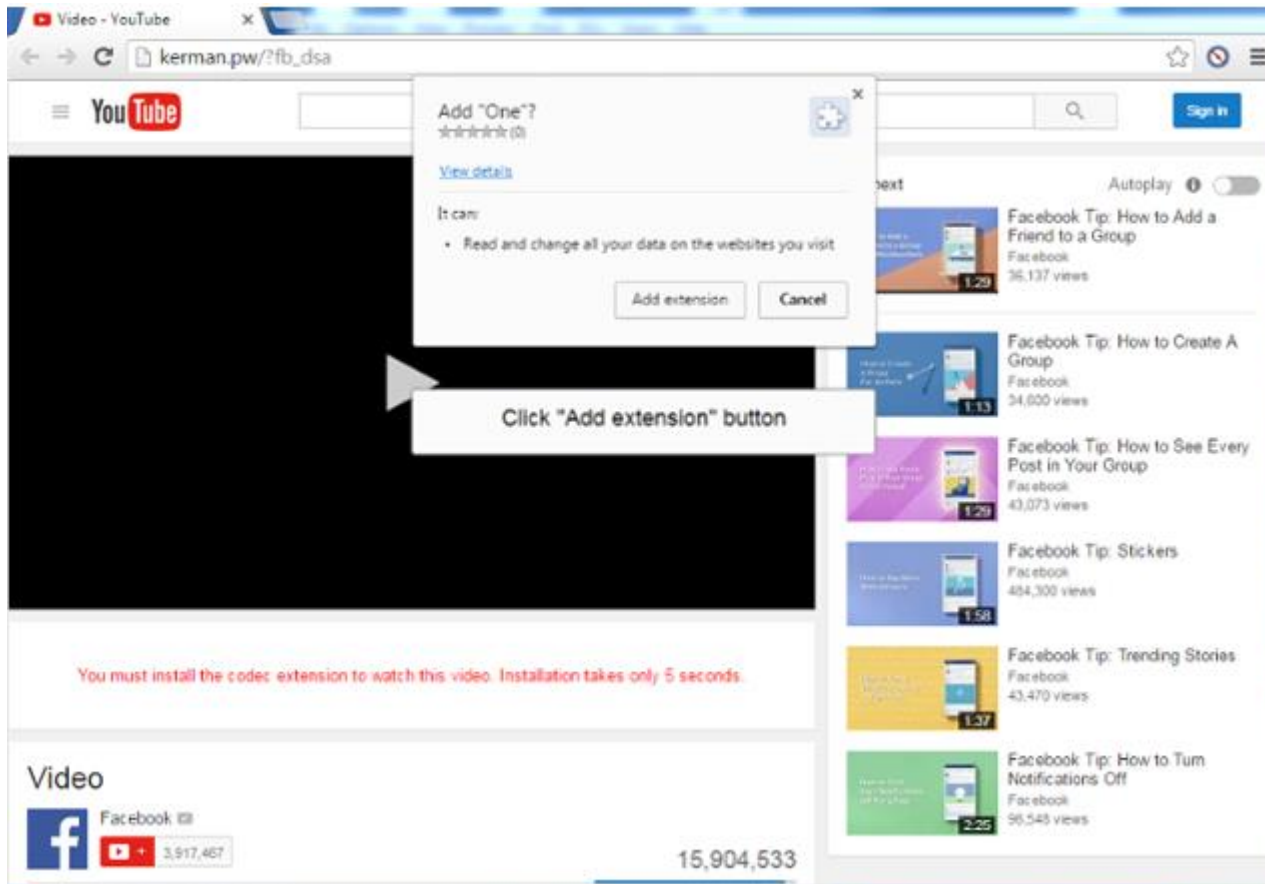
What is Phishing?

Social Media Examples



What is Phishing?

More Social Media Examples



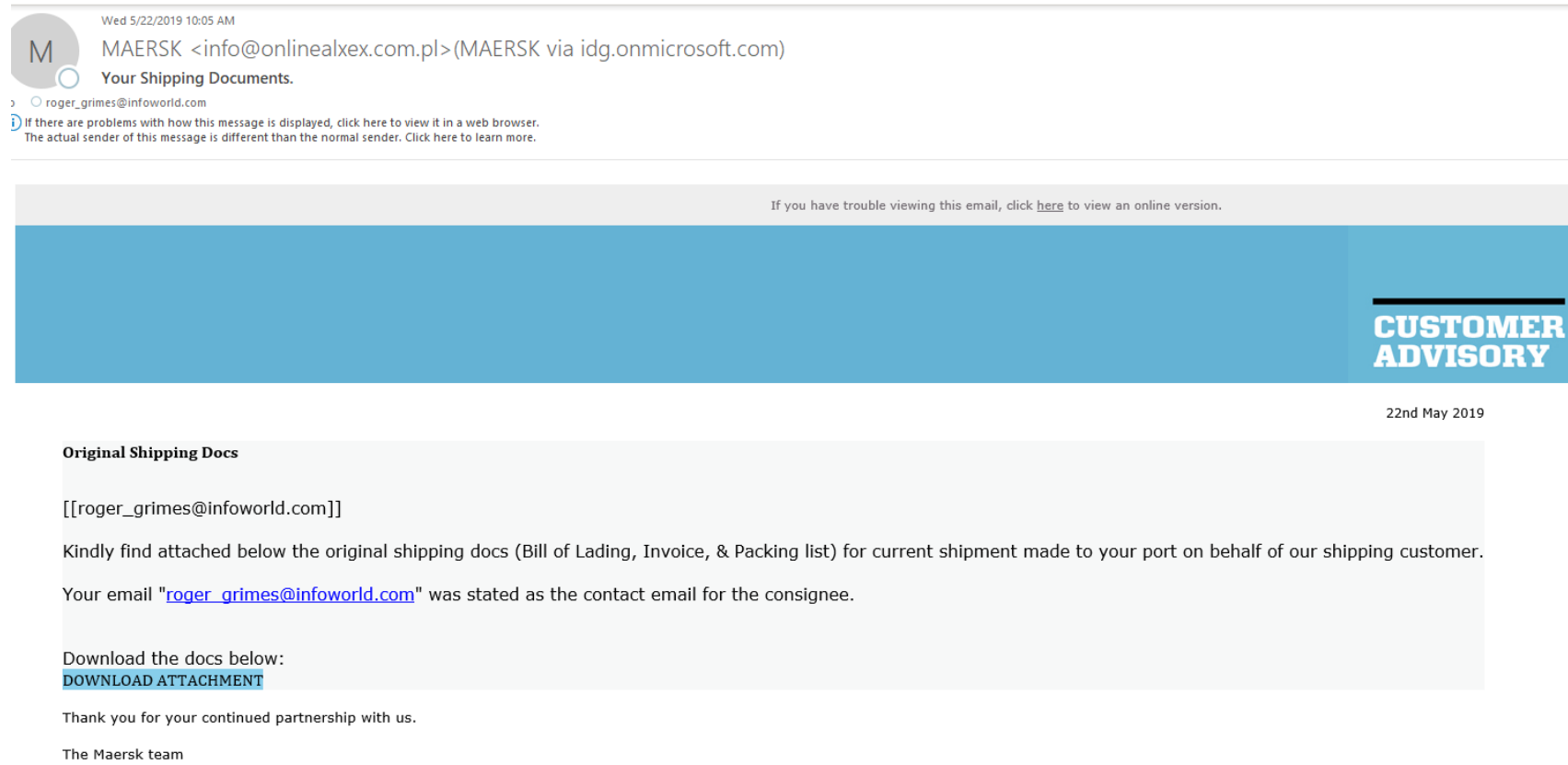
Business Email Compromise Scams

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



Business Email Compromise Scams

Spammer/Attacker/Phisher:

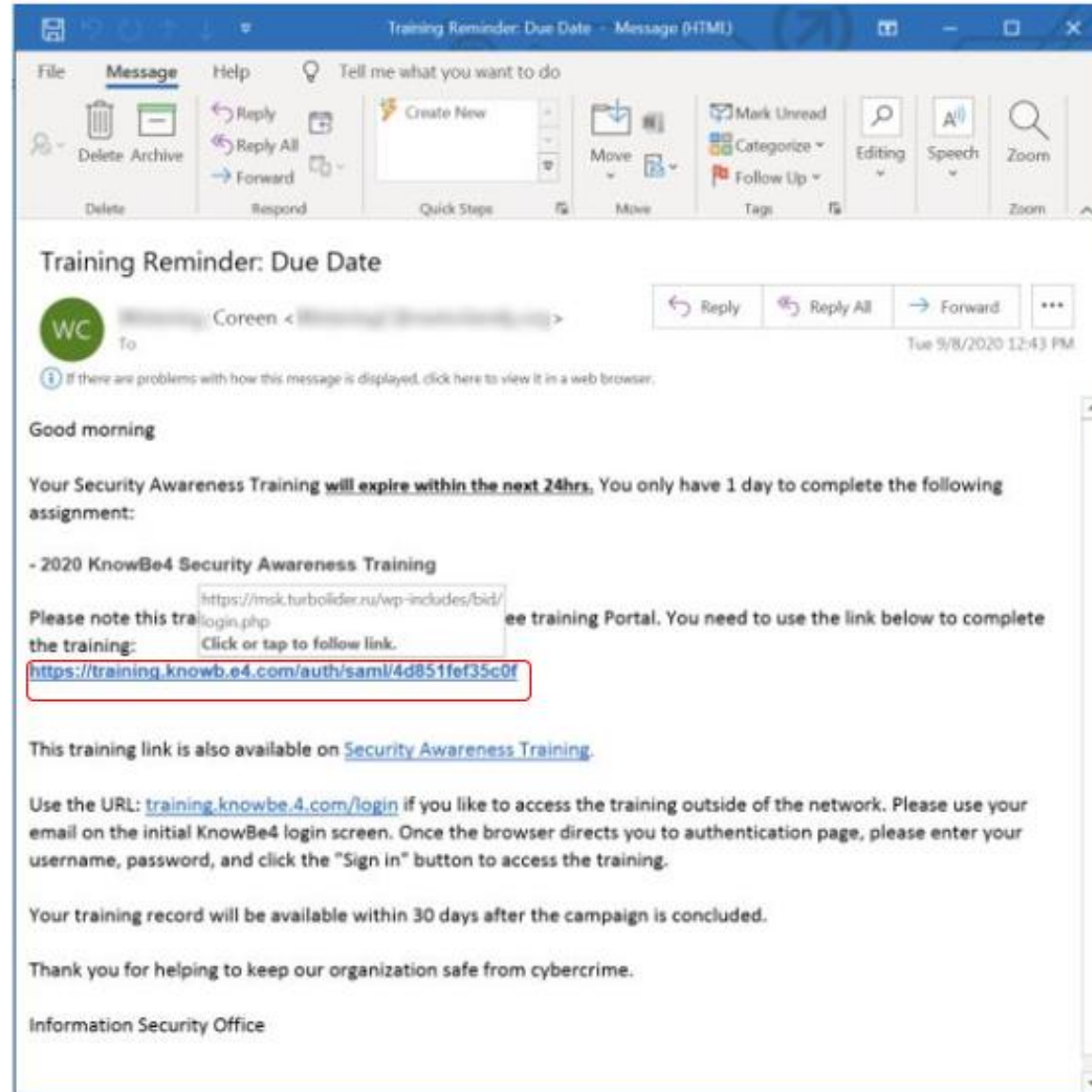
- Creates email purporting to be from boss, co-worker, invoicing company, etc.
- Can **Facebook and Google were victims of**
- Ask: **a \$100 million dollar phishing scam:**
nor **Fortune**

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!")

- Defense: Can be defeated after the company was hit by a cyber fraud that cost it 42 million euros (\$47 million).
unexpected requests for money, bill payments, etc. to be verified verbally

What is Phishing?

Sneaky Rogue URLs



COVID-Related Phishing?

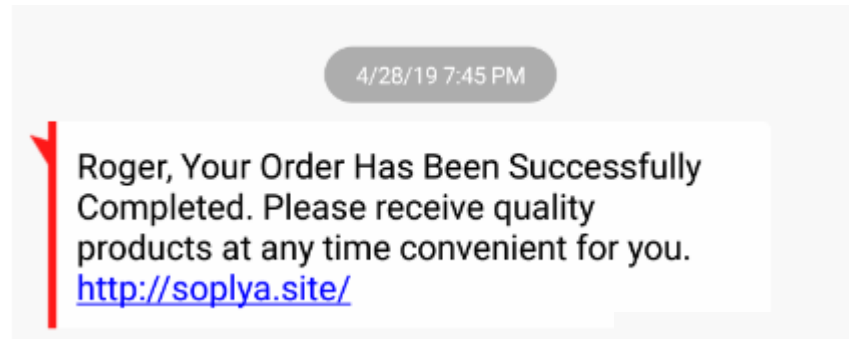
6000% Increase in Phishing Attacks Leveraging COVID-19,
Healthcare Industry Often The Target



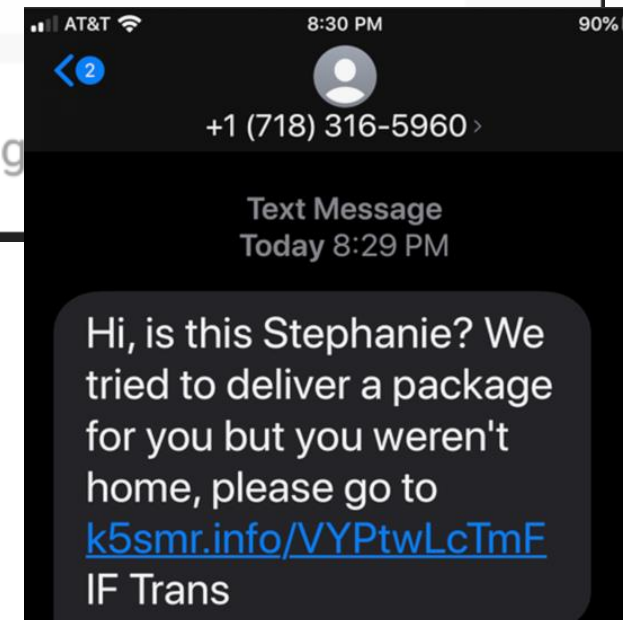
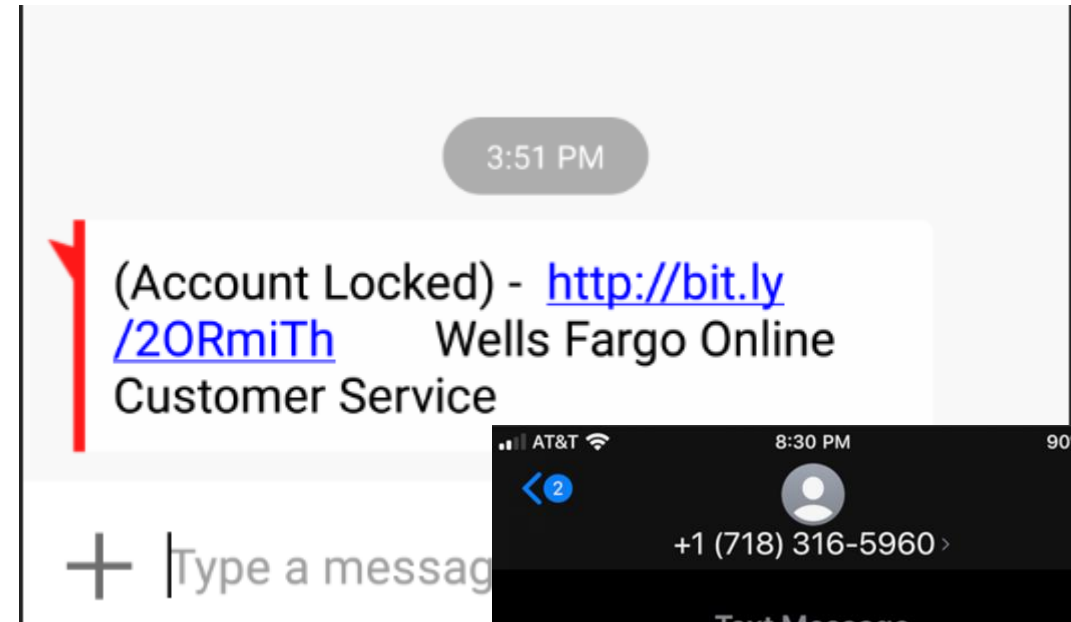
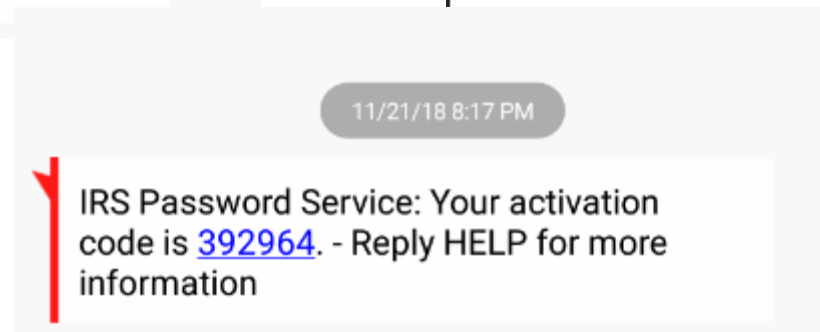
What is Smishing?

Smishing Examples

- Malicious SMS message
- Becoming very common



+19256341172 - Message id 98551 We removed the abusive content that was posted on your facebook account, visit:



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:

- Your email address and associated phone number

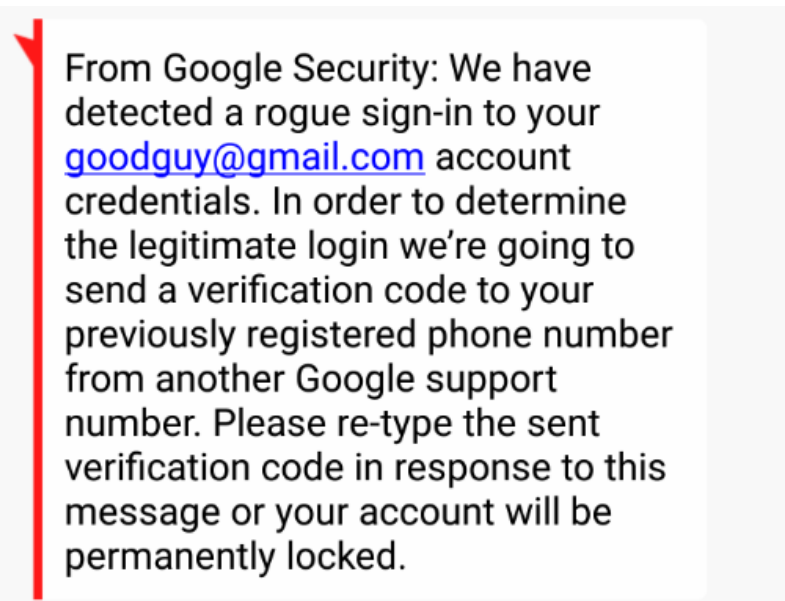
Rogue Recoveries

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 recovery

The image displays three sequential screenshots of the Google Account recovery process, illustrating a 'Rogue Recovery' method where a hacker forces an account into SMS recovery.

Screenshot 1 (Left): Shows the initial recovery screen. It features the Google logo, the text 'Hi Roger', and a dropdown menu showing the email address 'rogeragrimes@gmail.com'. Below this is a password input field with the placeholder text 'Enter your password'. At the bottom, there is a link for 'Forgot password?' and a blue 'Next' button.

Screenshot 2 (Middle): Shows the next step in the recovery process. It features the Google logo, the text 'Account recovery', and a dropdown menu showing the email address 'rogeragrimes@gmail.com'. Below this is a text input field with the placeholder text 'Enter the last password you remember using with this Google Account'. At the bottom, there is a link for 'Try another way' and a blue 'Next' button.

Screenshot 3 (Right): Shows the final step in the recovery process. It features the Google logo, the text 'Account recovery', and a dropdown menu showing the email address 'rogeragrimes@gmail.com'. Below this is a section titled 'Get a verification code' with the text 'Google will send a verification code to (...)55. Standard rates apply'. At the bottom, there are two buttons: 'Text' and 'Call', and a link for 'I don't have my phone'.

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

Your Google verification code is
[954327](#)

From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

[954327](#)

Sent

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery

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



9:45 AM

You have been enrolled in the National Weather System's Tornado Warning System.

Please reply YES or NO to accept enrollment.

Yes

Thank you. Please reply with the confirmation code just sent to confirm your phone number.

357291

Thank you. You are now protected by the NWS emergency warning system. You can stop any time by replying with STOP.

Read

You have been enrolled in Florida's COVID vaccine warning program to alert you if adverse side effects with your shot have been reported from the batch you were given.

Please reply YES or NO to accept enrollment.

We can do this
all
day

County Emergency Message:
A large water main break has been detected near your primary place of residence. Do not drink or use water from tap until further notice. We apologize for the inconvenience. Do you wish to be enrolled for proactive status updates about this event? Reply YES or NO.

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



Palm Harbor • 9 hr ago

FRAUD ALERT!!!! I received a call this afternoon from an Achieva Bank number advising me that there were attempted fraudulent transactions on my account. They knew my name and address. After talking with them for a little while they asked me for part of my card number. I told them that they should have that information and that I would have to call them back. I called the bank and they said there was no activity on my account. The caller also sent a text about charges (that I answered later that night) saying that there was no fraudulent activity on my account, to which they responded with an insulting remark. I told them too bad I didn't fall for it to which they responded with a threat. Anyway I blocked that



• 6 Sep

Scammed by alleged Duke Energy. I was called by a man saying it was in regards to my Duke energy bill. He did not ask me any personal information other than verifying my address and name. He told me that a technician was on his way to cut off my electricity and that I need to go to the store and buy two vouchers called moneypac.

I was Caught off guard and very confused. He stated I only had an hour to do this or my power would be cut-off and a re-connection fee would incur. it. Instructions for buying a voucher could be no more than \$500. He said that if a cashier asked me if this is for a bill tell them no because they charge you 16.95 for each moneypac voucher verses 5.95.

12:41 ▲

44%

← Unknown
+1 502-206-5427

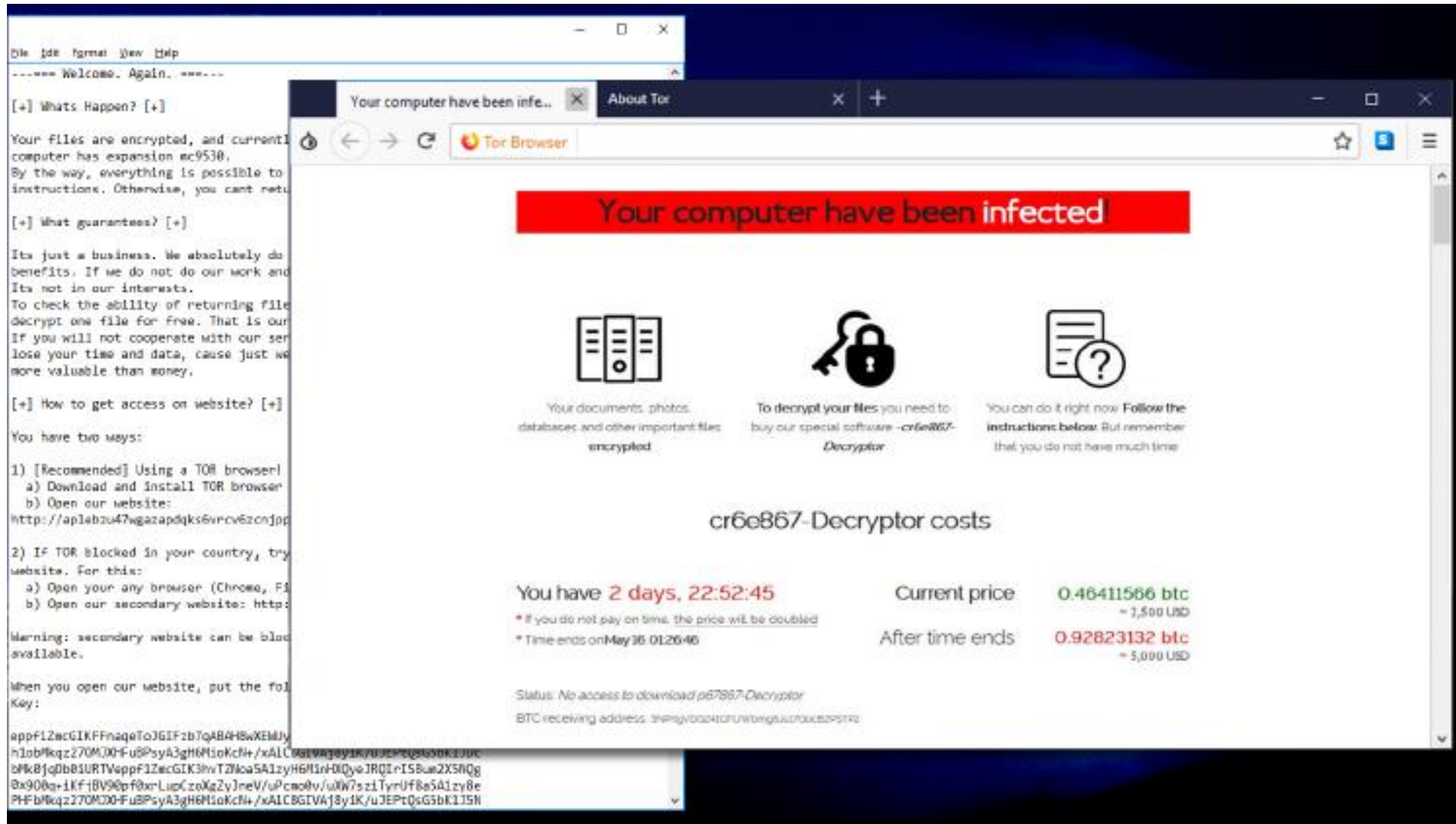


6/3, 12:25 PM Today

Yes this is Karen Stewart. I'm calling in reference to your federal student loan. I do need to discuss your repayment options with some new changes that are taking effect recently so if you could please be sure to just give me a call back my number is [866-264-5225](tel:866-264-5225) and I'm gonna go ahead and give you a reference number if you would just have this handy when you call back it makes things a lot easier. Your reference number is 022206. Thank you.



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



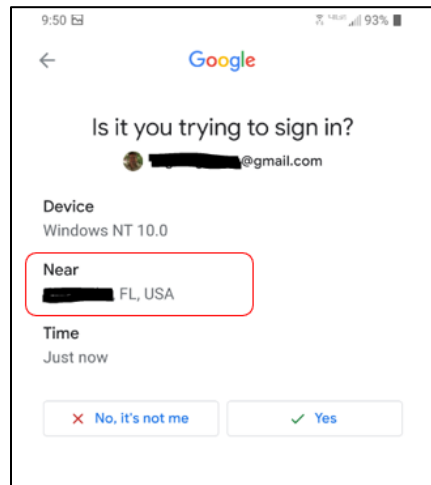
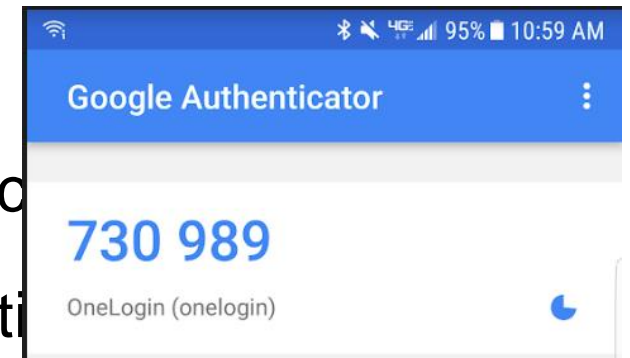
- USB token, smartcard, RFID transmitter, dongle, etc.

- Something You



- Biometrics, , retina scan

- Continuous authentication, behavioral analytics, active



Multifactor Authentication (MFA) Hack

Network Session Hijacking

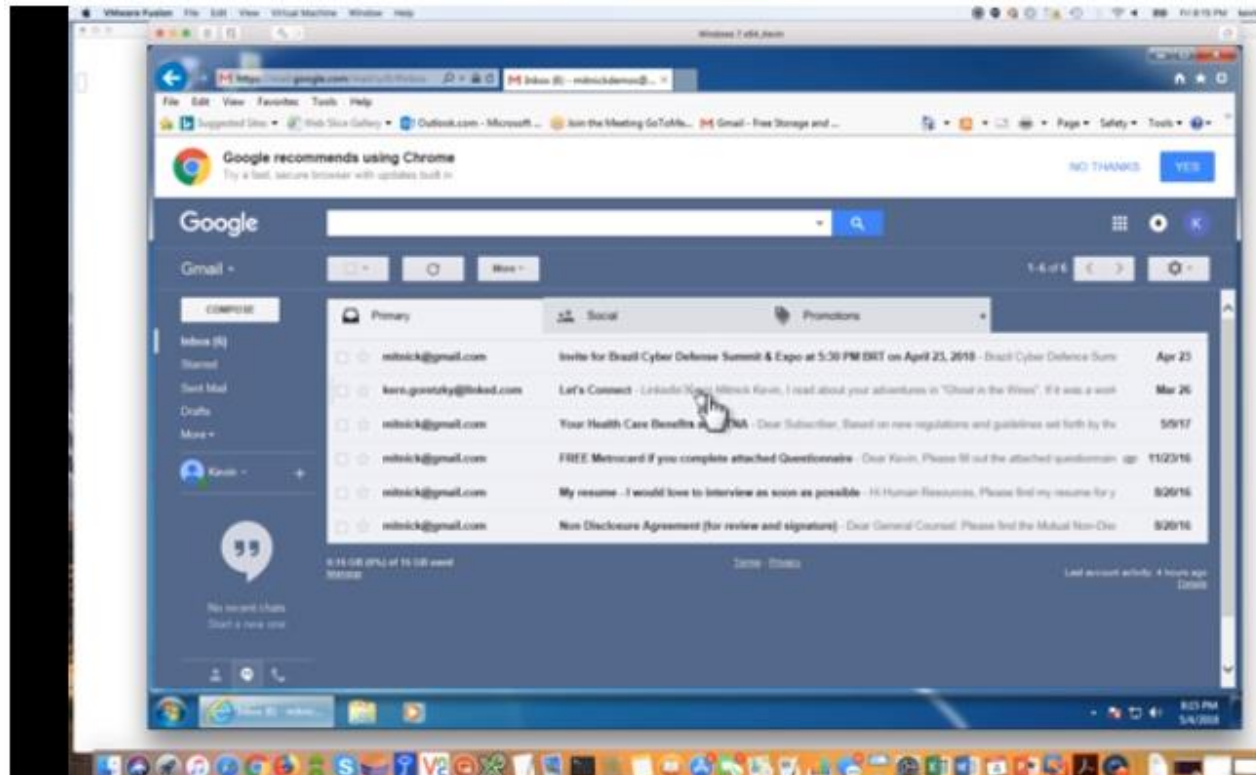
Network Session Hijacking Proxy Theft

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

Kevin Mitnick Hack Demo

Network Session Hijacking



<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 do with awareness of digital crime than anything else
- Once people are aware of social engineering, phishing, and all its forms, the less likely they are to fall victim to it

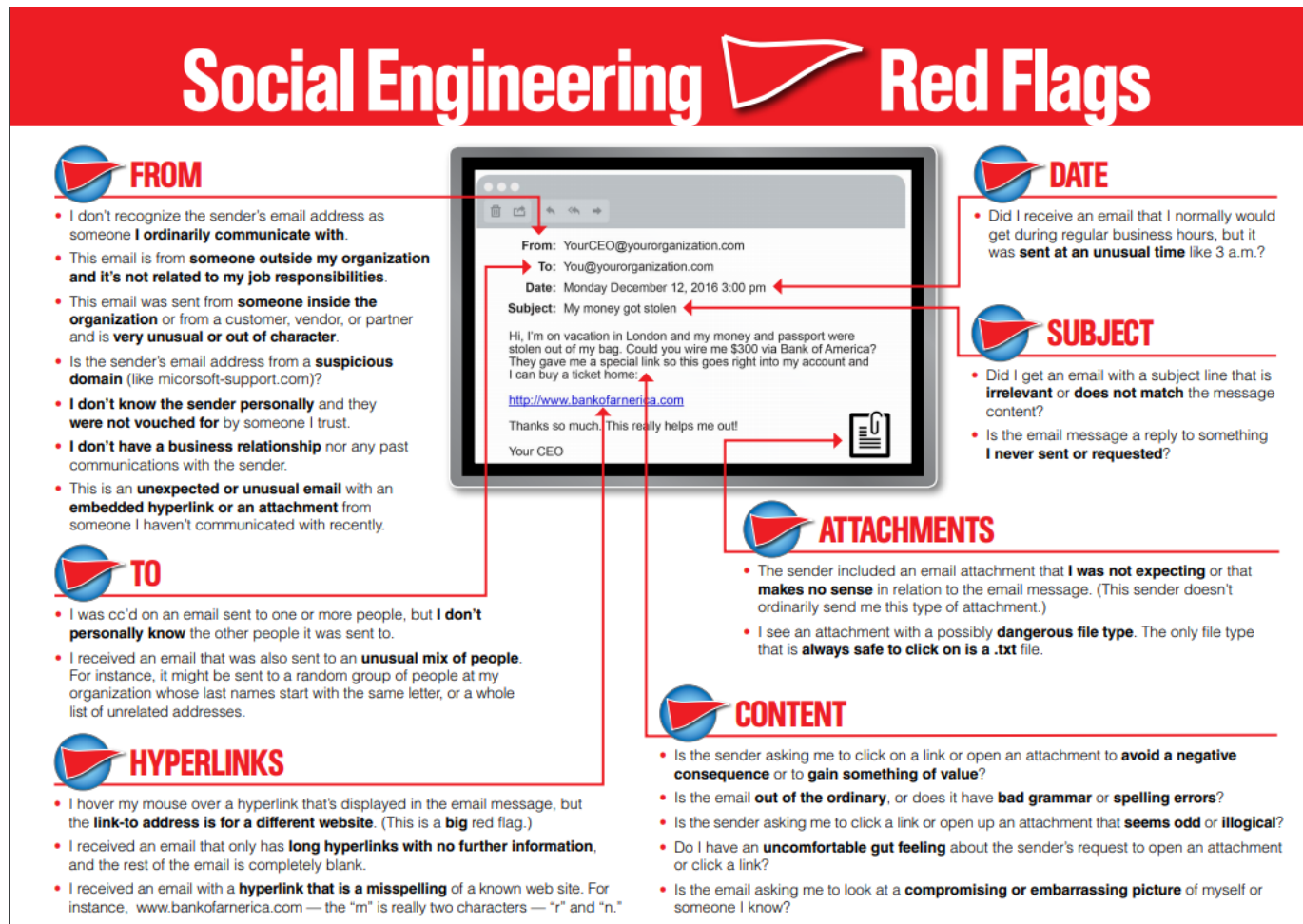
Best Defenses

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**

THE RED FLAGS OF ROGUE URLS

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

 Microsoftonline
<v5pz@onmicrosoft.com>

 www.llnkedin.com

Brand name in URL, but not real brand domain

 ee.microsoft.co.login-update-dec20.info

 www.paypal.com.bank/logon?user=johnsmith@gmail.com

 ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

 Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

 devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

 <https://%77%77%77%6B%6E%6F%77%62%65%63%6F%6D>

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

 <https://bit.ly/2SnA7Fnrm>

Domain Mismatches

 Human Services .gov
<Despina.Orrantia6731610@gmx.com>

 <https://www.le-blog-qui-assure.com/>

Strange Originating Domains

 MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

 <http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndfjnbkasldjfbkajdsbfkjbasdf/adsnfjksdngkfdgfgjhfgd/ght.php>

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.

 INV39391.pdf 52 KB <https://d.pr/free/f/jsaeoc>
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

 t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

KnowBe4

<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](https://twitter.com/rogeragrimes)

LinkedIn: www.linkedin.com/in/rogeragrimes