How and Why Hackers Hack

Your Best Practice Defenses

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

About Roger

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

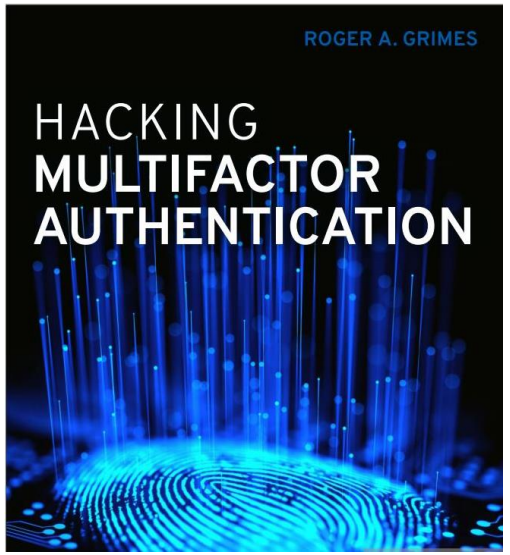
e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

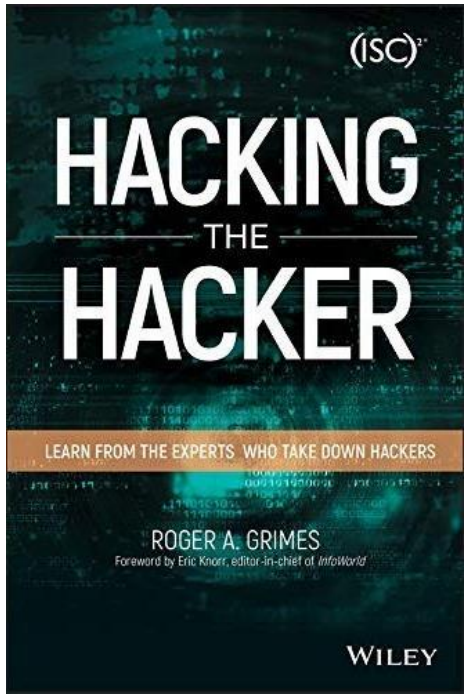
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 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)

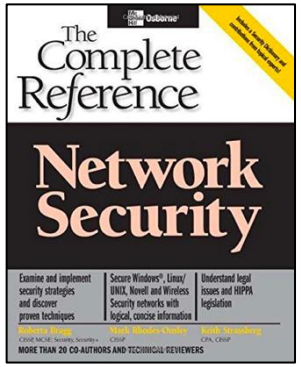
Certification exams passed include:

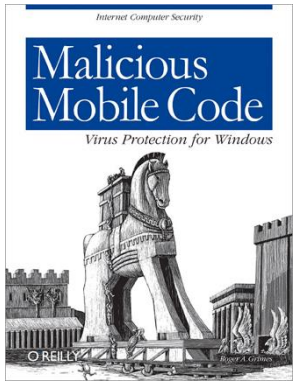
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

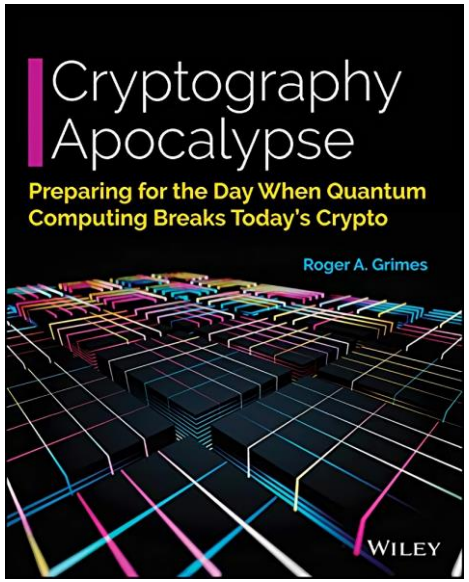
Roger's Books

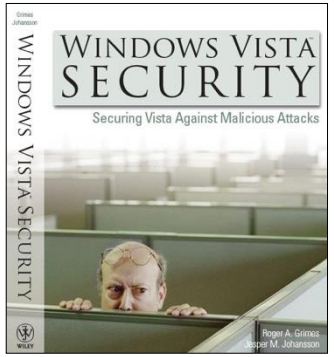


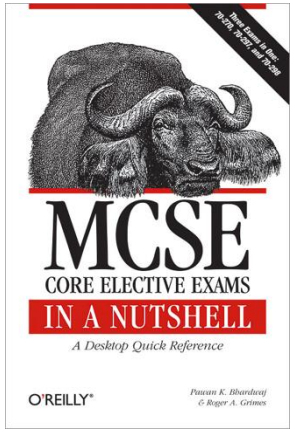


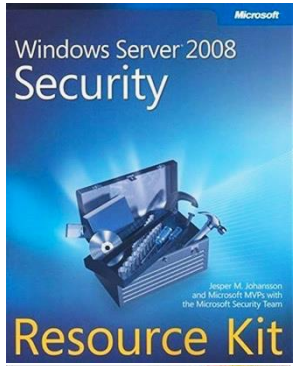


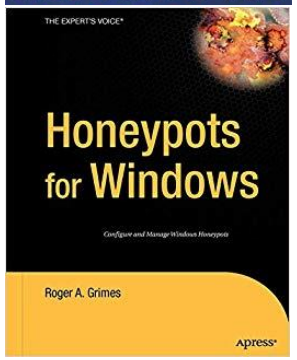












About Us

- 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

- How and Why Hackers Hack
- Why is Fighting Phishing Important?
- Best Practice Defenses

Agenda

- How and Why Hackers Hack
- Why is Fighting Phishing Important?
- Best Practice Defenses

Why Hackers Hack You

Your Org Was a:

- Victim of opportunity (random)
- Targeted (human adversary involved from the start)

- Victims of opportunity attacks are far more common

Why Hackers Hack

Financially-Motivated

Does whatever it takes to get money

- Robs your bank account, identity theft, account take over (ATO)
- Phishing
- Ransomware
- DDOS/Extortion
- Carders

Vast majority of hackers are this type

Why Hackers Hack

Nation State Attackers

- Looking for information or money to benefit their country
- Sabotage a country's military or civilian infrastructure
- Destabilize an opponent country, sow doubt
- Can't arrest or easily stop nation-state hackers
- Right now if they can get away with it they will do it
- Stuxnet discovered in 2010 was a major milestone in cyberwarfare

Why Hackers Hack

Corporate Espionage

Corporate spies

- Looking for information and intellectual property
- May be intentional, by a competitor
- May be for nation state
- May be a victim of opportunity scenario

Why Hackers Hack

Insider Attack

- Usually for financial gain

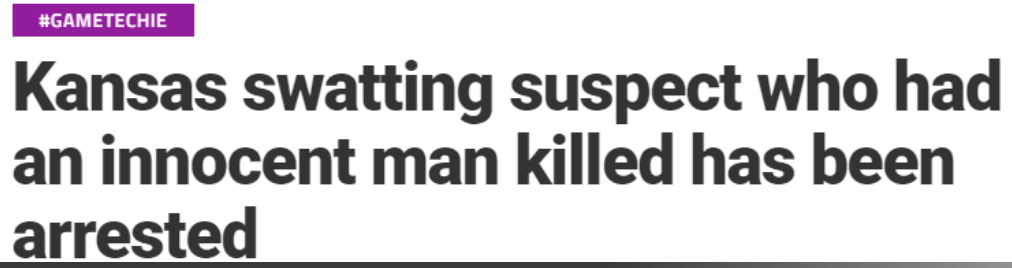
- May be for a competitor
- May be for nation state
- May be revenge

Why Hackers Hack

Gamers

Looking to unethically advance themselves in a game or punish competitors

- Get a competitive advantage
- Steal gaming credits from others
  - Can be charged with financial theft
- Denial of service attacks against competitors
- Swatting attacks
  - People have been shot and died



Why Hackers Hack

Computer Resource Theft

Want to use your computer's resources for free

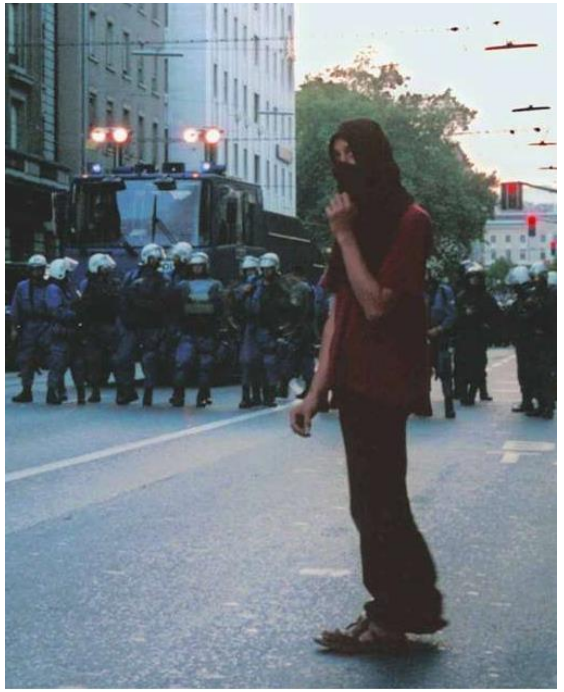
- Bots and botnets
- Used as malware servers
- DDoS
- Bitcoin miners
- SETI

Why Hackers Hack

Hacktivists

Want to harm your organization to promote their objectives

- DoS
- Financial Harm
- Public Embarrassment
- Doxxing
- Anonymous hacking group
- Anti-Child Abuse Activists
- Anti-Child Porn Activists



Why Hackers Hack

Adware

Want to redirect your computer resources or browser to promote their hired advertising objectives

- Will maliciously manipulate your browser or OS
- Add malicious add-on to your browser
- Modify your hosts

- Need to be worried about this as much as more serious threats because how it exploited host is the same way the other types of hacking can exploit the host

Why Hackers Hack

Hobbyist

Solely motivated to show they can hack something

- Used to be the biggest group of hackers; now a minority group
- Actively look for vulnerabilities
- Can be white hat (only legal hacking) or black hat (only illegal hacking)
- Often active looker for victims of opportunity
- Known as “script kiddies” if all they do is use other hacker’s tools to do bad things

Why Hackers Hack

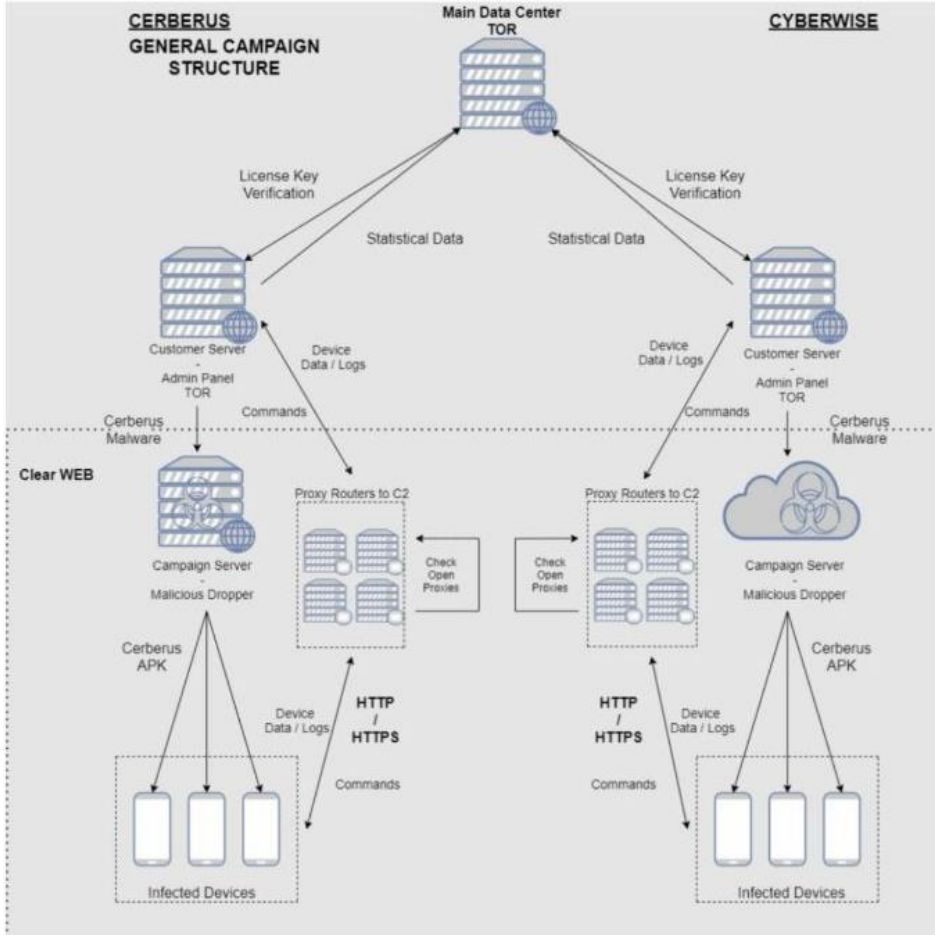
Corporation/Gang

It's the day job for a lot of hackers

- We see less activity during a hacker's country's weekends and holidays
- Some hacker companies have even been traded on their stock exchange
- Some pay a "fee" to their country's "anti-hacking" organization as sort of an unofficial bribe for their country to look the other way
- We sometimes arrest foreign-country hackers when they go on holiday to a country that accepts our subpoenas
- We sometimes set up fake jobs in countries that accept or subpoenas so we can arrest them

Why Hackers Hack

Cerberus Banking Trojan logical network diagram



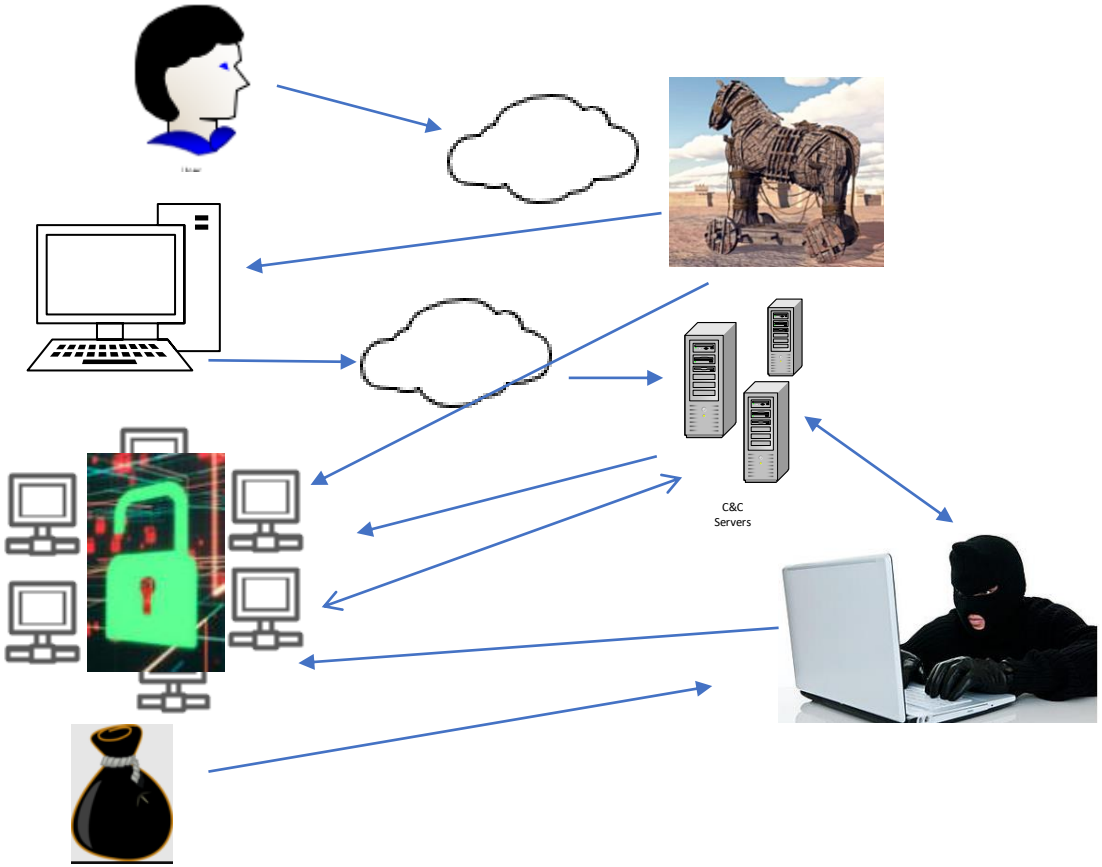
How Hackers Hack You

One of Three Ways

- Automated Malware
- Human Adversary
- Hybrid
  - Initial access was malware
  - Malware “dials home”
  - Human adversary takes over

Attacker Workflow

Today's Attacker Workflow



1. Victim tricked into executing "stager" trojan horse program, modifies host system
2. After executing, it immediately downloads updates and additional malware & instructions from C&C servers
3. Updates itself to keep ahead of AV/EDR detection, new payloads, spreads
4. Collects as many passwords as it can
5. Notifies C&C/hacker about new intrusion
6. Dwells (sometimes up to 8 to 12 months)
7. Hackers come in, assess and analyze target
8. Steal whatever they want
9. Launch encryption and ask for ransom

More Malicious Ransomware

Today's Ransomware Summary

- Steals Intellectual Property/Data
- Steals Every Credential It Can – Business, Employee, Personal, Customer
- Threatens Victim's Employees and Customers
- Uses Stolen Data to Spear Phish Partners and Customers
- Does Public Shaming

Good luck having a good backup save you!

1-hour webinar on this subject: https://info.knowbe4.com/nuclear-ransomware

More Malicious Ransomware

Today's Ransomware Summary

- Threats to exfiltrate data are over 80% of all ransomware attacks now

81% of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+5% From Q1 2021)

Despite the prevalence of the tactic, fewer organizations that are JUST facing a data exfiltration threat (i.e. they are not concerned or impacted by encrypted files or data loss) are opting to pay a ransom. In 2020, almost 65% of victims that were just faced with a data leak threat opted to pay, despite the reality that paying to suppress a leak provides almost zero value. In Q2, only 50% of data leak victims opted to pay. We hope to see this trend continue until the percentage reaches zero. We feel very strongly that mandatory federal reporting of a ransom payment will have a positive material impact on this as well. Mandatory reporting may not seem like a major forcing function, but piercing the veil of disclosure will tilt the mindset of decision makers further away from making this specific kind of payment.

https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

Agenda

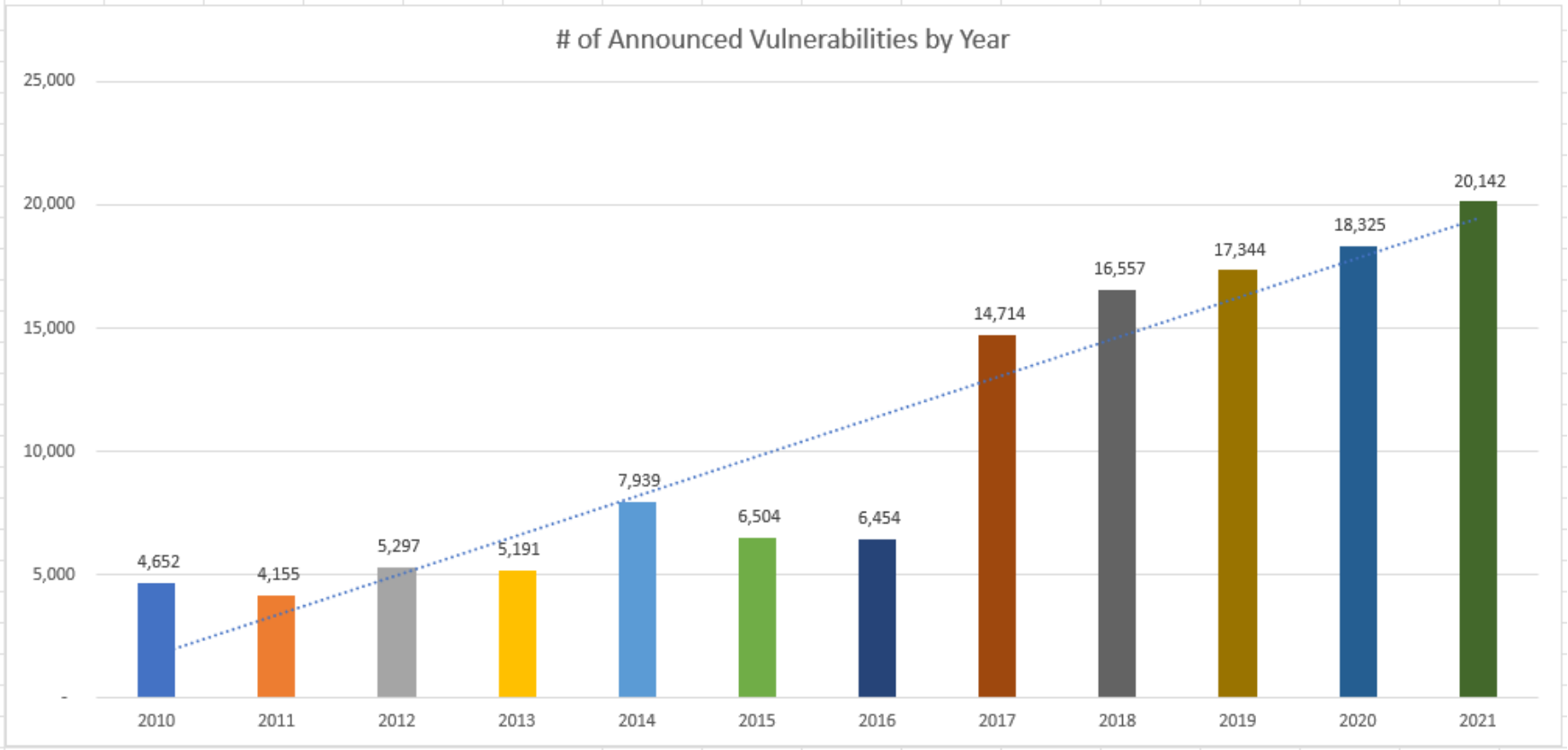
- How and Why Hackers Hack
- Why is Fighting Phishing Important?
- Best Practice Defenses

Problem – Overwhelming Number of Vulnerabilities

# of Vulnerabilities

- Avg: 4K-20K+ new threats/year
- 11-55/day, day after day

Year	# of vulns
2010	4,652
2011	4,155
2012	5,297
2013	5,191
2014	7,939
2015	6,504
2016	6,454
2017	14,714
2018	16,557
2019	17,344
2020	18,325
2021	20,142

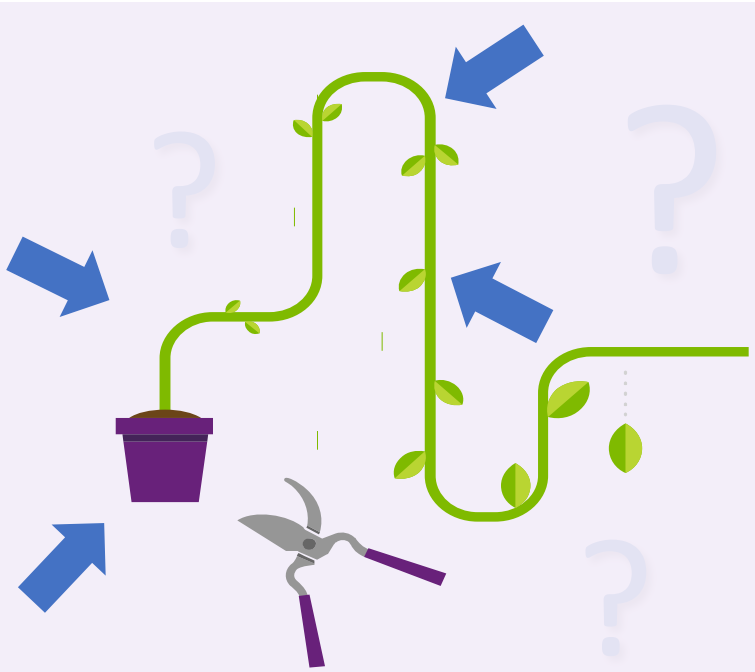


Source: https://www.cvedetails.com/browse-by-date.php

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

Initial Root Access Exploit Methods

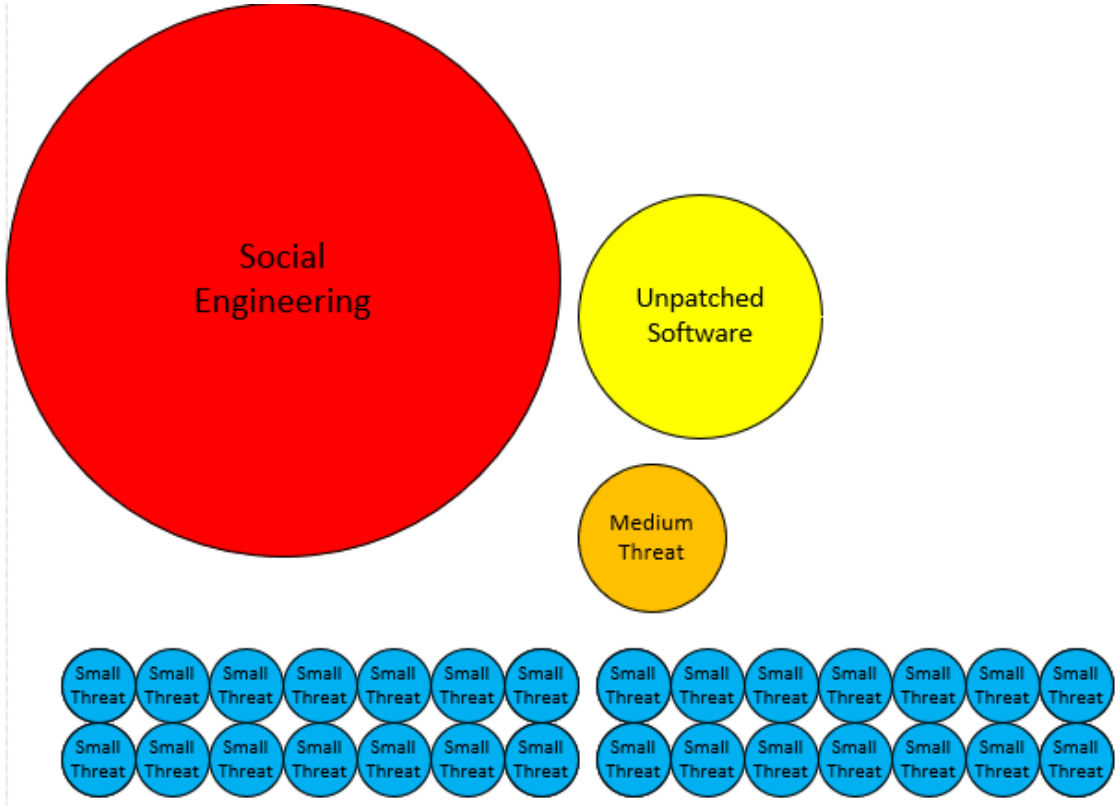
- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Data Malformation
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don't trust me,

measure your own risk

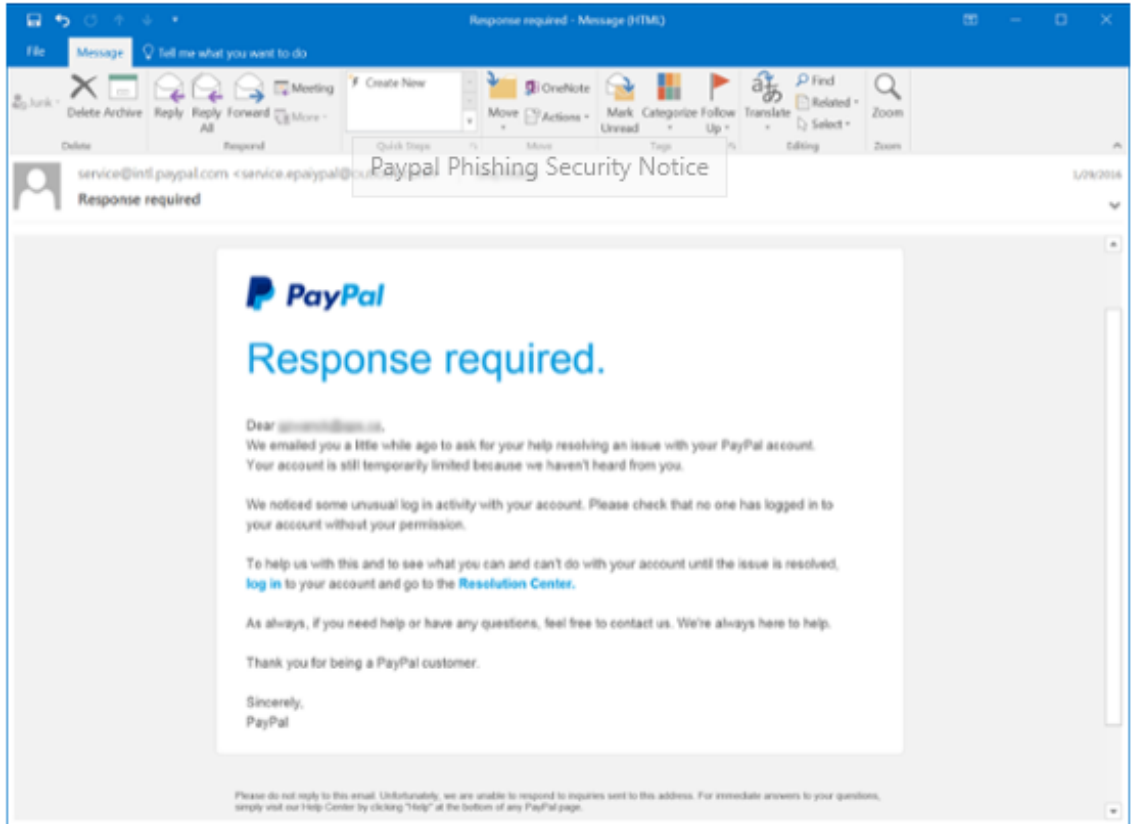


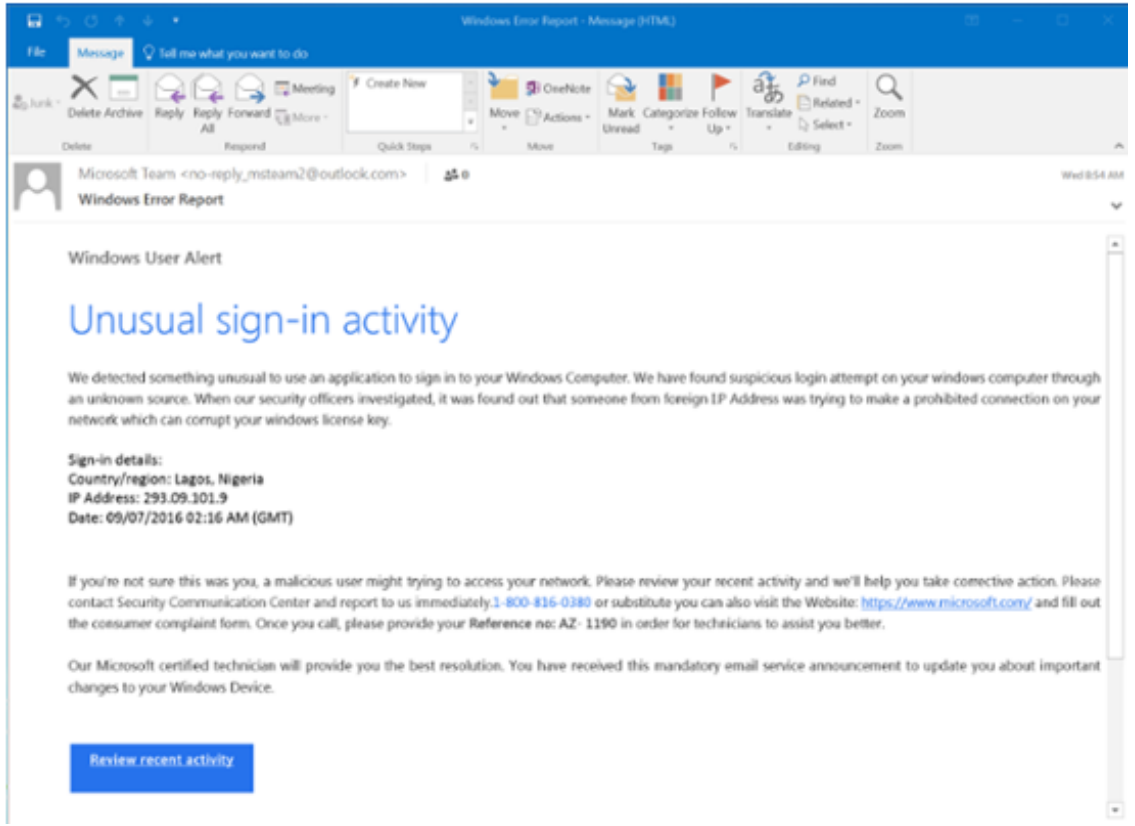
Social engineering is responsible for majority of malicious data breaches

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

What is Phishing?

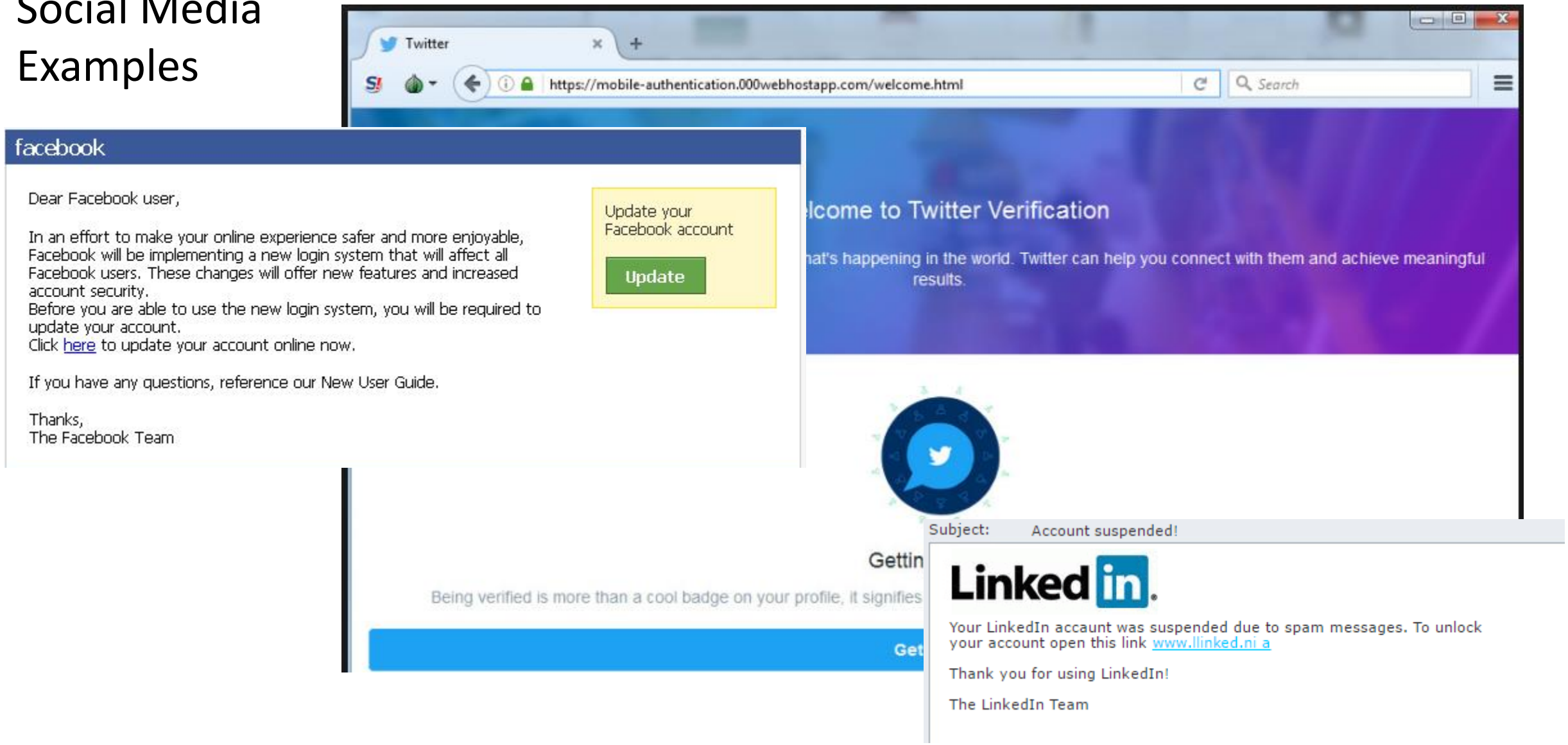
Email Examples





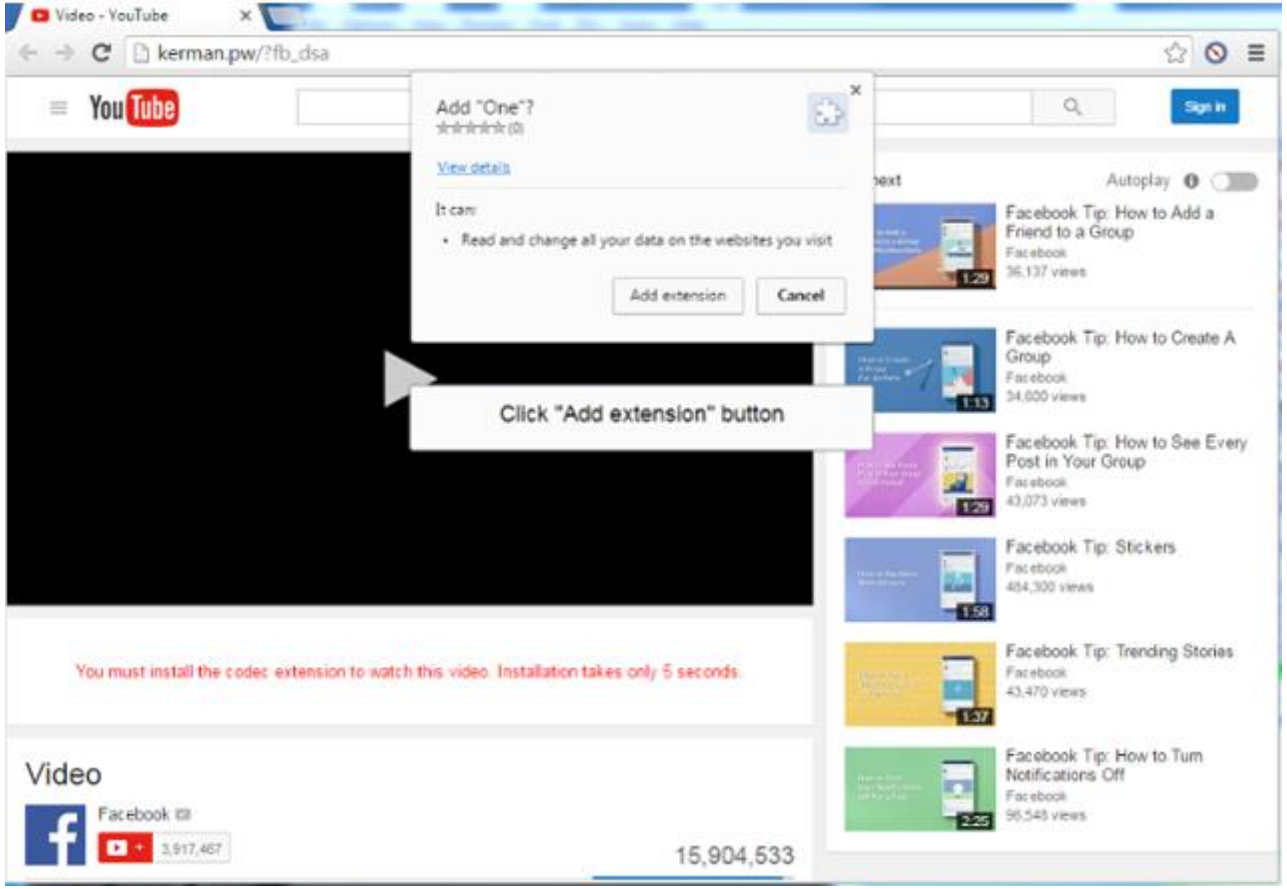
What is Phishing?

Social Media Examples



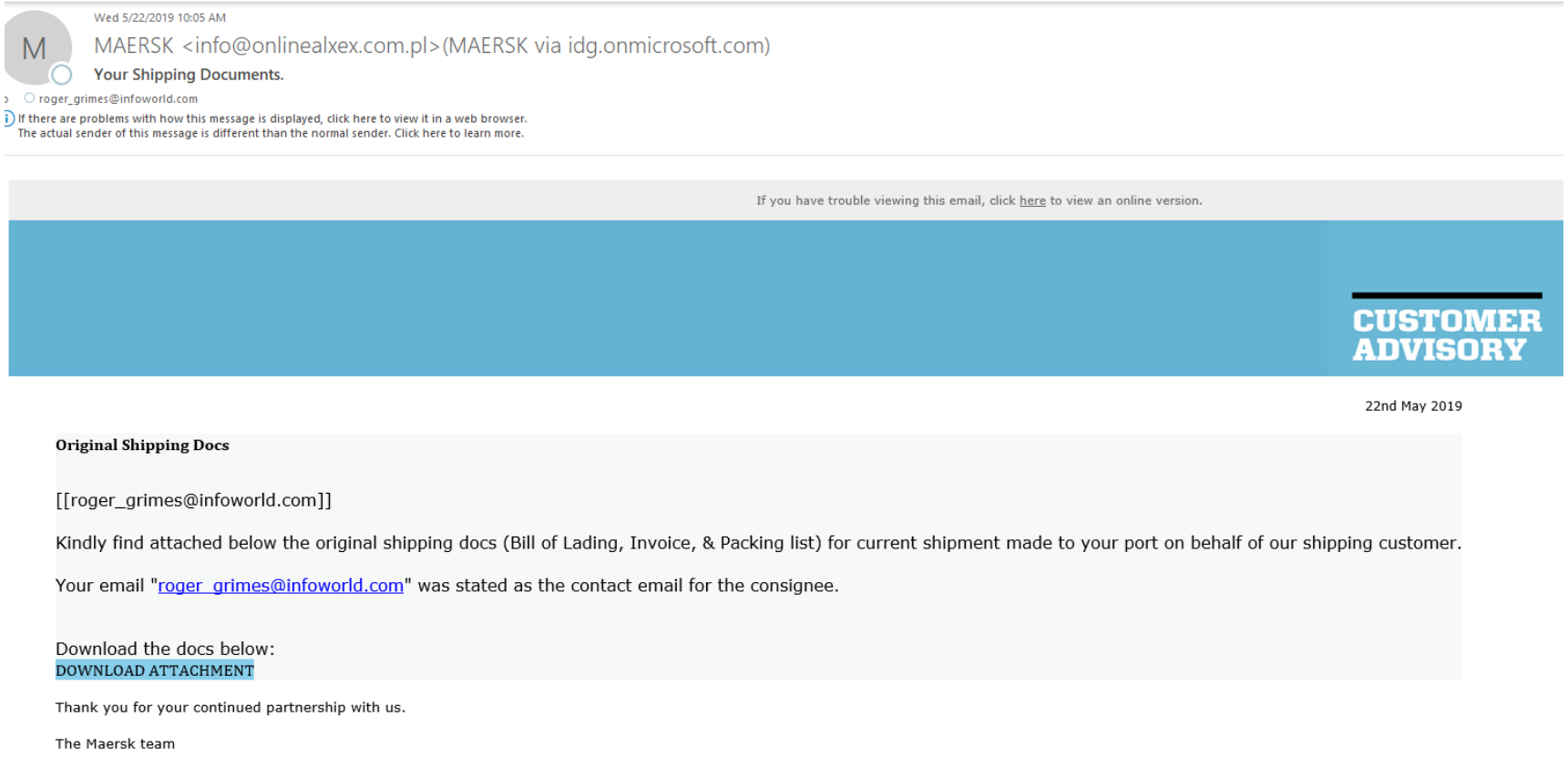
What is Phishing?

More Social Media Examples



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

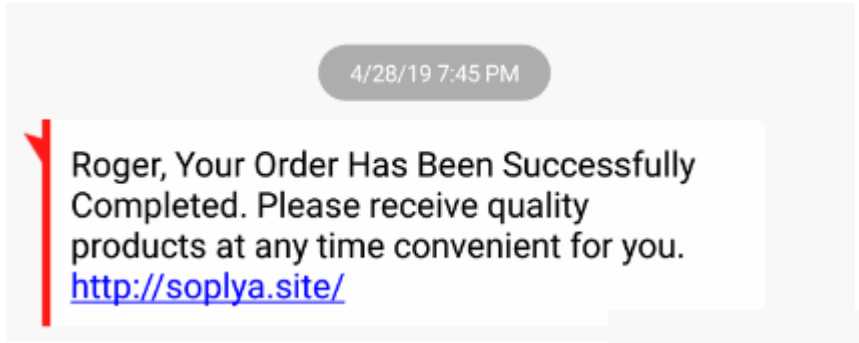
Thank you for your continued partnership with us.

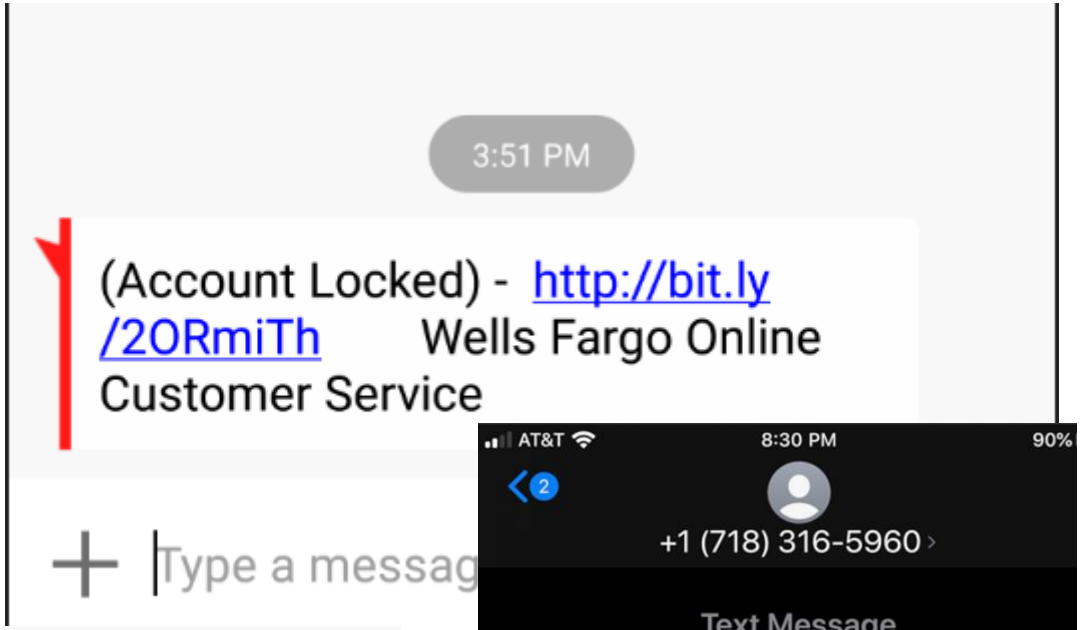
The Maersk team

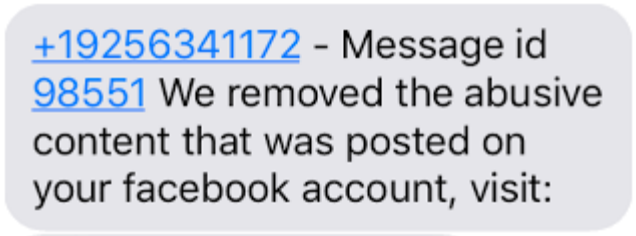
What is Smishing?

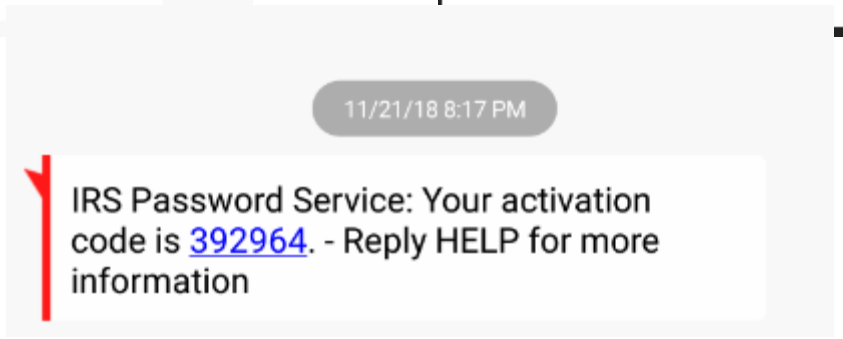
Smishing Examples

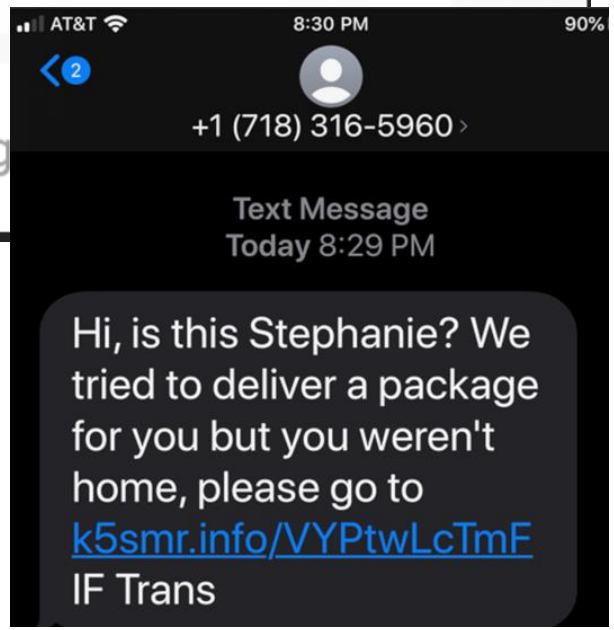
- Malicious SMS message
- Becoming very common











How Hackers Break In

Human Adversary

How Hackers Break In

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something.

- Step 1 – Find an exploit scanning tool that will tell you what software and versions computers are running (e.g., Nmap, etc.)
- Step 2 – Figure out what unpatched vulns are available in that version of the software
- Step 3 – Find or code the exploit to break into the computer

Exploitation Databases

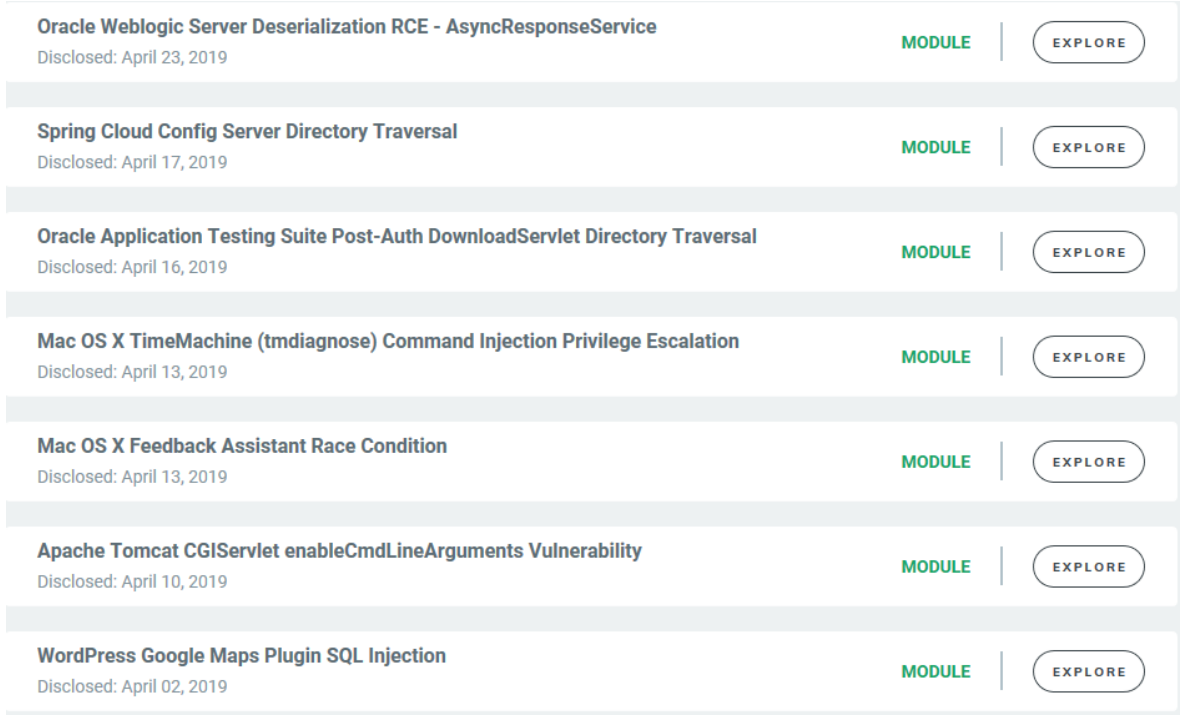
There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something, including:

- Exploit Database (https://www.exploit-db.com/)
  - Over 44,500 exploits

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something, including:

- Metasploit Framework
  - https://www.metasploit.com/
  - Free and commercial tool
  - Over 3000 exploit modules



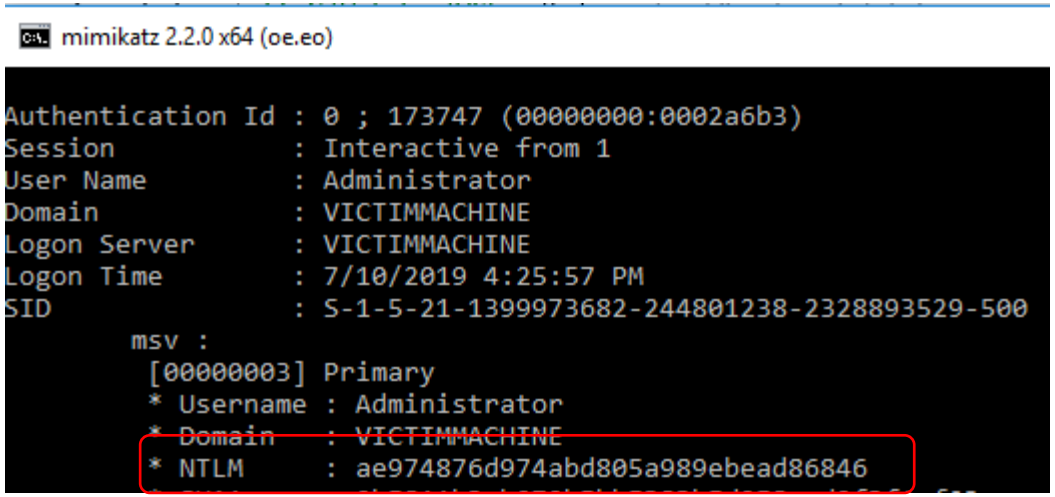
Hacker Tricks to Take Over Your Network

Empire Powershell:

Currently one of the most commonly used hacker tools

Mimikatz

- https://github.com/gentilkiwi/mimikatz
- Dumps AD password hashes, pass-the-hash, and “golden ticket” attacks

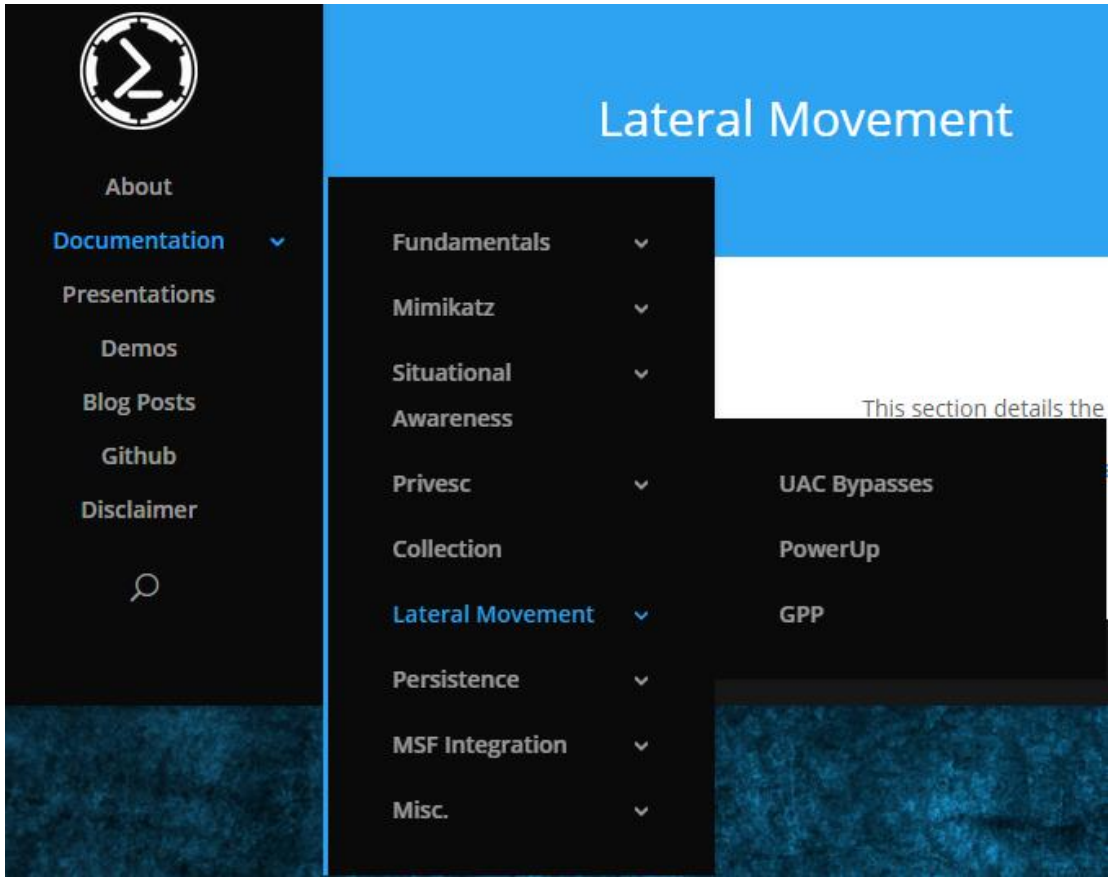


Hacker Tricks to Take Over Your Network

Empire Toolkit:

Currently one of the most commonly used hacker tools

- https://www.powershellempire.com/
- On Windows uses PowerShell scripts
- Privilege escalations
- Lateral movement
- Persistence
- Mimikatz and Metasploit integration

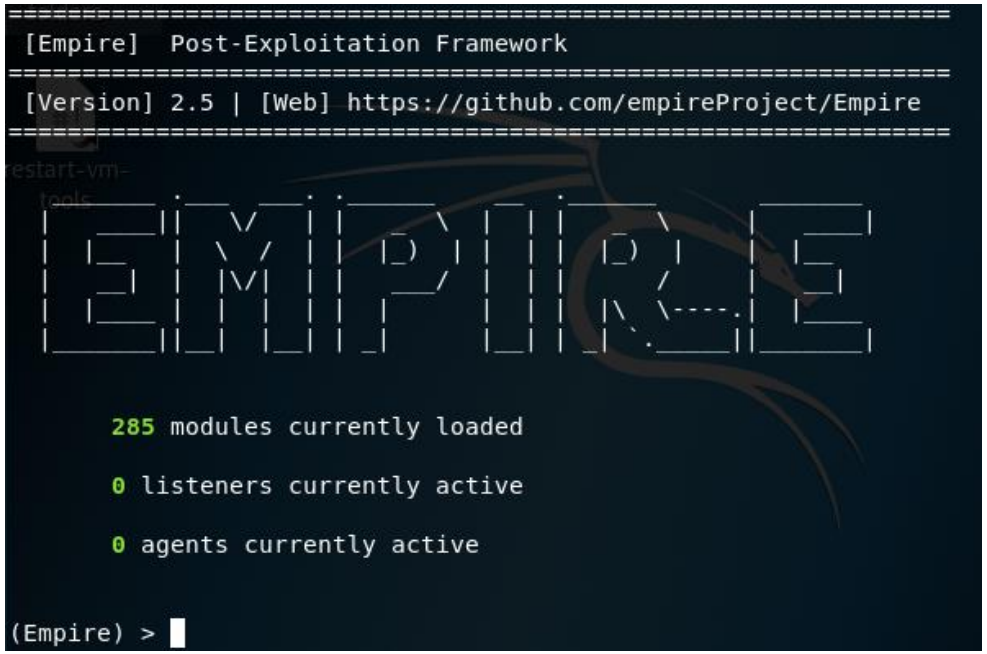


Hacker Tricks to Take Over Your Network

Empire Powershell:

Currently one of the most commonly used hacker tools

- https://www.powershellempire.com/
- Over 285 hacker modules



List of modules: https://www.infosecmatter.com/empire-module-library/

Hacker Tricks to Take Over Your Network

Empire Powershell:

285+ hacking modules

OSX Examples

```
python/persistence/osx/mail

    Installs a mail rule that will execute an AppleScript stager when a
    trigger word is present in the Subject of an incoming mail.
```

```
python/collection/osx/osx_mic_record

    Records audio through the MacOS webcam mic by leveraging the Apple
    AVFoundation API.
```

```
python/collection/osx/search_email

    Searches for Mail .emlx messages, optionally only returning messages
    with the specified SeachTerm.

python/collection/linux/keylogger

    Logs keystrokes to the specified file. Ruby based and heavily adapted
    from MSF's osx/capture/keylog_recorder. Kill the resulting PID when
    keylogging is finished and download the specified LogFile.
```

But MFA will save us!

Very Common MFA Hack

Network Session Hijacking

- Usually requires Man-in-the-Middle (MitM) attacker
- Attacker puts themselves inside of the communication stream between legitimate sender and receiver
- Doesn’t usually care about authentication that much
- Just wants to steal resulting, legitimate access session token after successful authentication
- On web sites, session tokens are usually represented by a “cookie” (a simple text file containing information unique for the user/device and that unique session)
- Session token usually just good for session

MFA Hacks

Network Session Hijacking

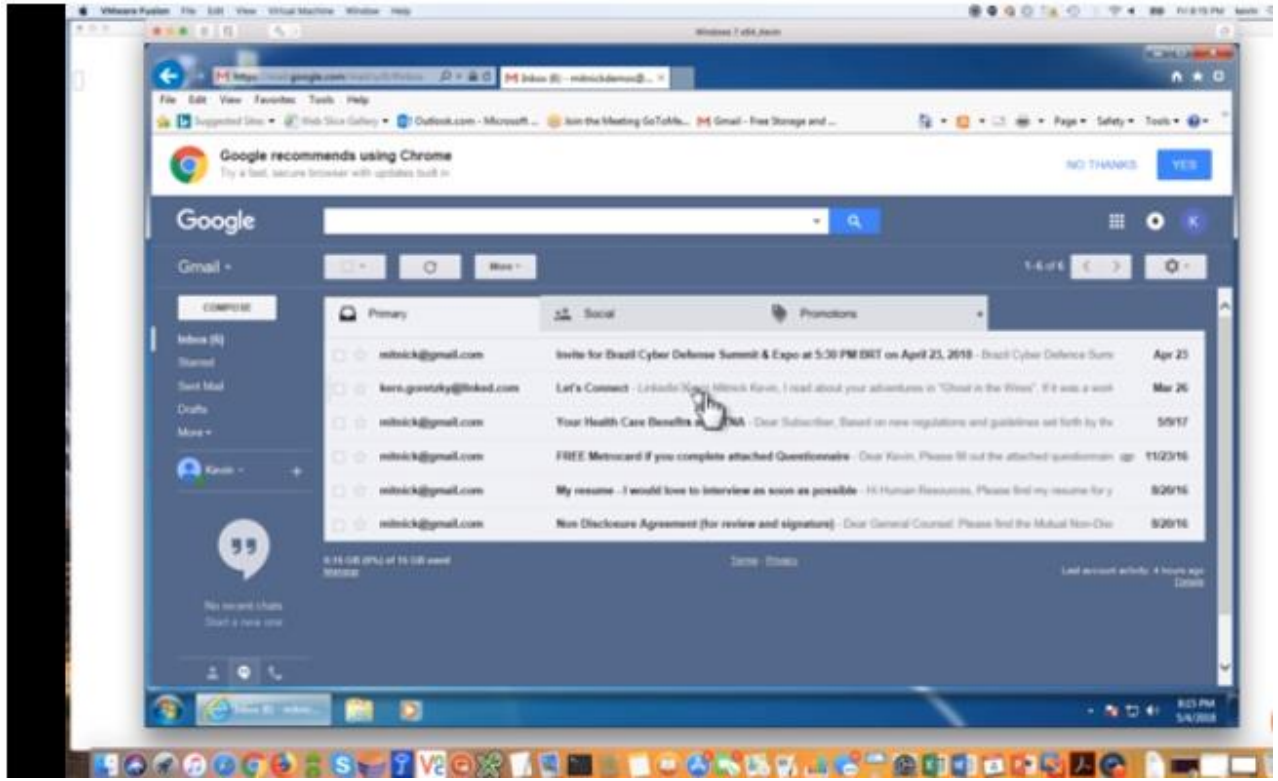
Network Session Hijacking Proxy Theft

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

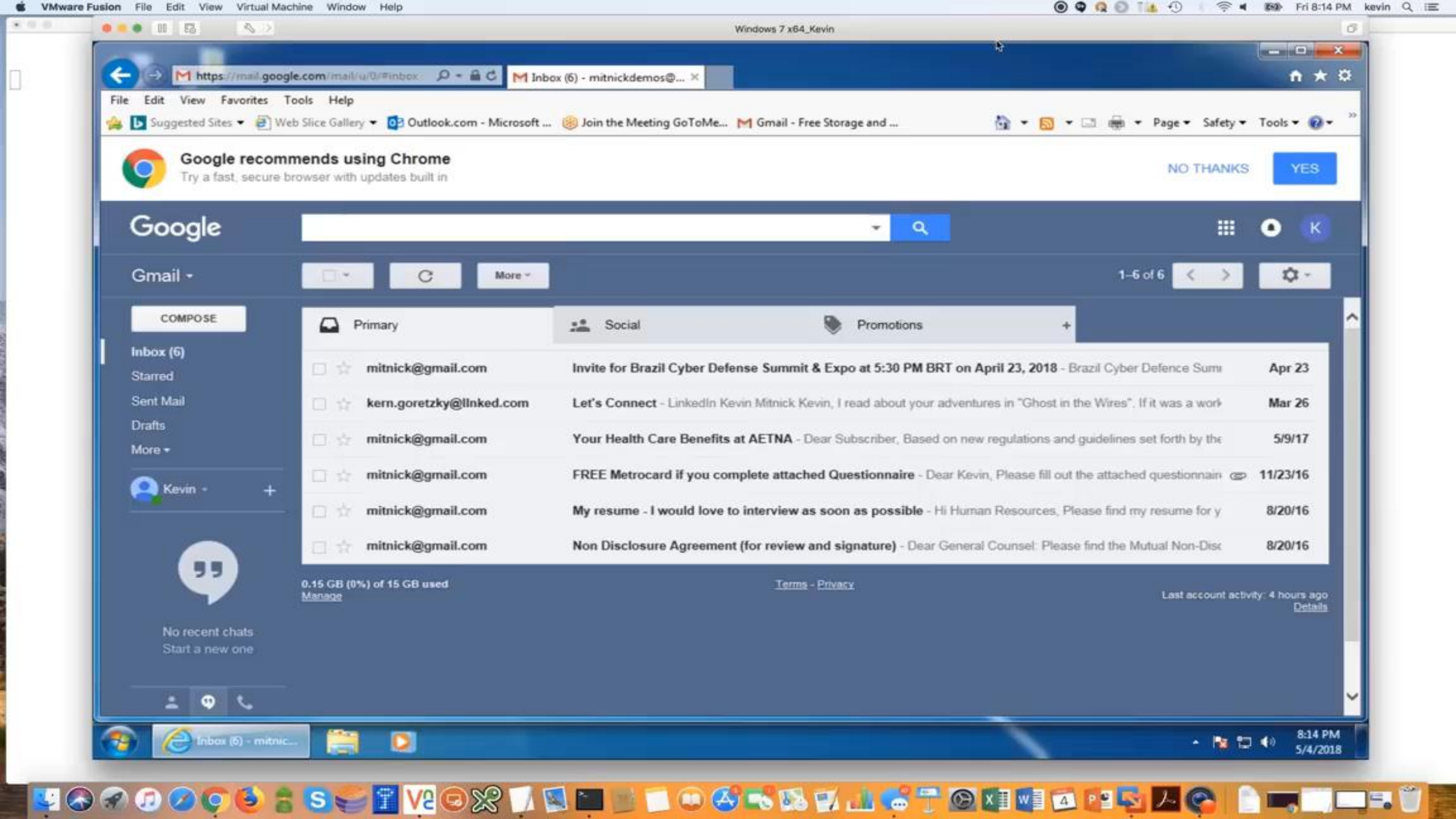
MFA Hacks

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


VMware Fusion File Edit View Virtual Machine Window Help
Fri 8:14 PM kevin
Windows 7 x64_Kevin
https://mail.google.com/mail/u/0/#inbox
Inbox (6) - mitnickdemos@...
File Edit View Favorites Tools Help
Suggested Sites Web Slice Gallery Outlook.com - Microsoft ... Join the Meeting GoToMe... Gmail - Free Storage and ...
Page Safety Tools
Google recommends using Chrome
Try a fast, secure browser with updates built in
NO THANKS
YES
Google
Gmail
More
1–6 of 6
COMPOSE
Inbox (6)
Starred
Sent Mail
Drafts
More
Kevin
Primary
Social
Promotions
mitnick@gmail.com Invite for Brazil Cyber Defense Summit & Expo at 5:30 PM BRT on April 23, 2018 - Brazil Cyber Defence Sumi Apr 23
kern.goretzky@linked.com Let's Connect - LinkedIn Kevin Mitnick Kevin, I read about your adventures in "Ghost in the Wires". If it was a work Mar 26
mitnick@gmail.com Your Health Care Benefits at AETNA - Dear Subscriber, Based on new regulations and guidelines set forth by the 5/9/17
mitnick@gmail.com FREE Metrocard if you complete attached Questionnaire - Dear Kevin, Please fill out the attached questionnair 11/23/16
mitnick@gmail.com My resume - I would love to interview as soon as possible - Hi Human Resources, Please find my resume for y 8/20/16
mitnick@gmail.com Non Disclosure Agreement (for review and signature) - Dear General Counsel: Please find the Mutual Non-Disc 8/20/16
0.15 GB (0%) of 15 GB used
Manage
Terms - Privacy
Last account activity: 4 hours ago
Details
No recent chats
Start a new one
Inbox (6) - mitnic...
8:14 PM
5/4/2018

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo

1. Phishing email contained URL to fake look-alike/sound-alike web site that was really an evil proxy
2. Email tricked user into visiting evil proxy web site
3. User typed in credentials, which proxy, now pretending to be the legitimate customer, presented to legitimate web site
4. Legitimate web site sent back legitimate session token, which Kevin then stole and replayed to take over user's session

- Kevin used Evilginx (https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/)
- One example hack out of the dozens, if not hundreds of ways to do session hijacking, even if MFA is involved

SMS Rogue Recovery

Rogue Recoveries

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

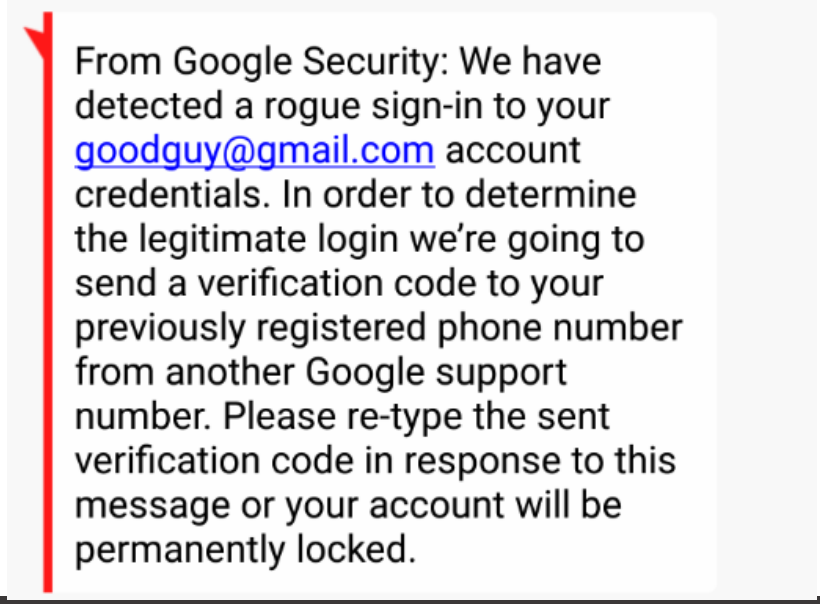
Rogue Recoveries

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



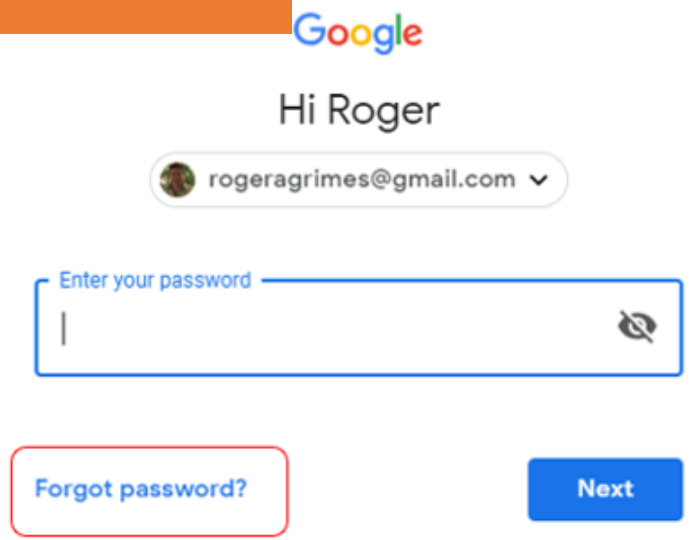
Rogue Recoveries

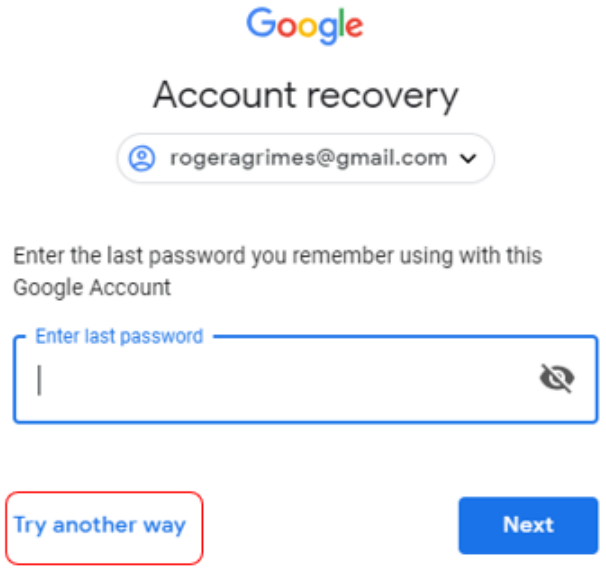
Hacking Into Your Email Using Recovery Methods

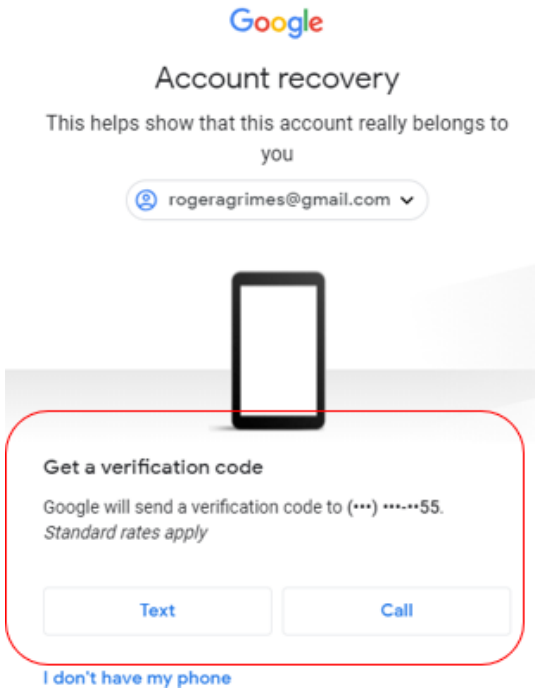
SMS Rogue Recovery

Steps

2. Hacker forces your email account into SMS PIN recoverv







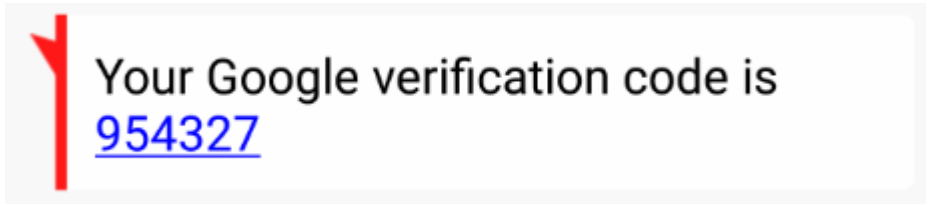
Rogue Recoveries

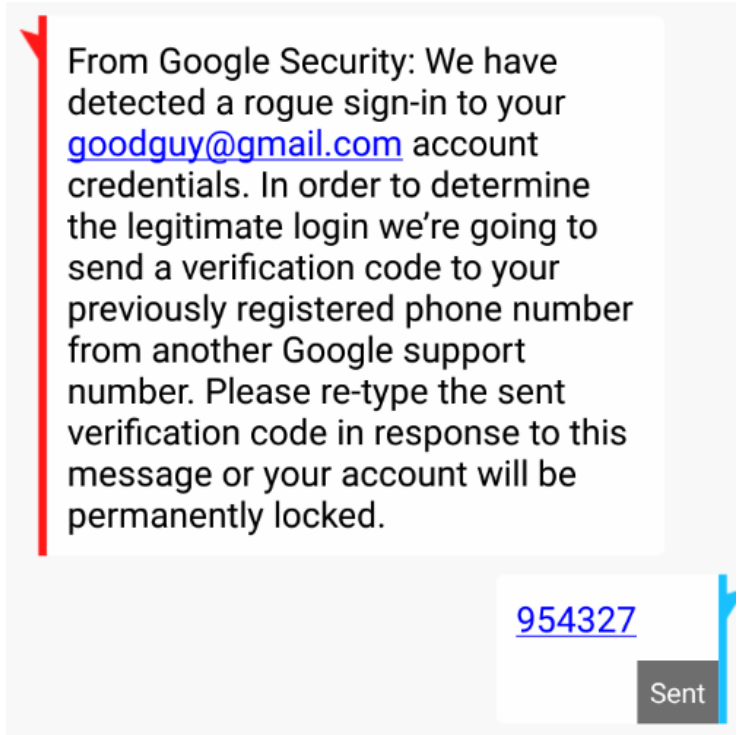
SMS Rogue Recovery

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



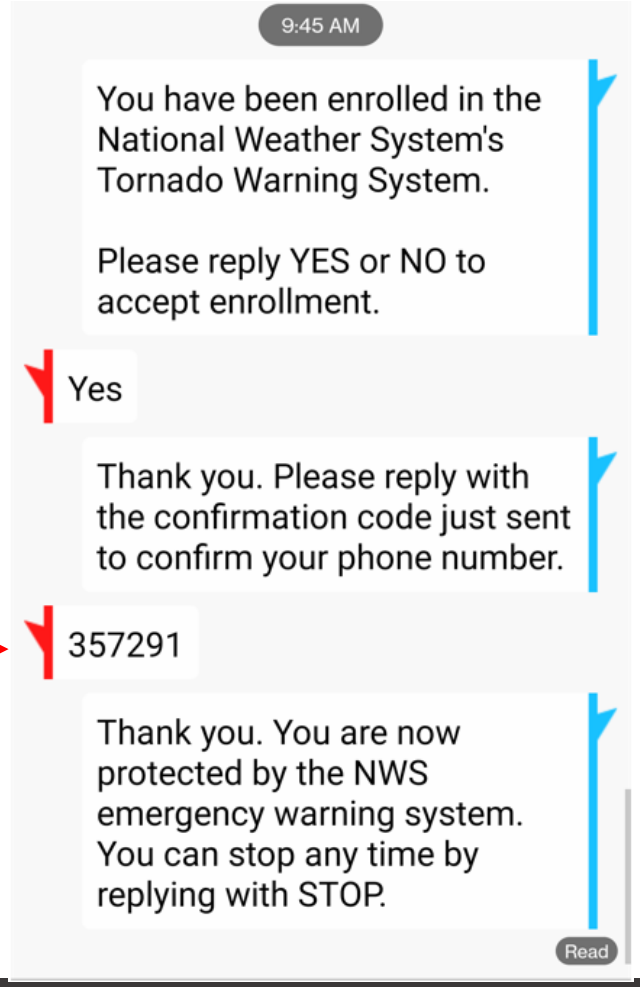


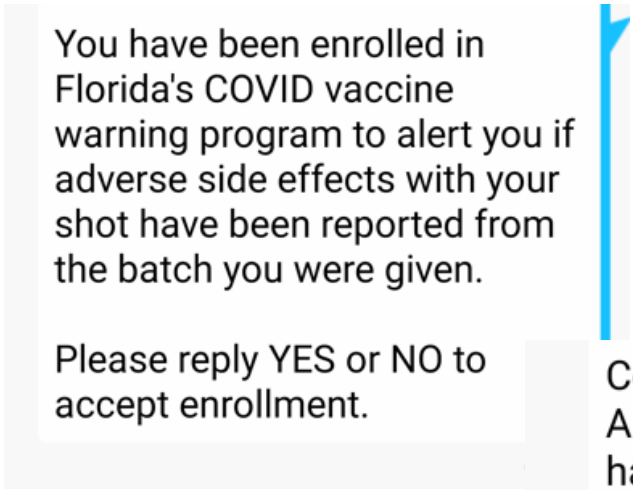
Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

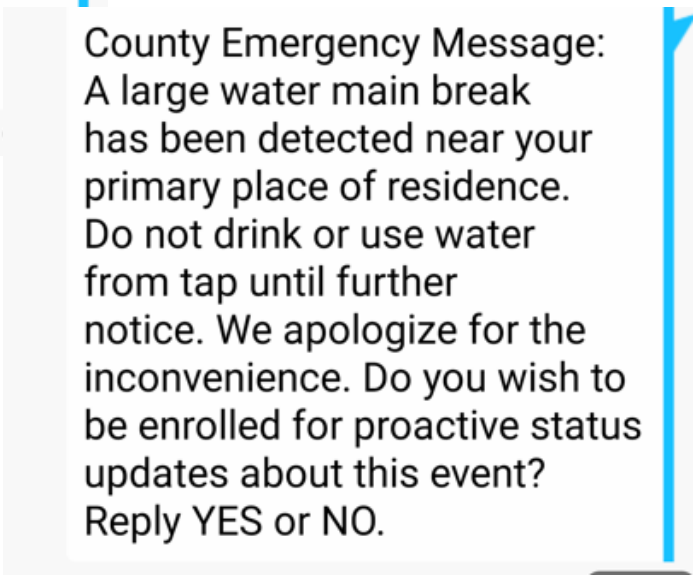
SMS Rogue Recovery

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

Agenda

- How and Why Hackers Hack
- Why is Fighting Phishing Important?
- Best Practice Defenses

Best Defenses

Top Defenses for All People and Organizations

- **Mitigate Social Engineering**
- **Patch Internet-accessible software**
- **Use Multifactor Authentication(MFA)/Non-Guessable passwords**
  - Use non-phishable MFA where you can, where you can't;
  - Use unique, unguessable, different passwords for every website and service
- **Teach Yourself and Everyone How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls

All Anti-Phishing Defenses

Everything You Can Try to Prevent Phishing

- Webinar
  - https://info.knowbe4.com/webinar-stay-out-of-the-net

- E-book
  - https://info.knowbe4.com/comprehensive-anti-phishing-guide

What Is the Goal of Security Awareness Training?

The overall goal is to help users make smarter security decisions every day

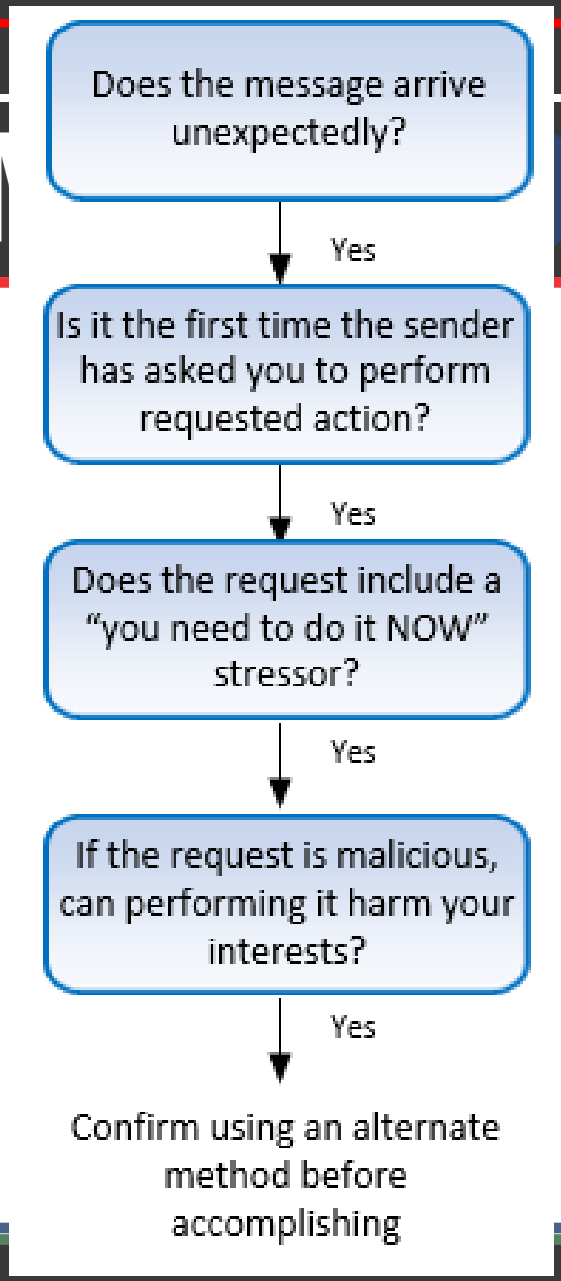
- To reach this goal you must make security awareness an integral part of your organizational culture that simply becomes reflexive

Training users to know

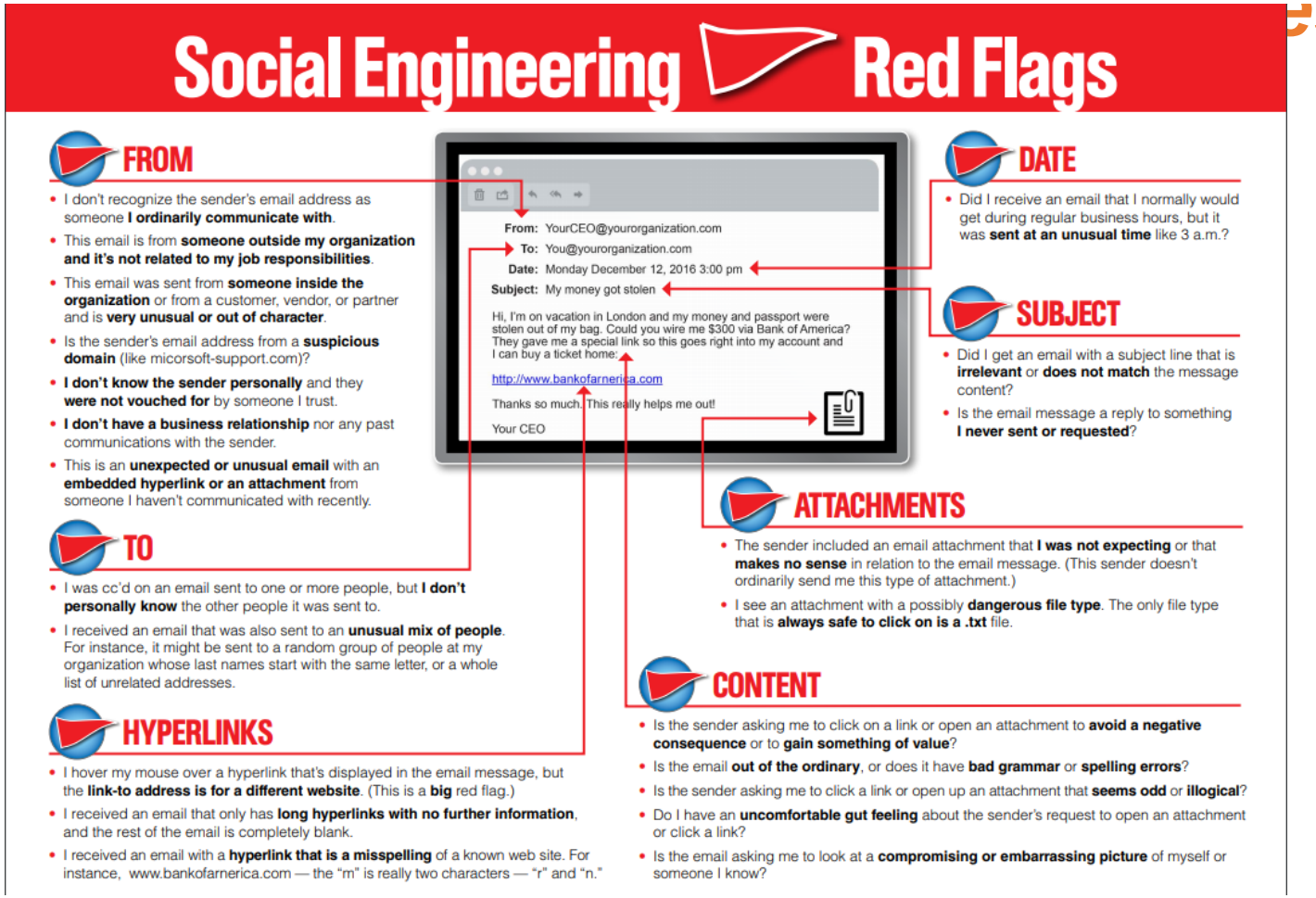
- How to spot bad things
- How to respond

CONFIRM

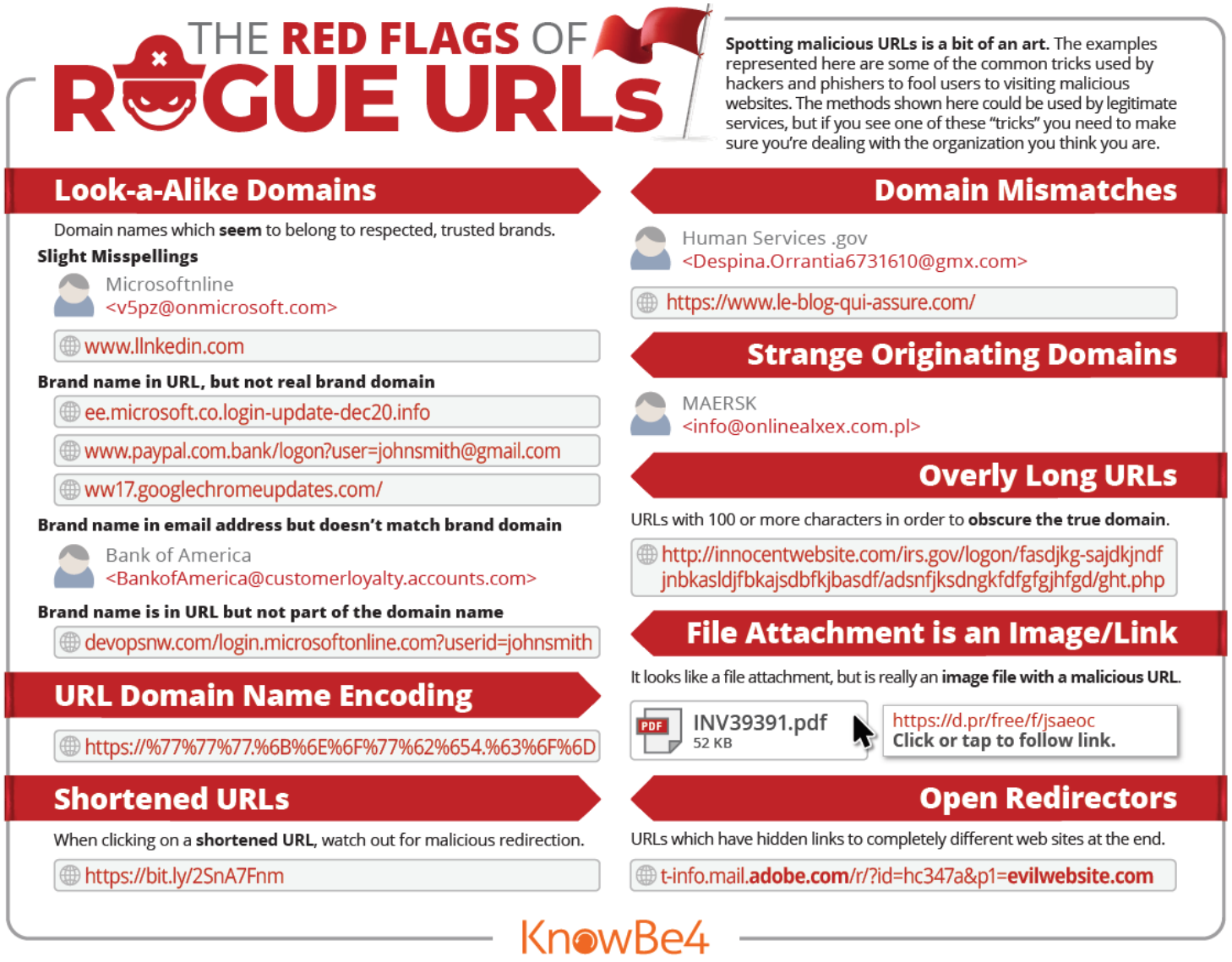
The Conference on Information and Records Management



Give “Red Flags” Training

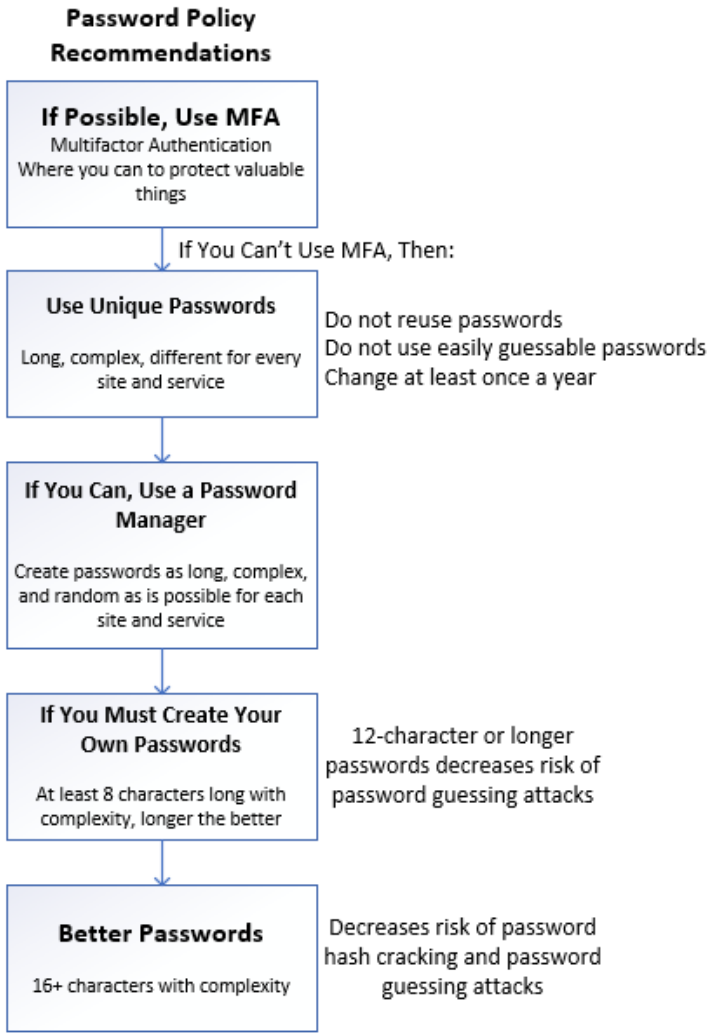


https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees



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

My Password Policy Advice



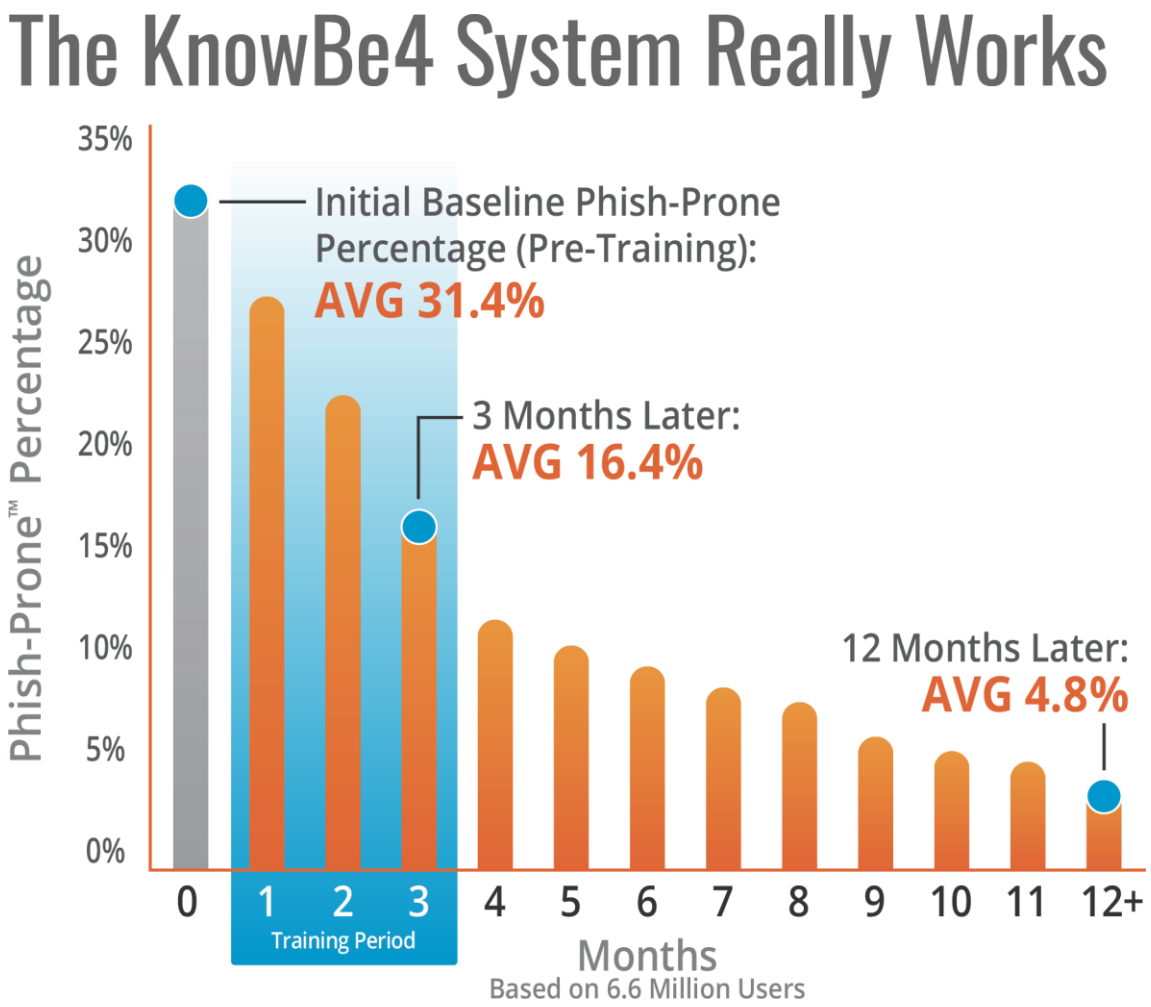
Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

84% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

Thank You!

Questions?

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