

How and Why Hackers Hack

Your Best Practice Defenses



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

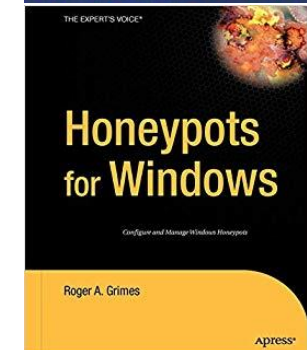
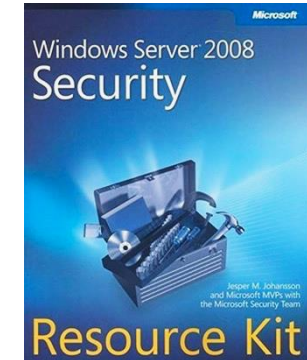
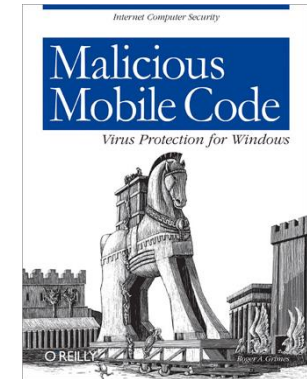
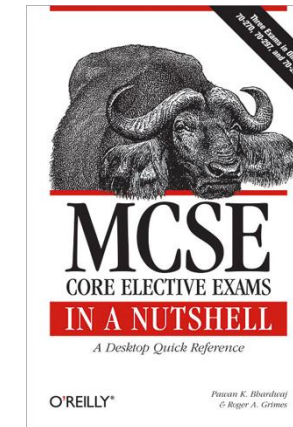
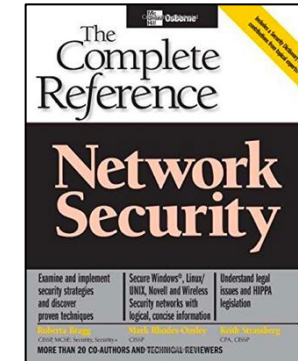
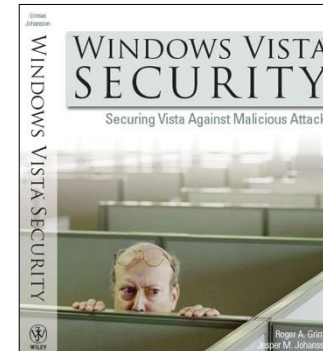
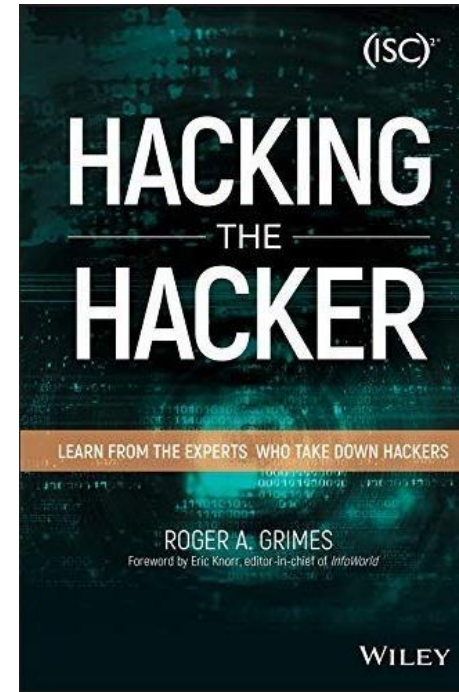
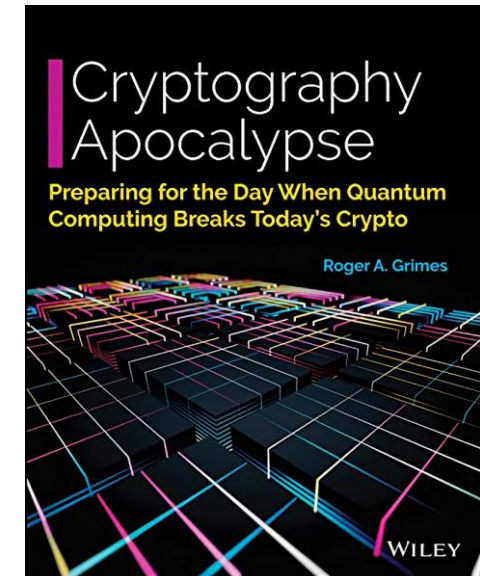
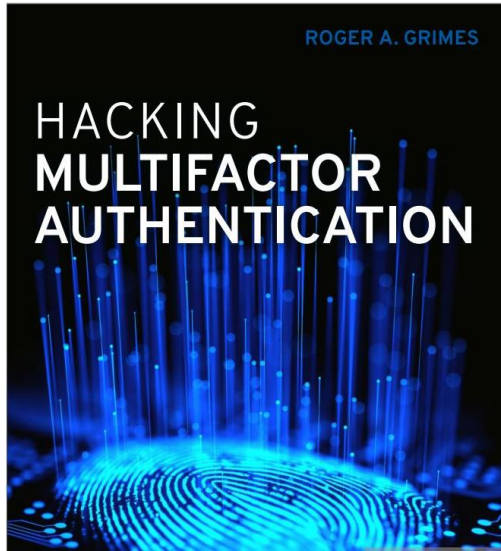
Twitter: @RogerAGrimes

LinkedIn: <https://www.linkedin.com/in/rogeragrimes/>

- 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





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

#GAMETECHIE

Kansas swatting suspect who had an innocent man killed has been arrested

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

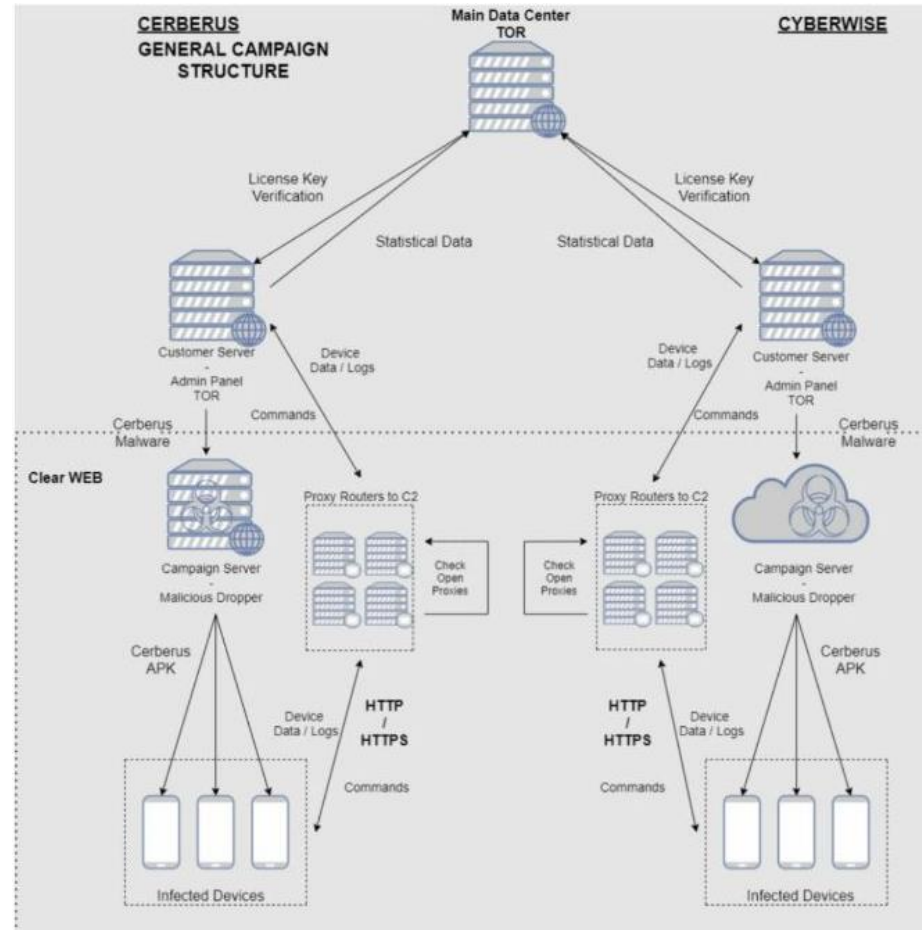
Corporation/Gang

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

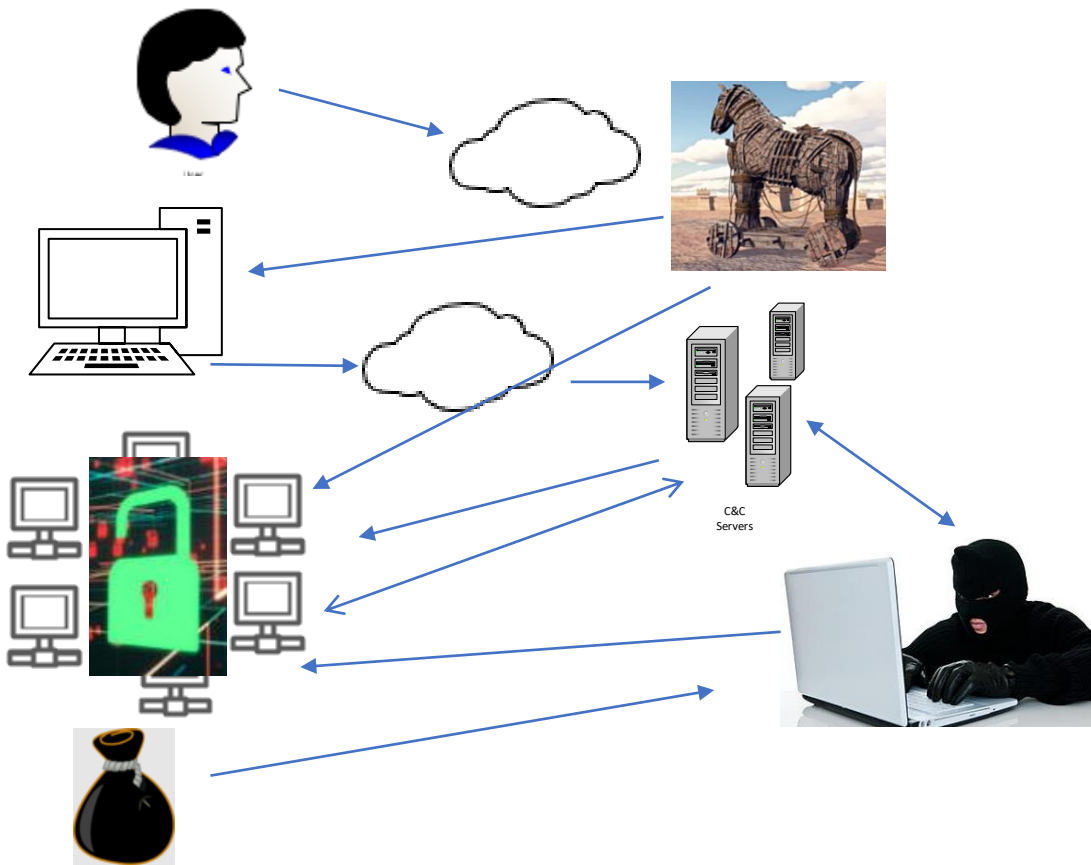
One of Three Ways

- ① Automated Malware
- ① Human Adversary
- ① 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

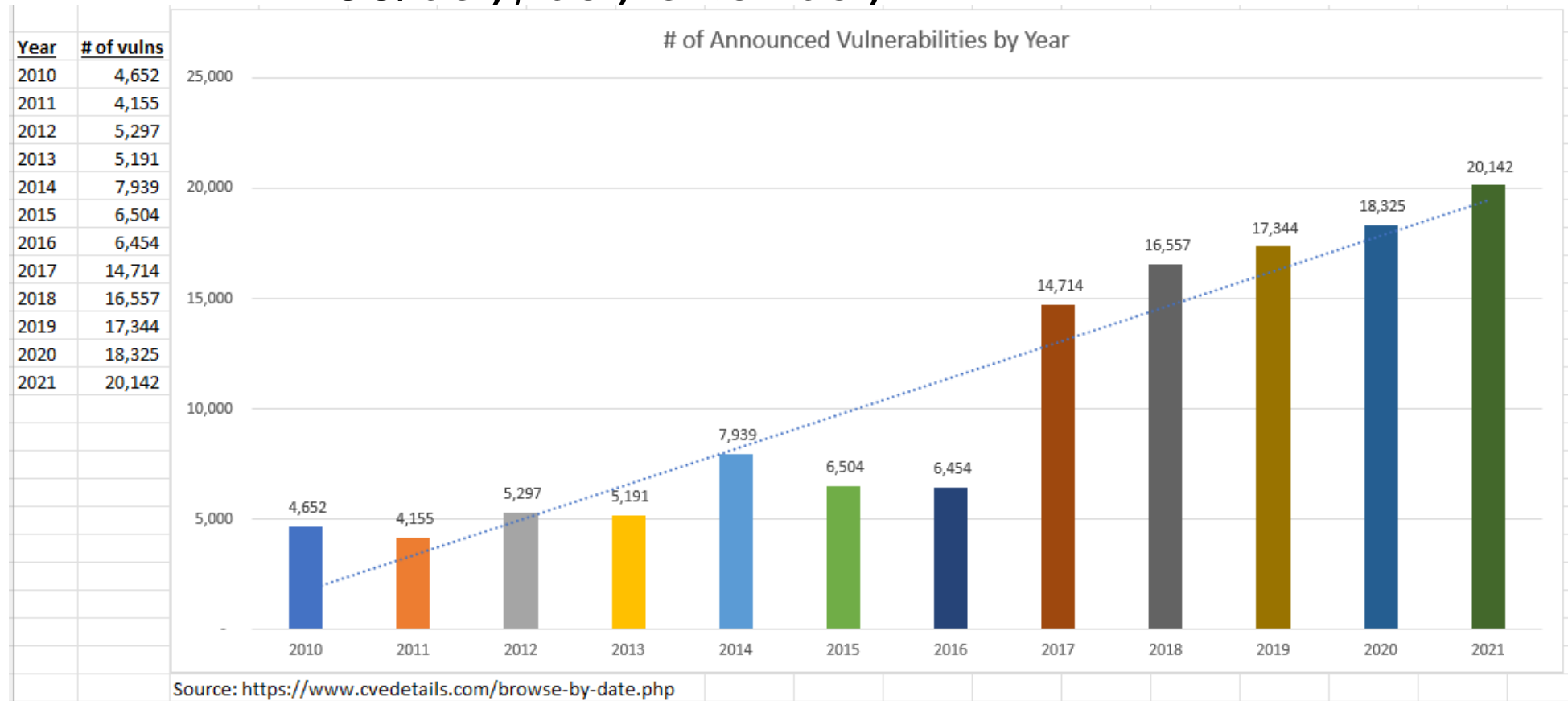
- How and Why Hackers Hack
- Why is Fighting Phishing Important?
- Best Practice Defenses

Problem – Overwhelming Number of Vulnerabilities

of Vulnerabilities

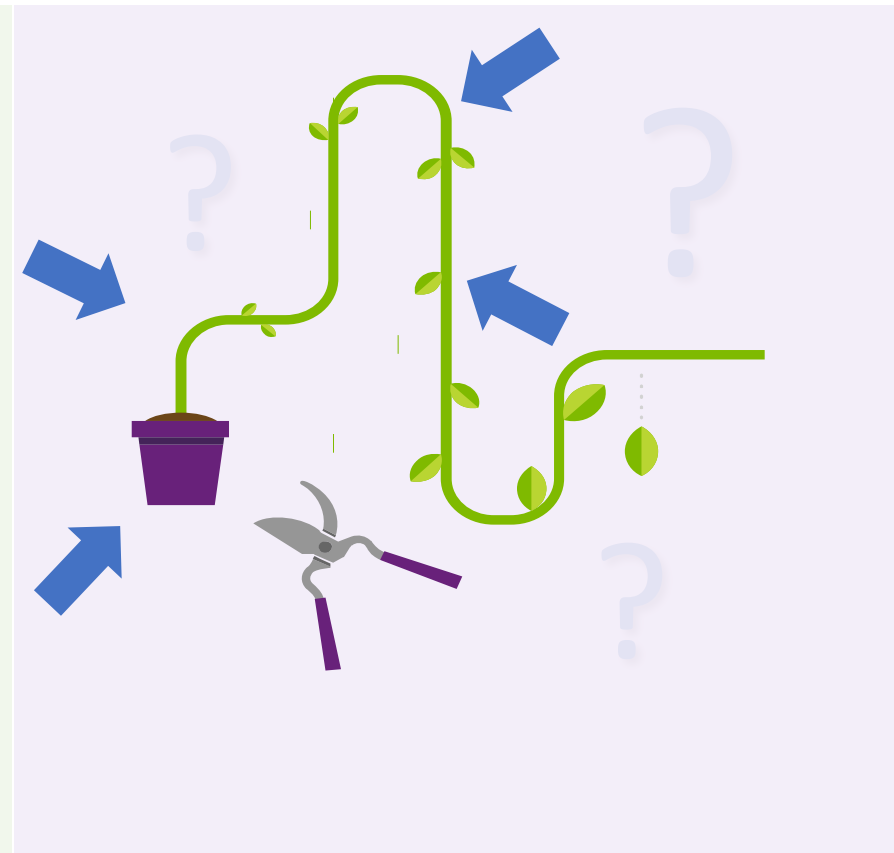
And this is just (known public) vulnerabilities, doesn't include hackers and a hundred million malware programs

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



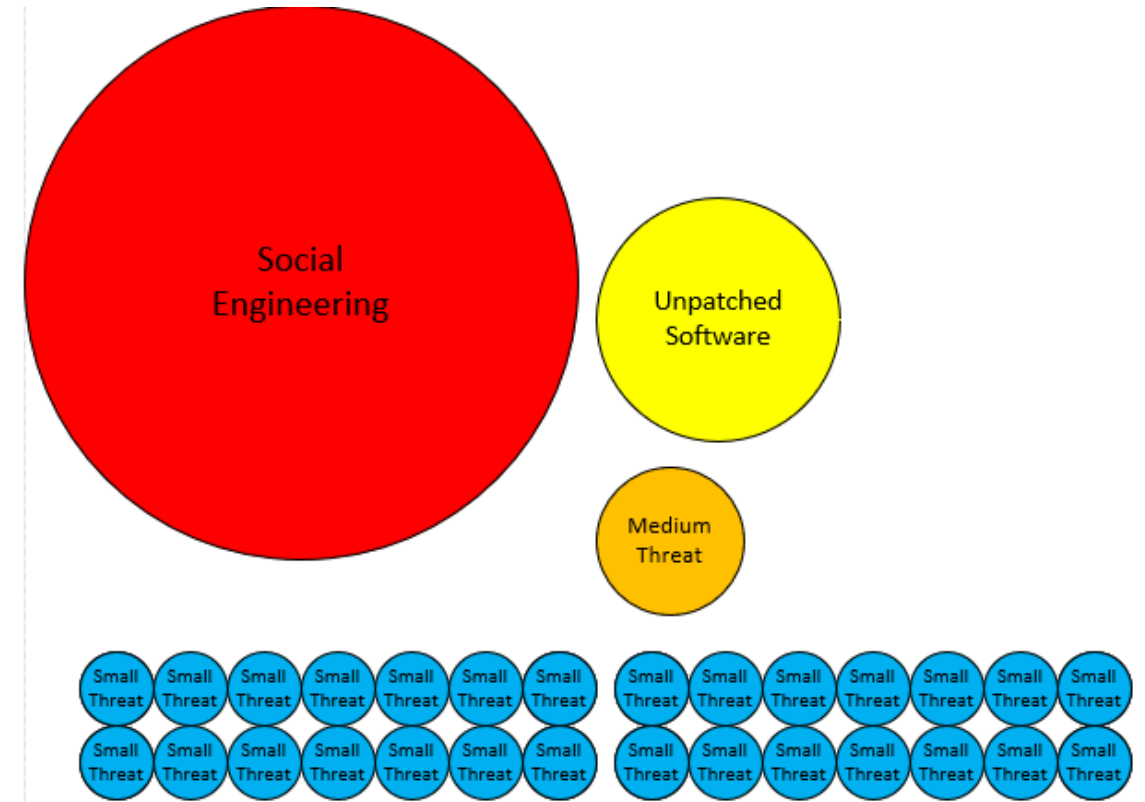
Initial Root Access Exploit Methods

- 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



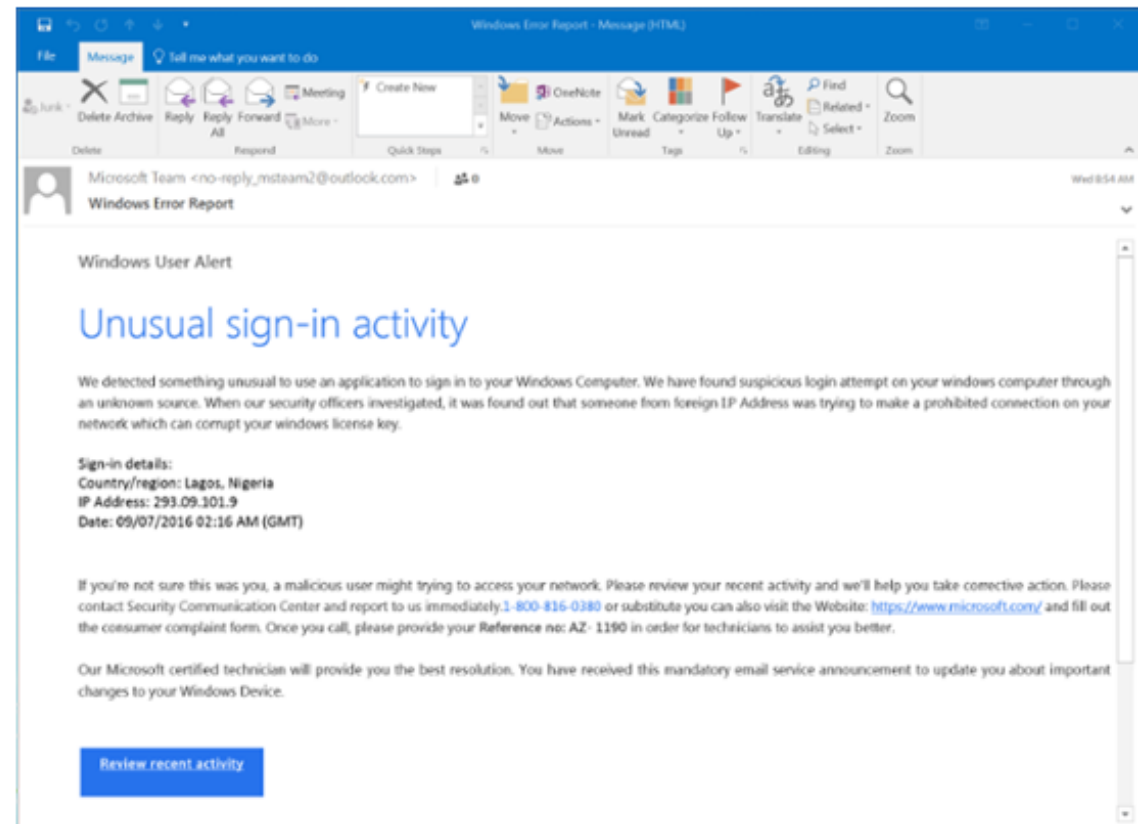
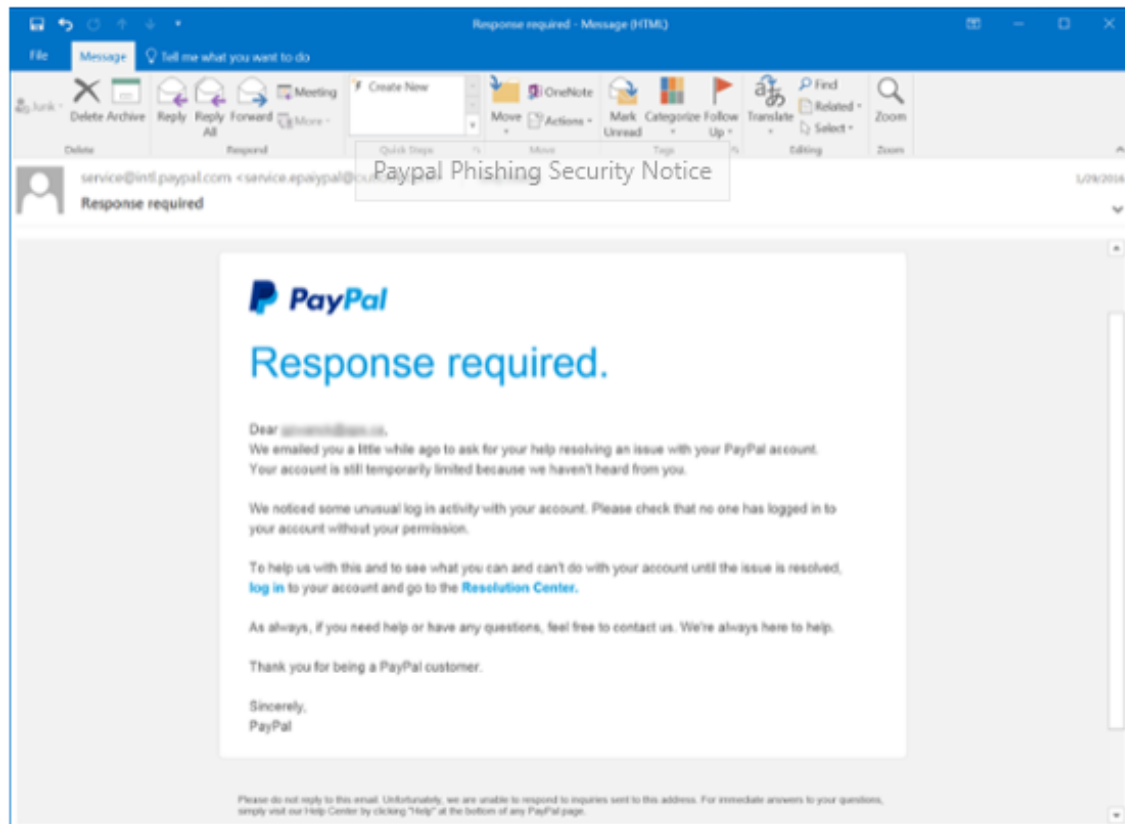
Social engineering is responsible for majority of malicious data breaches

<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?

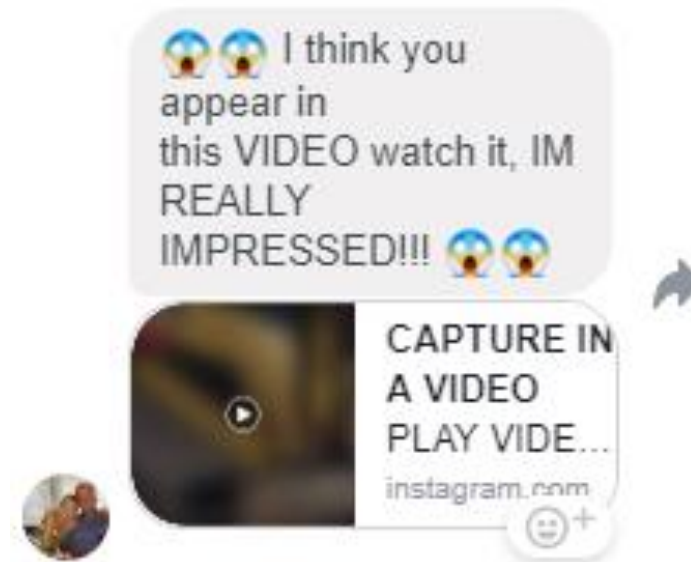
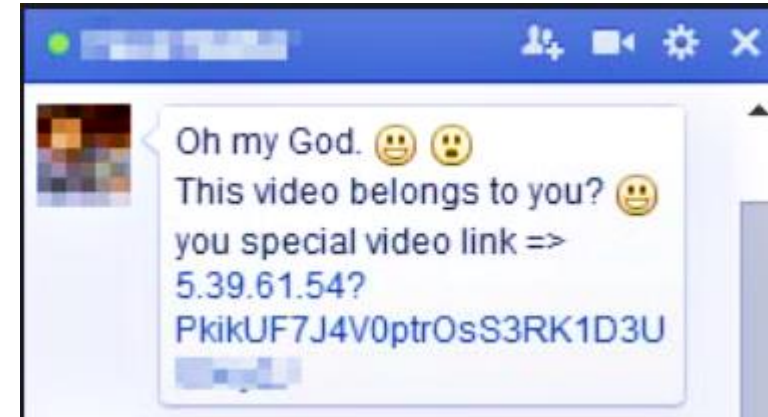
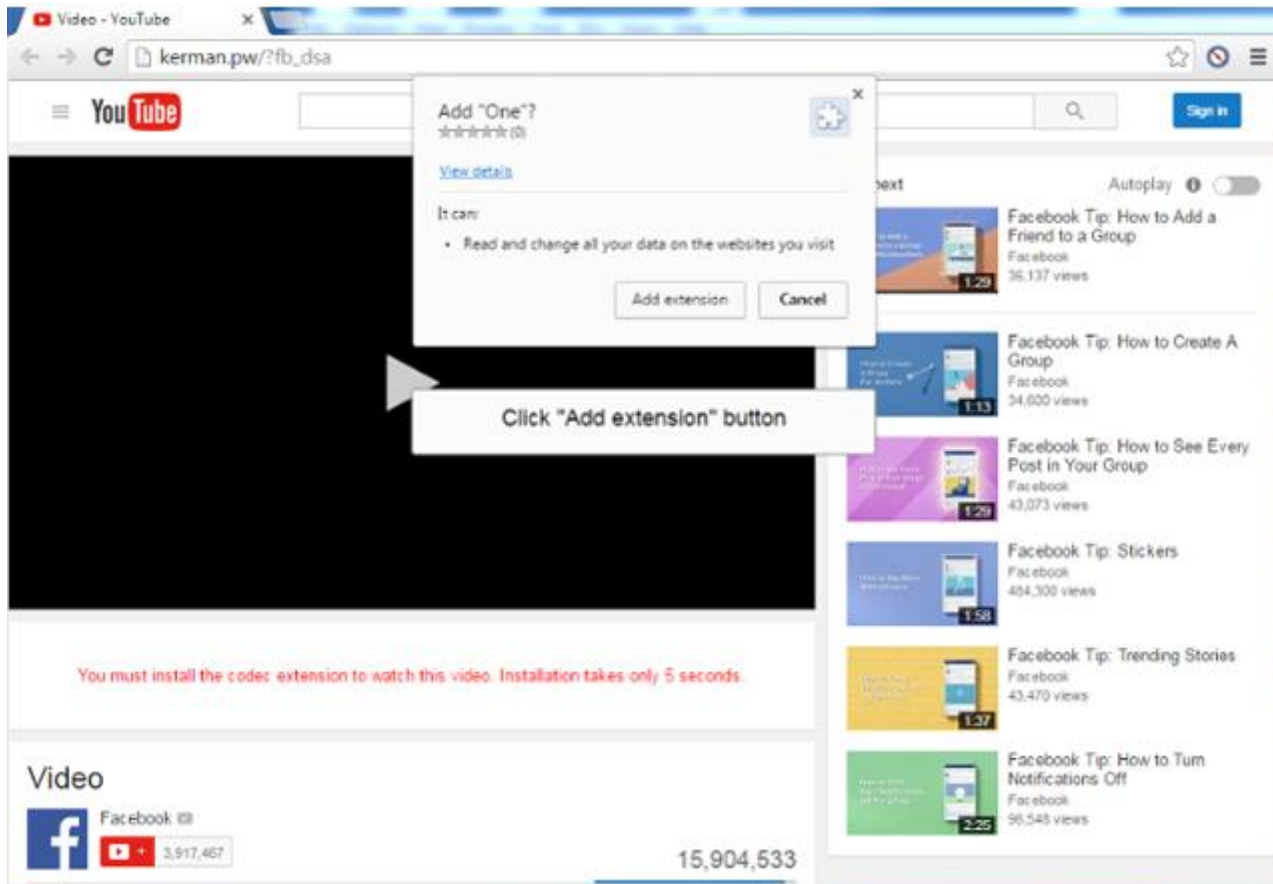
Social Media Examples

The image displays three examples of phishing attempts:

- Facebook Phishing:** A notification titled "facebook" addressed to a "Dear Facebook user," claiming a new login system is being implemented for security. It includes a yellow box with the text "Update your Facebook account" and a green "Update" button. The text concludes with "Thanks, The Facebook Team".
- Twitter Phishing:** A browser window showing a page titled "Welcome to Twitter Verification" with a URL of "https://mobile-authentication.000webhostapp.com/welcome.html". The page text says "Welcome to Twitter Verification" and "What's happening in the world. Twitter can help you connect with them and achieve meaningful results." Below the text is a circular Twitter logo.
- LinkedIn Phishing:** An email notification with the subject "Account suspended!". The body text reads: "Your LinkedIn account was suspended due to spam messages. To unlock your account open this link [www.linkedin.ni.a](\"http://www.linkedin.ni.a\"). Thank you for using LinkedIn! The LinkedIn Team".

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](#)

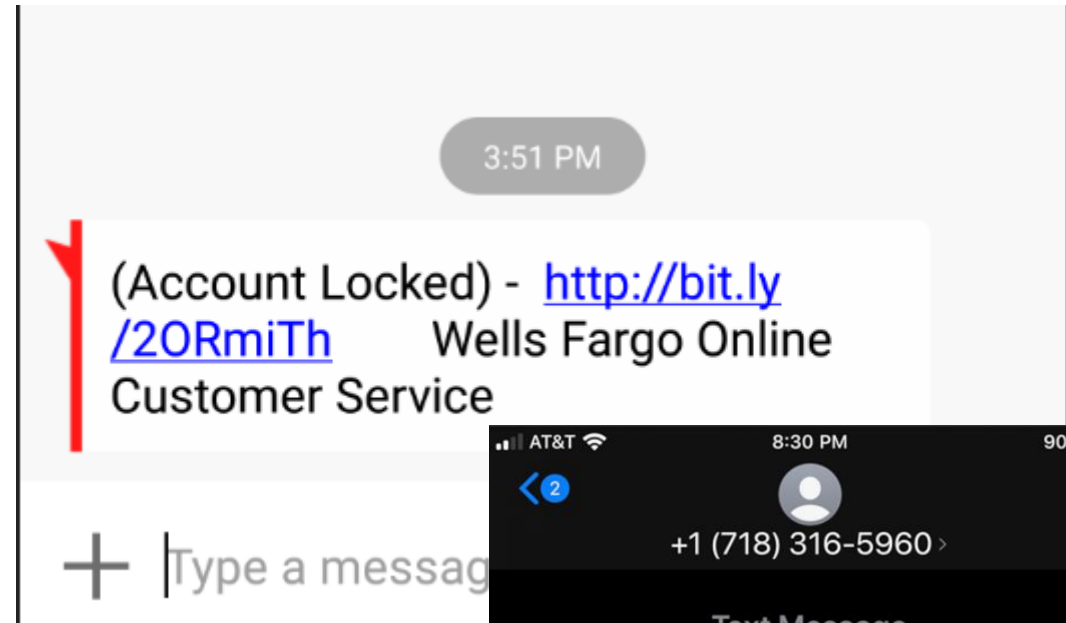
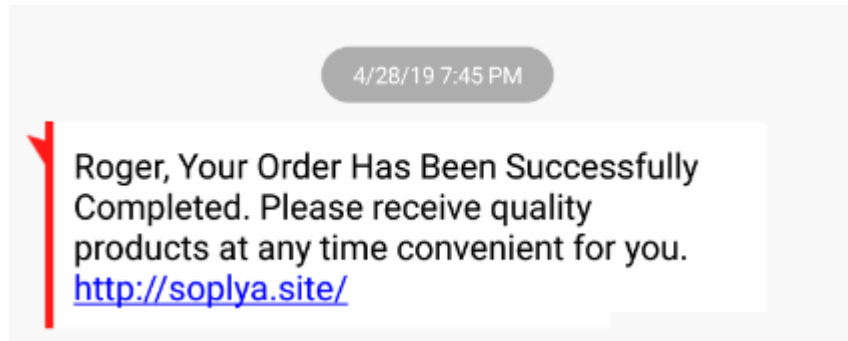
Thank you for your continued partnership with us.

The Maersk team

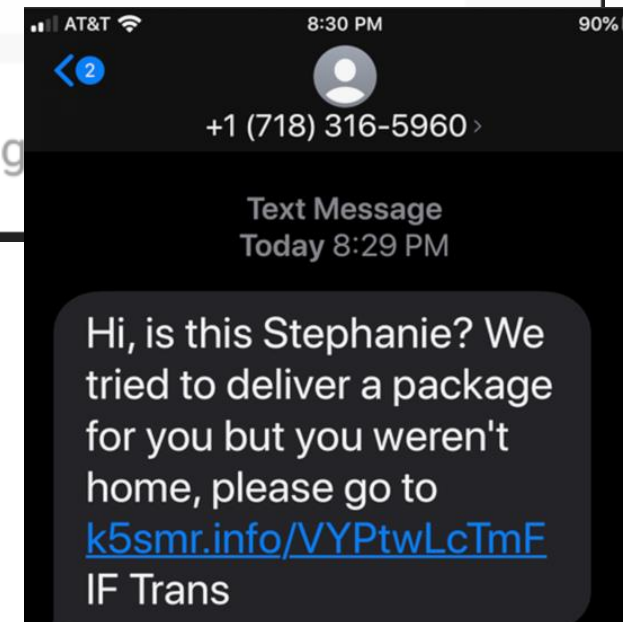
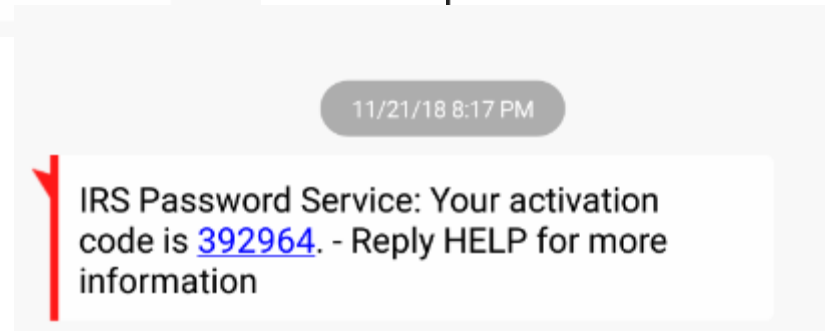
What is Smishing?

Smishing Examples

- Malicious SMS message
- Becoming very common



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



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

2019-07-10	↓	✓	Microsoft DirectWrite / AFDKO - Use of Uninitialized Memory While Freeing Resources in var_loadavar
2019-07-10	↓	✓	Microsoft DirectWrite / AFDKO - Stack-Based Buffer Overflow in do_set_weight_vector_cube for Large nAxes

Showing 1 to 15 of 41,484 entries

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

Oracle Weblogic Server Deserialization RCE - AsyncResponseService Disclosed: April 23, 2019	MODULE	EXPLORE
Spring Cloud Config Server Directory Traversal Disclosed: April 17, 2019	MODULE	EXPLORE
Oracle Application Testing Suite Post-Auth DownloadServlet Directory Traversal Disclosed: April 16, 2019	MODULE	EXPLORE
Mac OS X TimeMachine (tmdiagnose) Command Injection Privilege Escalation Disclosed: April 13, 2019	MODULE	EXPLORE
Mac OS X Feedback Assistant Race Condition Disclosed: April 13, 2019	MODULE	EXPLORE
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability Disclosed: April 10, 2019	MODULE	EXPLORE
WordPress Google Maps Plugin SQL Injection Disclosed: April 02, 2019	MODULE	EXPLORE

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

```
cmd mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 173747 (00000000:0002a6b3)
Session          : Interactive from 1
User Name        : Administrator
Domain           : VICTIMMACHINE
Logon Server     : VICTIMMACHINE
Logon Time       : 7/10/2019 4:25:57 PM
SID              : S-1-5-21-1399973682-244801238-2328893529-500

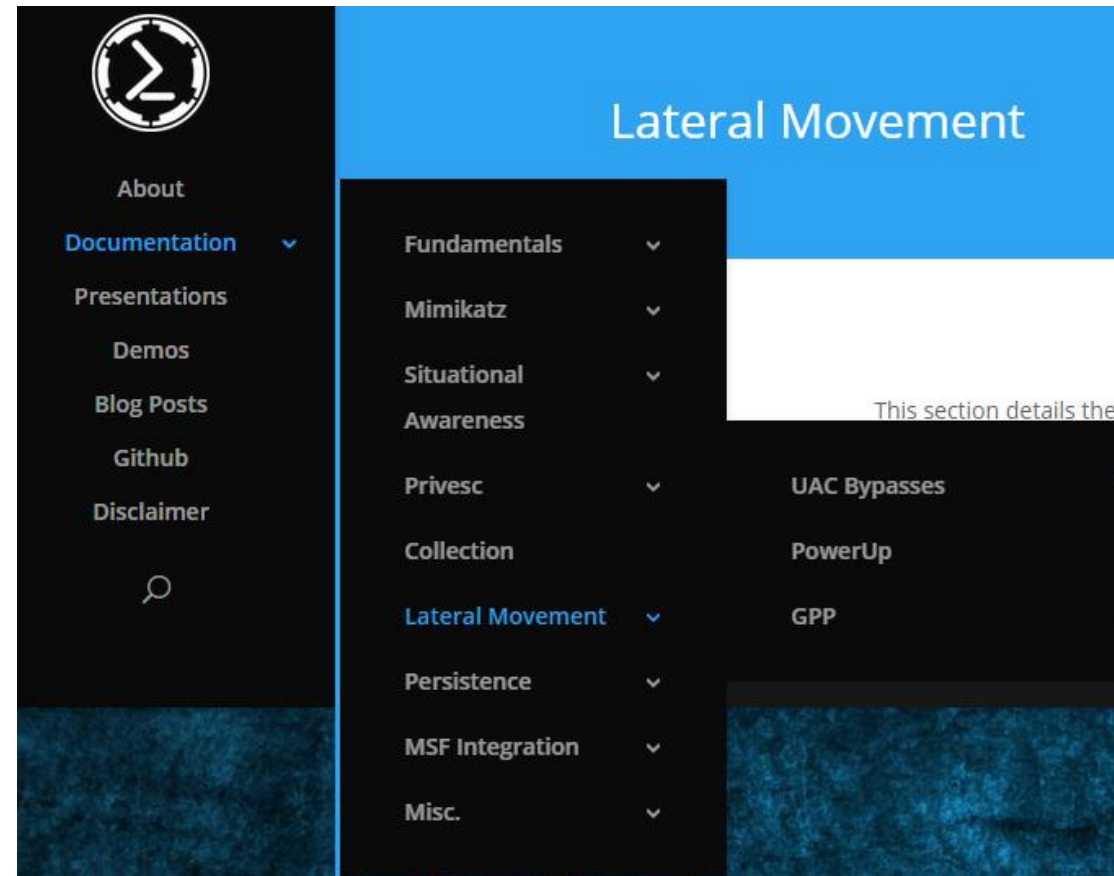
msv :
[00000003] Primary
* Username : Administrator
* Domain   : VICTIMMACHINE
* NTLM    : ae974876d974abd805a989ebeat86846
```

Hacker Tricks to Take Over Your Network

Empire Toolkit:

Currently one of the most commonly used hacker tools

- <https://www.powershell-empire.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

```
[Empire] Post-Exploitation Framework
=====
[Version] 2.5 | [Web] https://github.com/empireProject/Empire
=====
restart-vm-
tools
EMPIRE
=====
285 modules currently loaded
0 listeners currently active
0 agents currently active
(Empire) > |
```

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 SearchTerm.
```

```
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!

Network Session Hijacking

Very Common MFA Hack

- 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

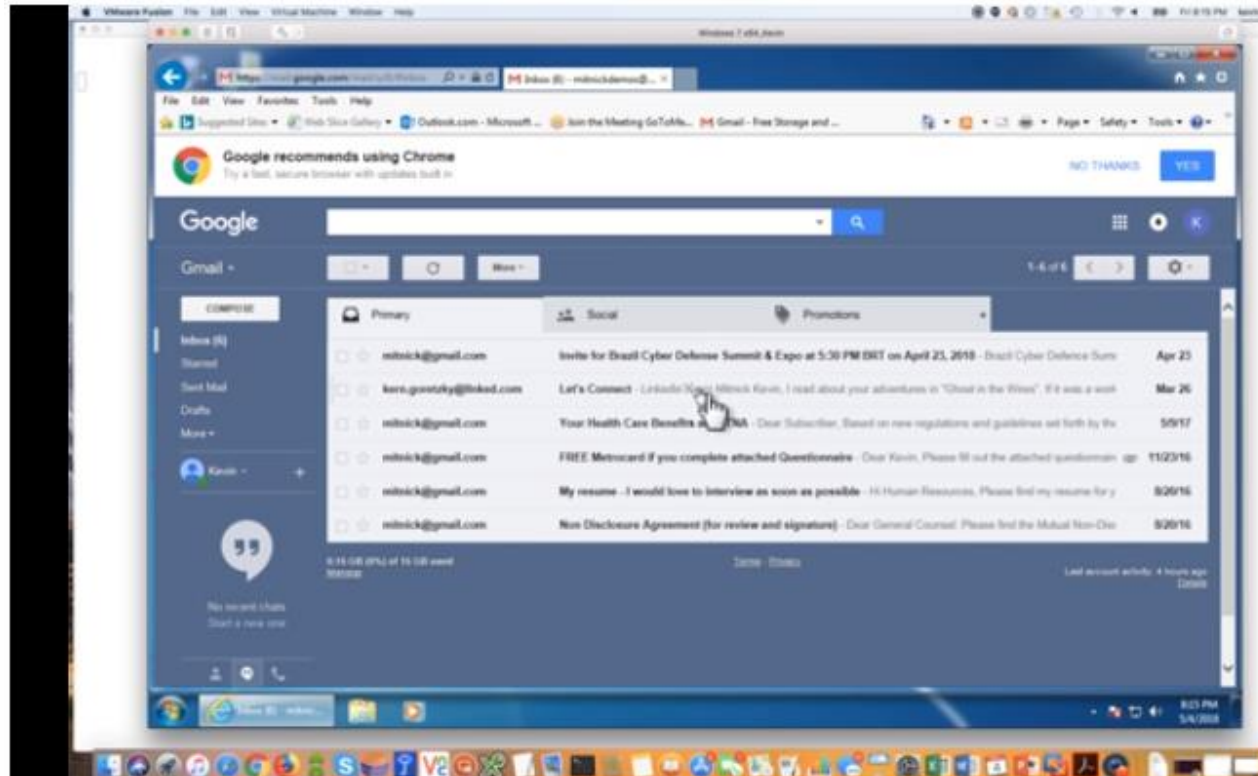
Network Session Hijacking Proxy Theft

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

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>

https://mail.google.com/mail/u/0/#inbox... Inbox (6) - mitnickdemos@... x

File Edit View Favorites Tools Help

Suggested Sites Web Slice Gallery Outlook.com - Microsoft ... Join the Meeting GoToMe... Gmail - Free Storage and ...

Google recommends using Chrome Try a fast, secure browser with updates built in NO THANKS YES

Google

Gmail - 1-6 of 6

COMPOSE

Inbox (6) Starred Sent Mail Drafts More + Kevin -

Primary Social Promotions +

<input type="checkbox"/>	<input type="checkbox"/>	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
<input type="checkbox"/>	<input type="checkbox"/>	kern.goretzky@lnked.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
<input type="checkbox"/>	<input type="checkbox"/>	mitnick@gmail.com	Your Health Care Benefits at AETNA - Dear Subscriber, Based on new regulations and guidelines set forth by the	5/9/17
<input type="checkbox"/>	<input type="checkbox"/>	mitnick@gmail.com	FREE Metrocard if you complete attached Questionnaire - Dear Kevin, Please fill out the attached questionnain	11/23/16
<input type="checkbox"/>	<input type="checkbox"/>	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
<input type="checkbox"/>	<input type="checkbox"/>	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

MFA Hacks

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

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

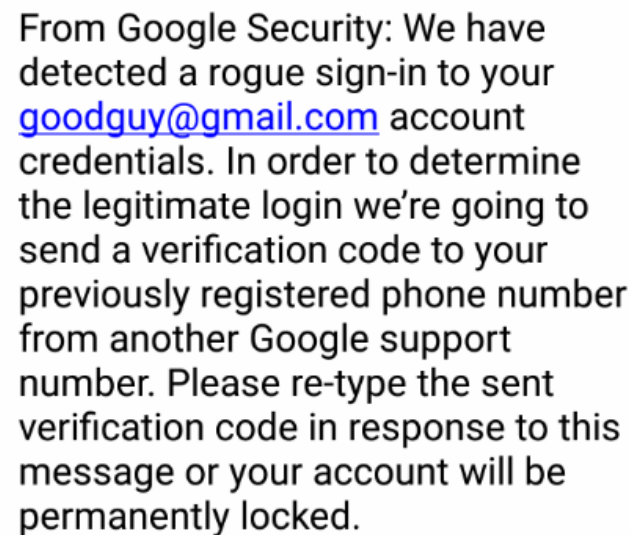
*SMS
Rogue
Recovery*

Rogue Recoveries

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



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.

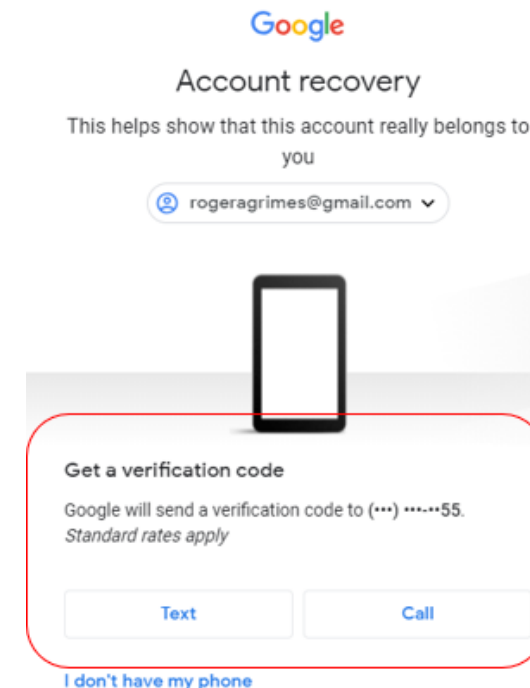
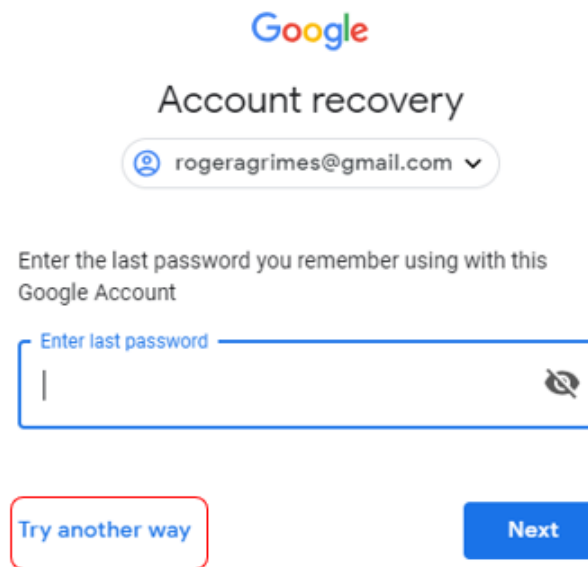
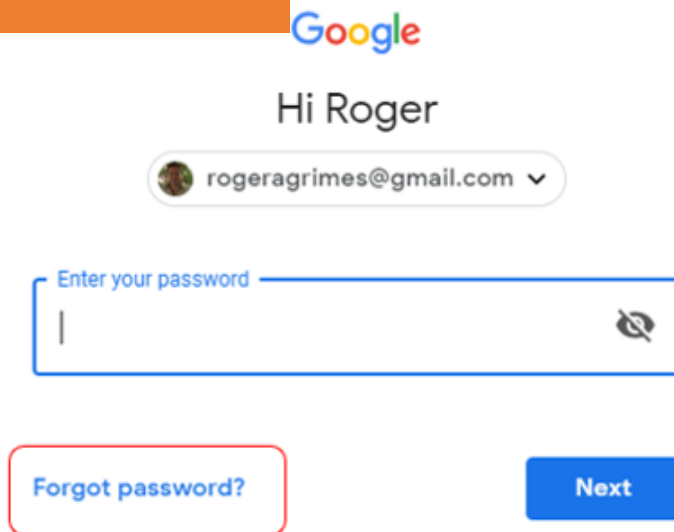
Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

**SMS
Rogue
Recovery**

Steps

2. Hacker forces your email account into SMS PIN recovery



Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery

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

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

Does the message arrive
unexpectedly?

Yes

Is it the first time the sender
has asked you to perform
requested action?

Yes

Does the request include a
"you need to do it NOW"
stressor?

Yes

If the request is malicious,
can performing it harm your
interests?

Yes

Confirm using an alternate
method before
accomplishing

Give "Red Flags" Training

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."

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

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-Like 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%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/2SnA7Fnm>

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-sajdkjndfjnbkasldjfbkajsdbfkjbasdf/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

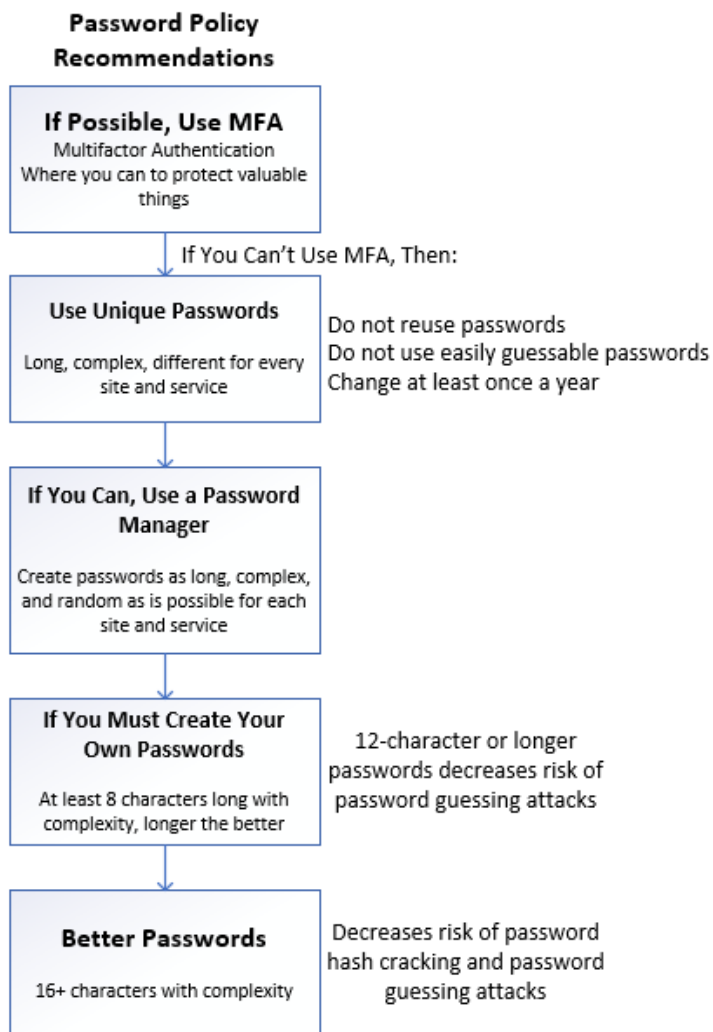
URLs which have hidden links to completely different web sites at the end.

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



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

My Password Policy Advice



Generating Industry-Leading Results and ROI

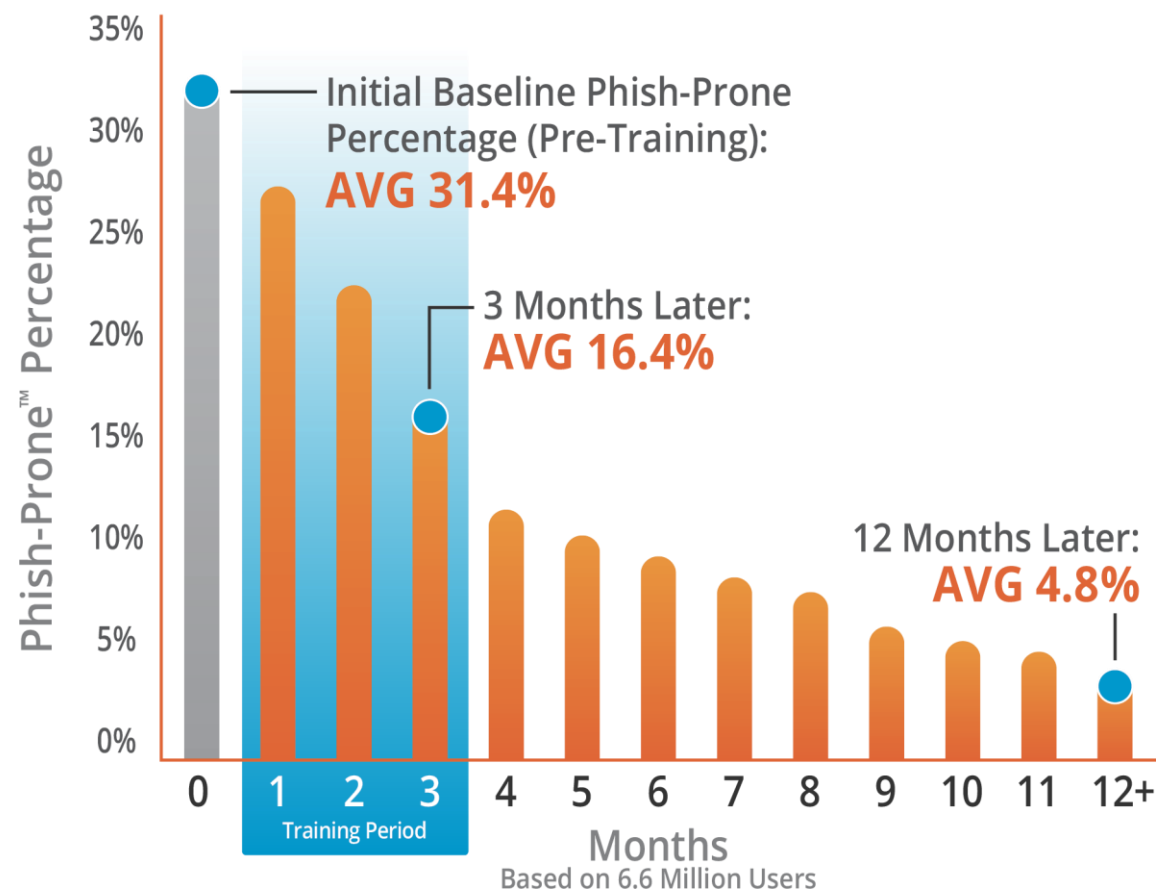
- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

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.

The KnowBe4 System Really Works



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