



# Third-Party Phishing:

**The New Spear-Phishing Attacks That  
Traditional Defenses Just Don't Stop**



**Erich Kron**  
Security Awareness  
Advocate, KnowBe4, Inc.  
**@ErichKron**



**Erich Kron**  
Security Awareness Advocate

## About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc...
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)<sup>2</sup>
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments



Certified Information  
Systems Security Professional



Certified Information  
Systems Security Professional

**ISSAP** Architecture

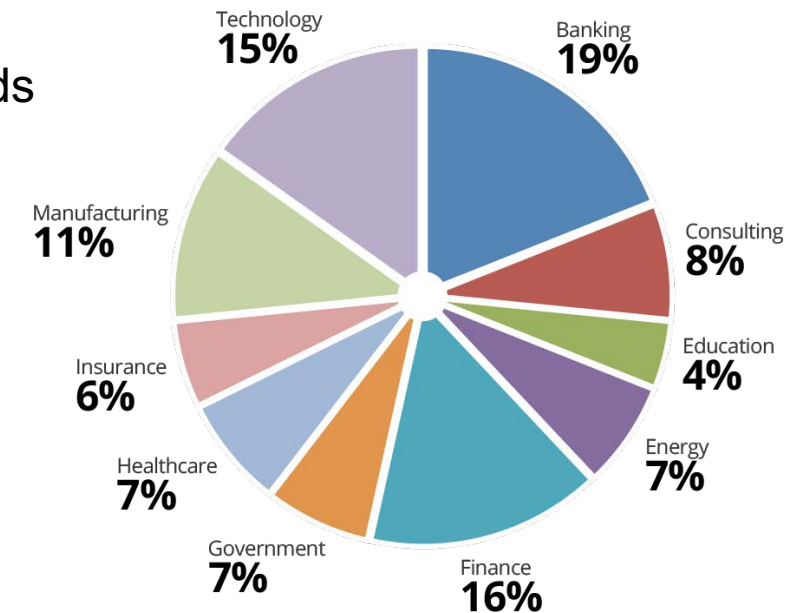
**Microsoft**  
**CERTIFIED**  
*IT Professional*





# 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
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



# Today's Presentation

- Examples of Real Third-Party Phishing Schemes
- What Doesn't Work
- How to Defend

# What is 3<sup>rd</sup> Party Phishing?

- Very targeted spear phishing
- Personal- or business-focused
- Email/Social Media/Phone to specific person
- Email/Social/Phone media request comes from person/organization receiver already trusts
- If email or social media, real email/account of 3<sup>rd</sup> party may be used
- Often trusted person's account is compromised
- AKA “lateral phishing”
- May involve “pre-texting”, multiple moves

# Agenda

- Examples of Real Third-Party Phishing Schemes
- What Doesn't Work
- How to Defend



# Example of Real 3<sup>rd</sup> Party Phishes

## Escrow Mortgage Fraud example

From: [REDACTED]

Sent: Tuesday, June 19, 2018 4:05 PM

To: [REDACTED]

Cc: [REDACTED]

Subject: [REDACTED]

Hi Mr. [REDACTED]

Attached please find the finalized settlement statement for closing. Please make arrangements to wire \$27,647.91.

Following this e-mail in a secure format will be our wire instructions. The password is the zip code of the property [REDACTED].

If you have any questions, please let me know.

Thank you!

Best Regards,

Megan V [REDACTED]

Licensed Title Agent/Business Development

|



Phone: [REDACTED]

# Example of Real 3<sup>rd</sup> Party Phishes

Escrow Mortgage Fraud example

[Redacted]

[Redacted]

**WIRING INFORMATION**

Our wiring instructions for the transaction referenced herein are as follows:

**To:** Title Agency [Redacted]  
Inc.

**Underwriter:** [Redacted] Title Insurance Company

**Bank:** Bank of America  
275 Valencia Blvd  
Brea, California 92823

**Routing No.:** 02600 [Redacted]

**Account Name:** Fidelity National Title [Redacted]

**Account No.:** 1257464 [Redacted]

**Swift Code:** BOF [Redacted]

**Please refer to our Escrow No.:** [Redacted] A18-59 [Redacted]

**For Reference Purposes:**

**Borrower(s):** [Redacted]

**Property:** [Redacted]

\*\*\*\*\*

**Attention Lenders:**  
**Email Loan Packages to**  
[Redacted]

**Packages MUST be received 24 hours prior to closing date.**

**PLEASE NOTE: OUR OFFICE DOES NOT ACCEPT ACH TRANSFERS. THESE INSTRUCTIONS ARE FOR THE PURPOSE OF SENDING WIRE TRANSFERS ONLY.**

**\*\*\*\*\*DON'T BE A VICTIM\*\*\*\*\***

Due to recent internet fraud and email hacking, we are hereby advising all of our clients that for your protection, call [Redacted] Inc. to verify any and all wire instructions you receive BEFORE initiating a wire transfer.

[Redacted] Inc., its affiliates and underwriters will not be held liable if you become a victim of this fraud.

Over the counter deposits will not be accepted at the bank.



# Example of Real 3<sup>rd</sup> Party Phishes

Payroll Fraud example

From: [REDACTED]

Sent: Friday, August 23, 2019 6:47 PM

To: [REDACTED]

Subject: My Payroll Update

Hello [REDACTED] are you on desk now? I have recently changed bank and would like to have my direct deposit change to a new account. Having technical error on my end. Can you email me the DD form or i can send you my banking information so you can effect the change for me.  
|  
I need your prompt response regarding this.

Thanks

[REDACTED]  
Chief Operating Officer

Sent from my iPhone

Sent to only person in company responsible for payroll changes

# Fake Facebook Tech Support Scams

## Fraud Steps

1. You complain on vendor's Facebook or social media site about something related to vendor's product or service
2. You receive a message or email purporting to be from the vendor responding to your claim
  - Email address they are using is look-alike/sound-alike of the real domain
3. They apologize and offer you some incredible benefit for "being a loyal customer"
4. They ask for your credit card info to confirm the "gift" coming your way or your login account information to "confirm your account"

# Example of Real 3<sup>rd</sup> Party Phishes

Sent to me after posting on APEC Facebook site about how much I loved the product after buying

Invoice - INV-12813 from APEC Water Systems



APEC Water Systems <reminders@freedinkingwater.com> (APEC Water Systems via bnc3.mailjet.com)

To: Roger Grimes

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.  
The actual sender of this message is different than the normal sender. Click here to learn more.

Action Items



**APEC WATER**  
FREE DRINKING WATER.com

Invoice #INV-12813

Dear Client,

Thank you for your business. We do expect payment by 2019-11-24, so please process this invoice within that time. There will be a 2% interest charge per month on late invoices. Your invoice can be viewed, printed and downloaded from the link below.

INVOICE AMOUNT

**\$1,729.70**

[http://s0hu.mj.am/lnk/anaaafkavskaaajuiiv4aag0owacaaiaik0zkajdciaafftwbdsctjw07ew\\_kjtpcf99ozyekjqabn7a/2/oc6f4hcn5mb\\_6ivnyyayg/ahr0chm6ly9kzn0aw5hdglvbnbyb3rly3quy29tI0njbznvawnlsuq9mi1iztjntgymwrmymnmzwe3owu5mjq4ody4zjdmztrimwjlmgjinzezota2zjrmzdmzmfmotkwmdk5ytg4zgm4mdm](http://s0hu.mj.am/lnk/anaaafkavskaaajuiiv4aag0owacaaiaik0zkajdciaafftwbdsctjw07ew_kjtpcf99ozyekjqabn7a/2/oc6f4hcn5mb_6ivnyyayg/ahr0chm6ly9kzn0aw5hdglvbnbyb3rly3quy29tI0njbznvawnlsuq9mi1iztjntgymwrmymnmzwe3owu5mjq4ody4zjdmztrimwjlmgjinzezota2zjrmzdmzmfmotkwmdk5ytg4zgm4mdm)  
Click or tap to follow link.

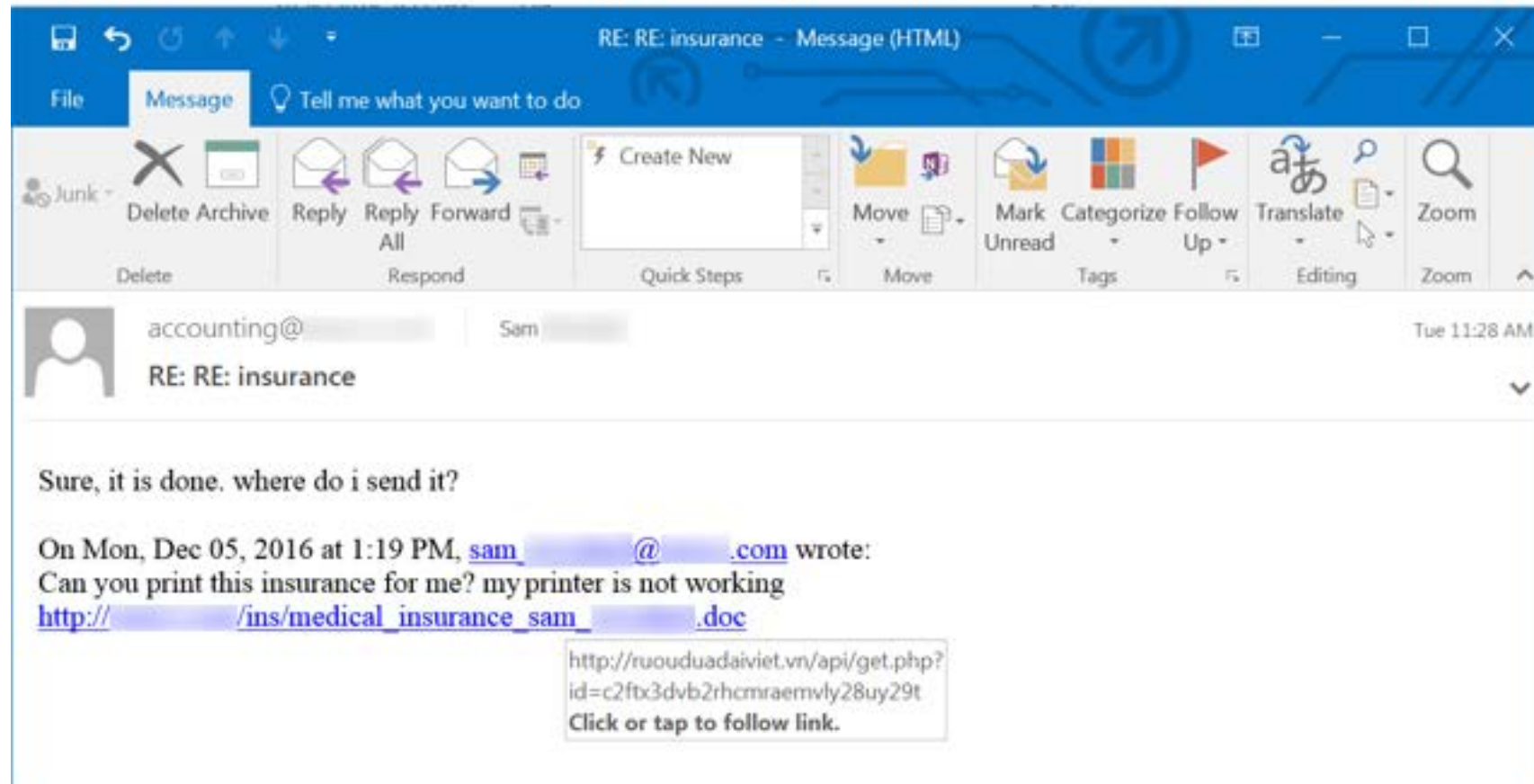
Invoice No INV-12813  
Invoice Date 2019-10-24  
Due Date 2019-11-24

[VIEW INVOICE](#)

Regards,

Pam Swartzentruber  
APEC Water Systems

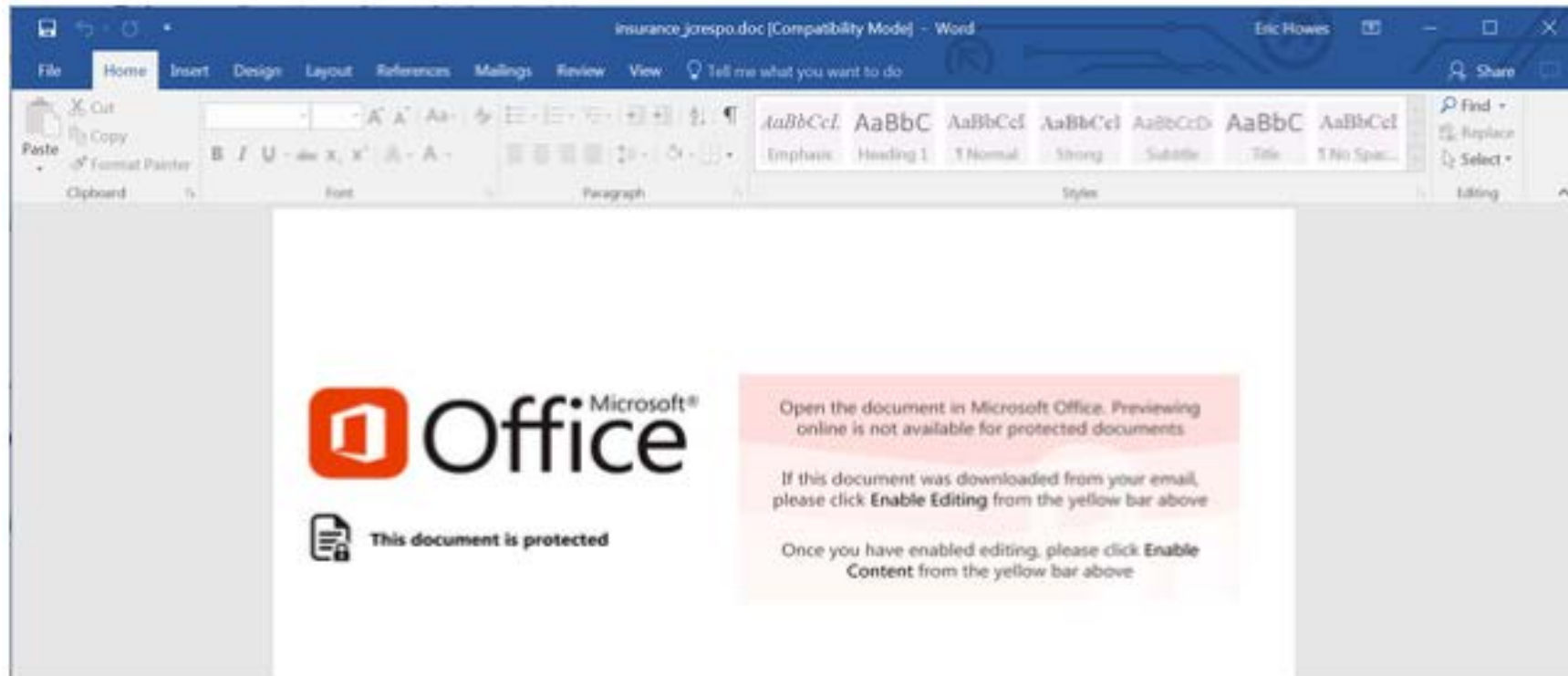
# Example of Real 3<sup>rd</sup> Party Phishes



Spooled email thread, innocent request



# Example of Real 3<sup>rd</sup> Party Phishes



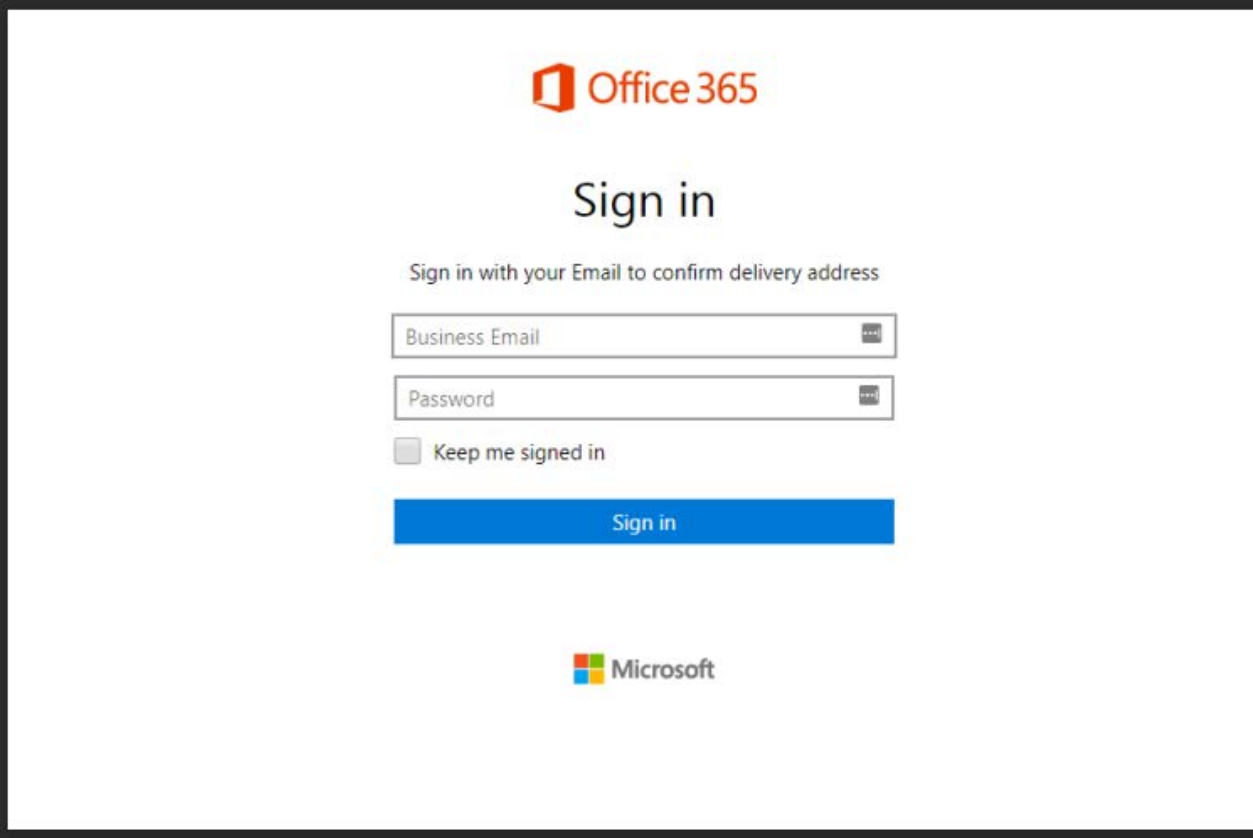
“Helpful instructions” for opening document

# Example of Real 3<sup>rd</sup> Party Phishes

## Fake O365 portals

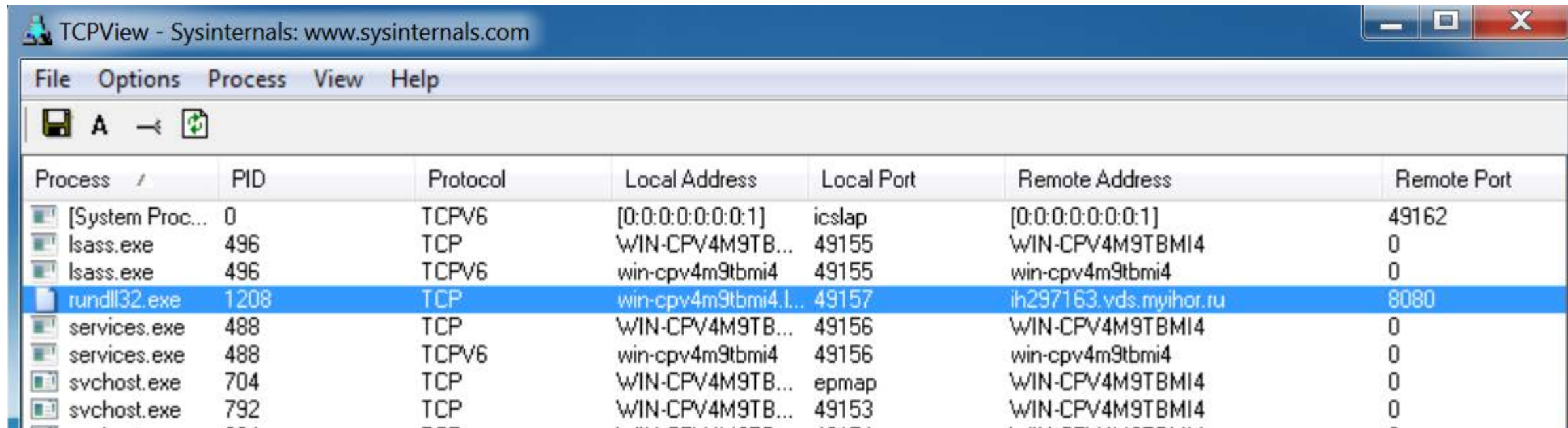
Makes you trust document more

They get your credentials



The image shows a screenshot of a fake Office 365 sign-in page. At the top, there is a red Office 365 logo. Below it, the text "Sign in" is centered. Underneath, a smaller text says "Sign in with your Email to confirm delivery address". There are two input fields: "Business Email" and "Password", both with placeholder text and a small icon on the right. Below the password field is a checkbox labeled "Keep me signed in". A blue "Sign in" button is positioned below the checkbox. At the bottom, there is a Microsoft logo.

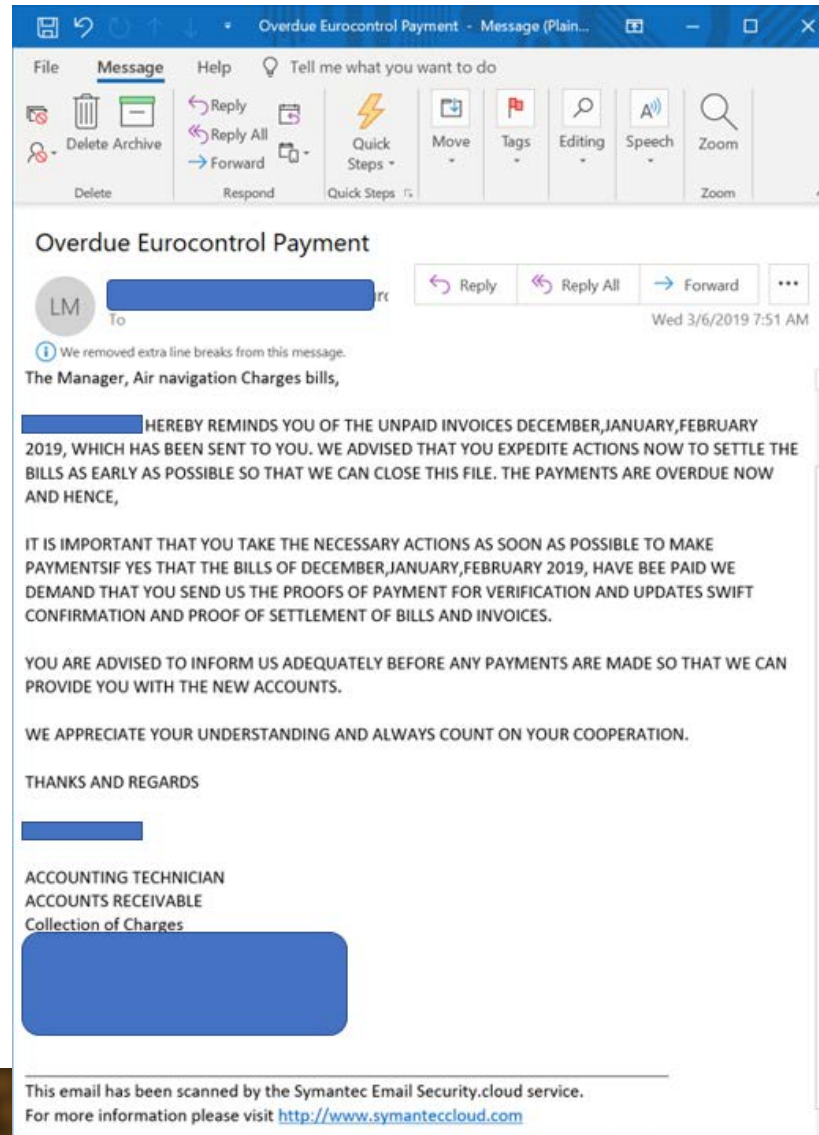
# Example of Real 3<sup>rd</sup> Party Phishes



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
[System Proc...	0	TCPV6	[0:0:0:0:0:0:1]	icslap	[0:0:0:0:0:0:1]	49162
lsass.exe	496	TCP	WIN-CPV4M9TB...	49155	WIN-CPV4M9TBMi4	0
lsass.exe	496	TCPV6	win-cpv4m9tbmi4	49155	win-cpv4m9tbmi4	0
rundll32.exe	1208	TCP	win-cpv4m9tbmi4.L...	49157	ih297163.vds.myihor.ru	8080
services.exe	488	TCP	WIN-CPV4M9TB...	49156	WIN-CPV4M9TBMi4	0
services.exe	488	TCPV6	win-cpv4m9tbmi4	49156	win-cpv4m9tbmi4	0
svchost.exe	704	TCP	WIN-CPV4M9TB...	epmap	WIN-CPV4M9TBMi4	0
svchost.exe	792	TCP	WIN-CPV4M9TB...	49153	WIN-CPV4M9TBMi4	0

If macro was enabled, launches Fareit password stealing trojan malware

# Example of Real 3<sup>rd</sup> Party Phishes



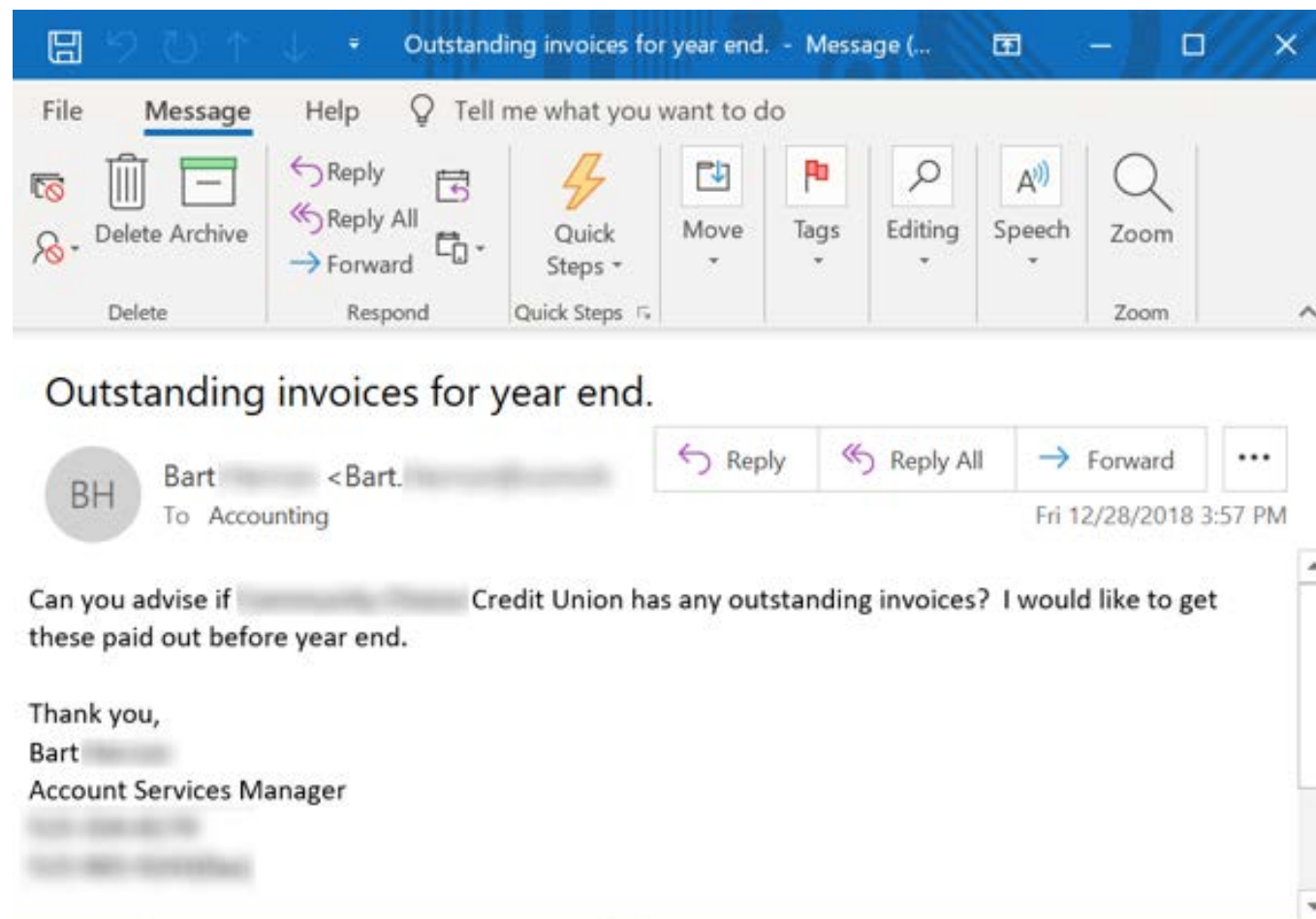


# Fake A/P Instruction Change

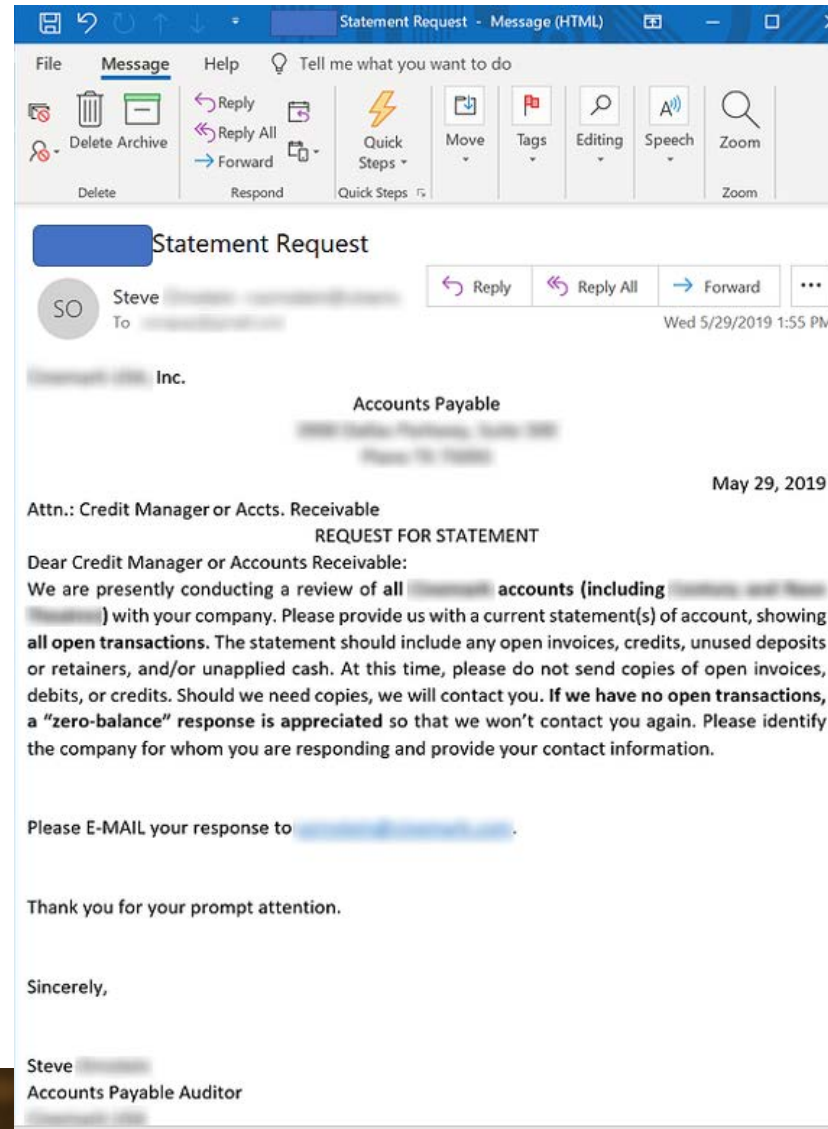
## Fraud Steps

1. Vendor who you regularly pay sends email telling you to update payment information (e.g. new bank, new account number, new wiring instructions, new A/P person to interact with, new company who is now handling payments, etc.)
  - They tell you not to change anything else or don't send any money now
2. 3<sup>rd</sup> party's email client has a rule intercepting any confirmation emails sent back to 3<sup>rd</sup> party from victim
3. Attackers just wait
4. When the normal invoicing happens, payment goes to new place
5. Usually not detected for weeks to months

# Example of Real 3<sup>rd</sup> Party Phishes



# Example of Real 3<sup>rd</sup> Party Phishes



# Example of Real 3<sup>rd</sup> Party Phishes

Compromised vendor

**From:** [REDACTED]  
**Sent:** Tuesday, October 8, 2019 9:18 AM  
**To:** [REDACTED]  
**Subject:** [EXTERNAL] Requested documents for Michael

Michael,

Please find [attached documents](#) regarding your order.

Regards,

[REDACTED]

[Unsubscribe](#) from email communications

[REDACTED]

erry Rd. SE

89



# Example of Real 3<sup>rd</sup> Party Phishes

Email from vendor announcing compromise shown on previous slide

**From:** [REDACTED]  
**Sent:** Tuesday, October 8, 2019 2:27 PM  
**To:** [REDACTED]  
**Subject:** [EXTERNAL] Important Notice / Impersonation

[REDACTED] uses an independent third-party to provide marketing services. A database maintained by that third party was compromised by an unknown actor.

That unknown actor sent a large number of e-mails this morning from the [REDACTED] account on that third-party server. Some, for example, were titled "Requested documents for".

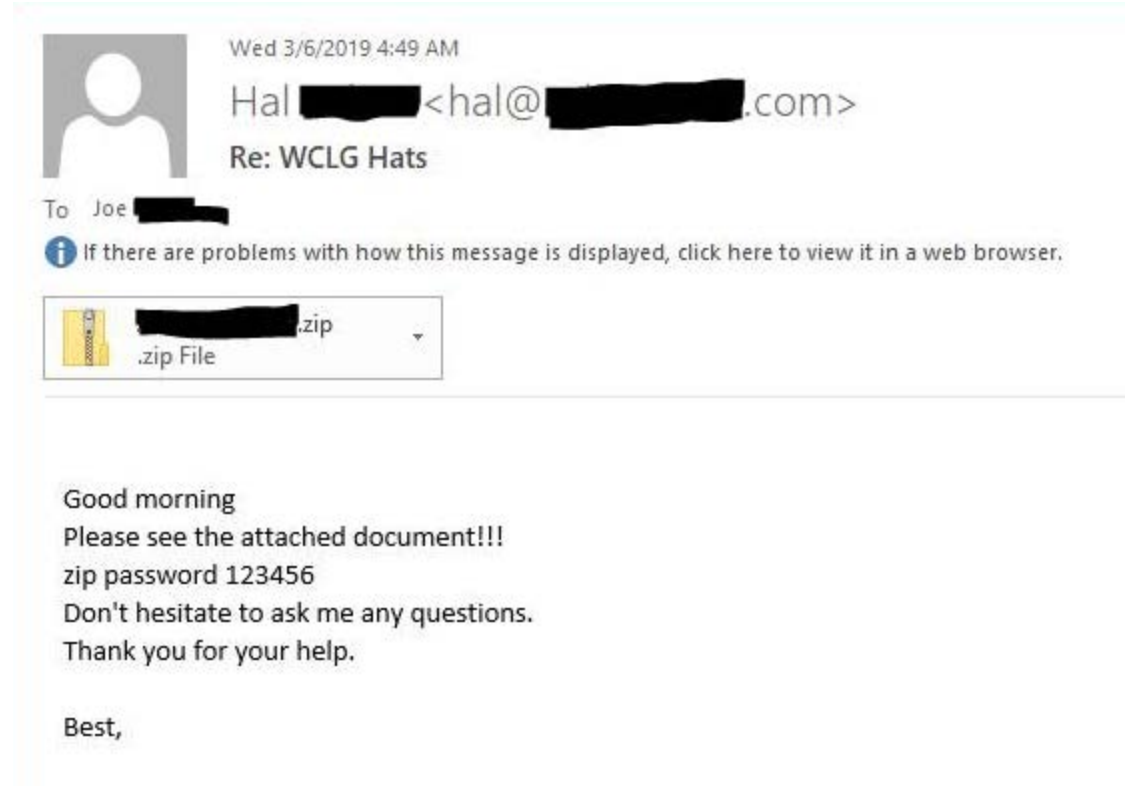
These emails may contain malware. Delete them immediately. They were not sent from [REDACTED]. We are working with the independent third party to further improve controls around this marketing database.

We apologize for any inconvenience this has caused.

[REDACTED]  
[REDACTED]  
Director of Lender Strategy  
[REDACTED]  
[Update Email Preferences](#)

# Example of Real 3<sup>rd</sup> Party Phishes

## Thread injection



Sent in response to a real existing conversation, but strange response

# Example of Real 3<sup>rd</sup> Party Phishes

Hello,

We have updated your [redacted] signing page to a more security guaranteed platform following the increased target on HR and payroll practitioners. Please proceed to sign in below to get familiar with the new sign in process.

[https://\[redacted\].com](https://[redacted].com)

Having trouble with your sign in? [Contact support](#)

Following this new development our updated terms and privacy policy will be sent out on November 1<sup>st</sup> 2019.

For more clarification and answers to your questions contact your administrator.

Thank you

[redacted]

[redacted] are registered trademarks, and [redacted] are trademarks,  
of [redacted] Copyright © 2019 [redacted] ALL RIGHTS RESERVED. #0916L [redacted]

This is a message from [redacted] To remove yourself from our marketing list, please [click here to opt out](#). You can also write to [redacted] Boulevard, Roseland, NJ [redacted] – Attn: Marketing Dept. - Unsubscribe and tell us to unsubscribe you. You may resubscribe to [redacted] marketing emails at any time by [clicking here](#). If your company is currently receiving services from [redacted] this will not impact the electronic messages we send to you for purposes of delivering such services. For additional information on our privacy practices, see [redacted] [Online Privacy Statement](#). Copyright © 2019 [redacted] LLC

# Example of Real 3<sup>rd</sup> Party Phishes

From: [REDACTED]

Sent: Friday, October 11, 2019 9:44 AM

To: [REDACTED]

Subject: Urgently Needed!!.. [REDACTED]

How are you? I need a favor from you.

I need to get an iTunes gift card for my Niece, Its her birthday but i can't do this now because I'm currently traveling.

i tried purchasing online but unfortunately no luck with that..Can you get it from any store around you?

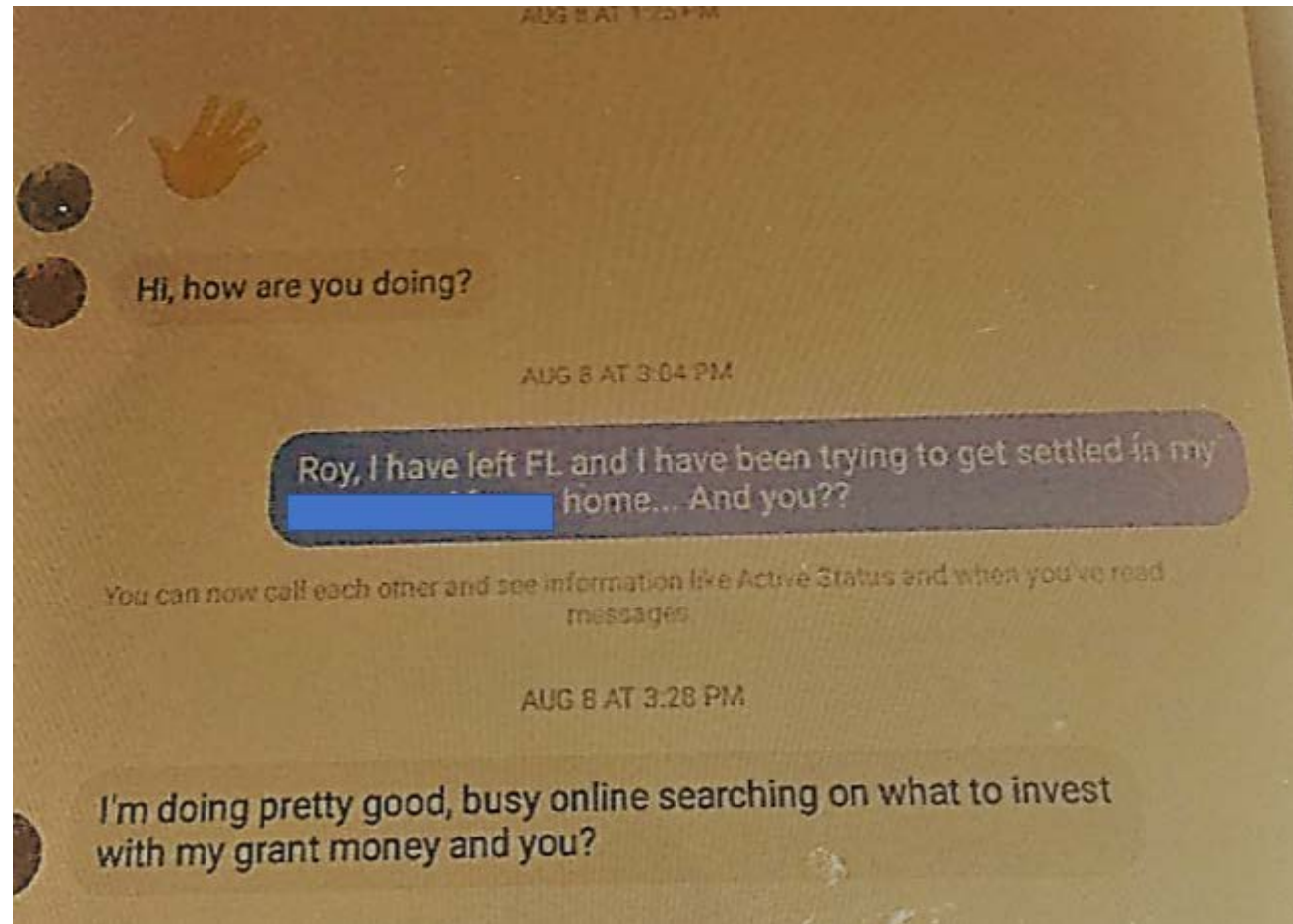
I'll pay back as soon as i am back. Kindly let me know if you can handle this.

THANKS  
[REDACTED]



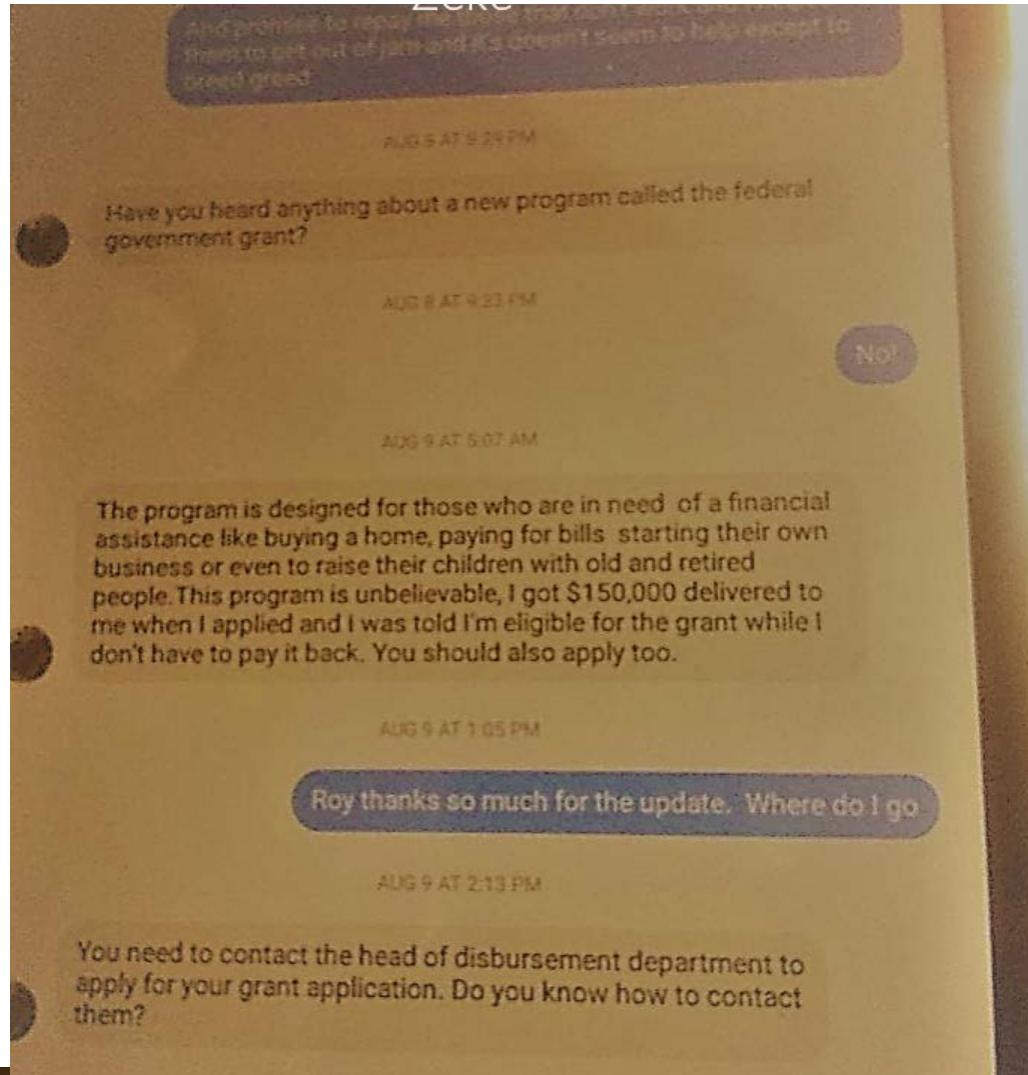
# Example of Real 3<sup>rd</sup> Party Phishes

## Twitter 3<sup>rd</sup> Party Scam Example



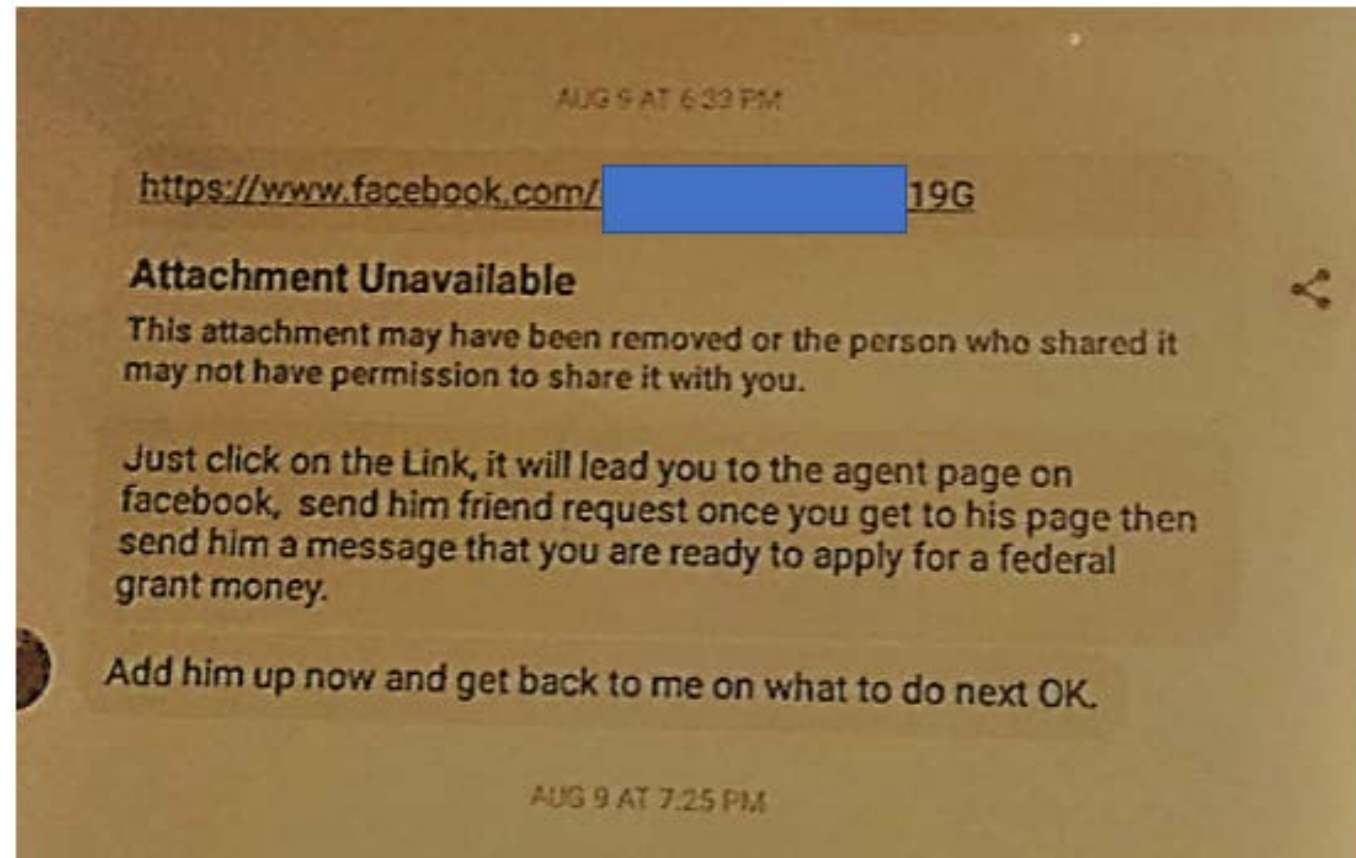
# Example Real 3<sup>rd</sup> Party Phishes

## Twitter 3<sup>rd</sup> Party Scam Example



# Example Real 3<sup>rd</sup> Party Phishes

## Twitter 3<sup>rd</sup> Party Scam Example



# Example Real 3<sup>rd</sup> Party Phishes

## Voice Phishing (Vishing) - Examples

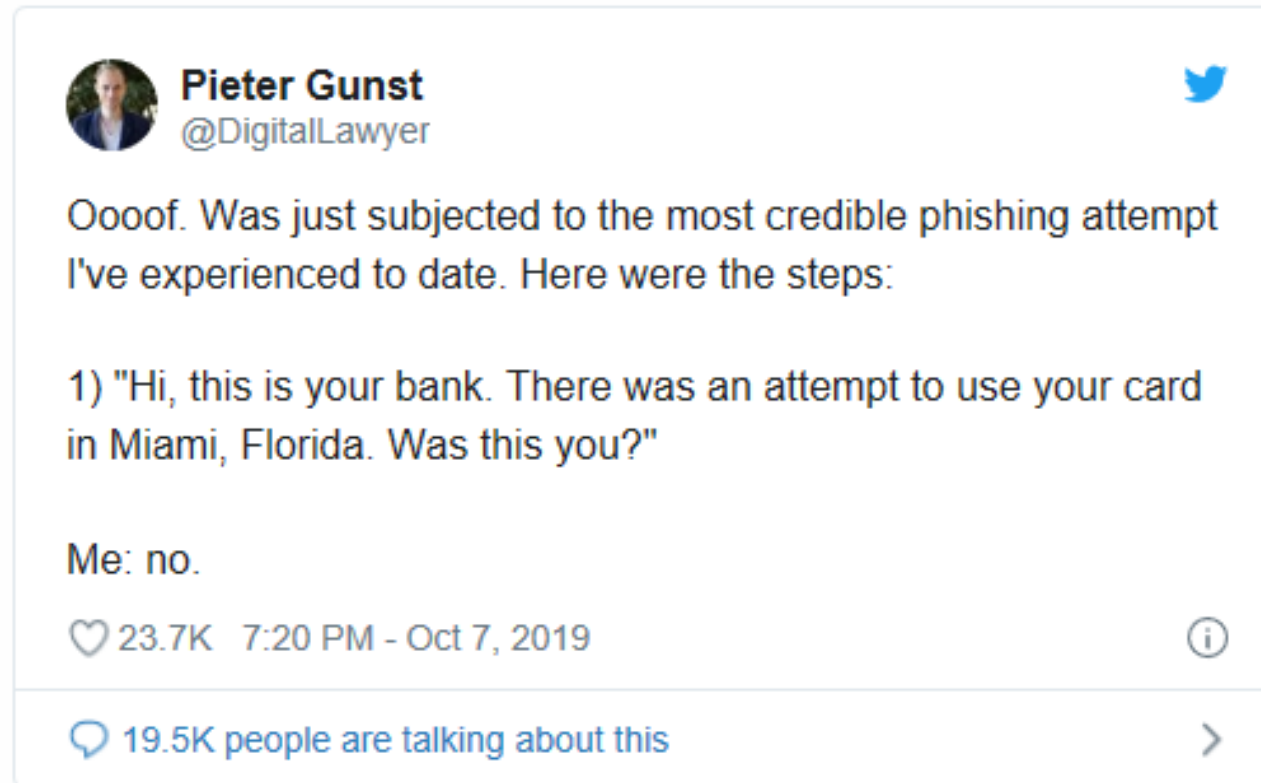
- Microsoft Technical Support fraud
- Bank account fake fraud report
- PayPal fake fraud report
- Airline ticket purchase fake fraud report
- Hotel points fake fraud report

\*As you accidentally give up more information, the more real information they give you



# Example of Real 3<sup>rd</sup> Party Phishes

Vishing – Phone Phishing



# Example of Real 3<sup>rd</sup> Party Phishes

Then it got weird.

After confirming that he did not use his card in Miami, Gunst says the caller told him that the transaction had been blocked, and then asked him for his member number.

Gunst then received a legitimate verification pin from the bank's regular number via text, which he promptly read back to the caller -- not realizing that it was a password reset code.

The person on the line -- a scammer -- was in. She could access his account and began to read off recent transactions that Gunst had actually made, lending a bit more credibility to the call.

Then came the next question, which immediately set off a red flag: "We now want to block the pin on your account, so you get a fraud alert when it is used again. What is your pin?"

<https://www.msn.com/en-us/news/crime/a-scam-targeting-americans-over-the-phone-has-resulted-in-millions-of-dollars-lost-to-hackers-dont-be-the-next-victim/ar-AAJpE2J>

# Rogue Recoveries

## SMS Rogue Recovery

### Hacking Into Your Email Using Recovery Methods

#### SMS Rogue Recovery Hack

- There is an inherent problem in that SMS message origination cannot be easily authenticated within SMS itself
- Anyone can claim to be anyone

To pull off hacker must have:

- Your email address and associated phone number

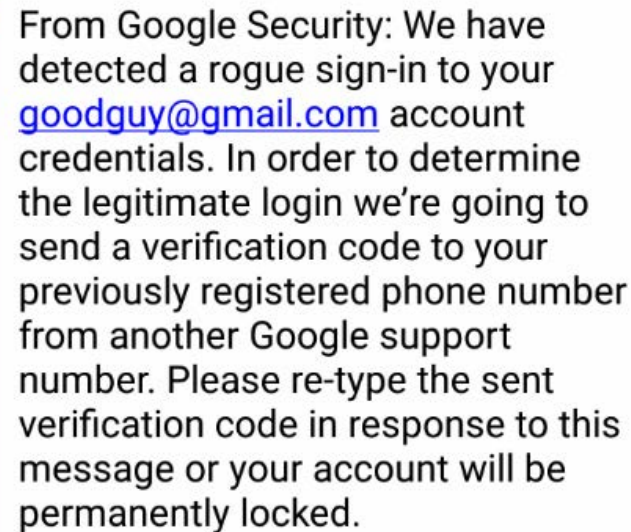
# Rogue Recoveries

## SMS Rogue Recovery

### Hacking Into Your Email Using Recovery Methods

Steps:

1. Hacker sends you a text pretending to be from your email provider asking for your forthcoming SMS PIN reset code



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.

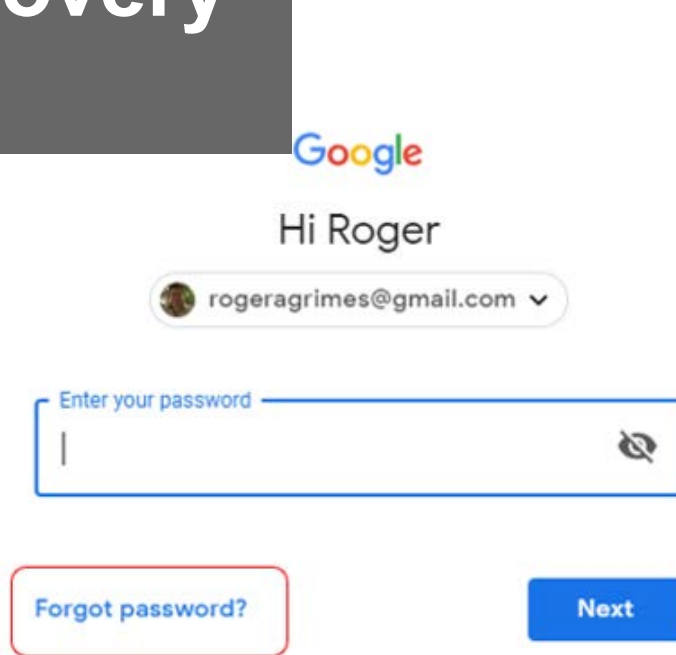
# Rogue Recoveries

## Hacking Into Your Email Using Recovery Methods

Steps:

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

### SMS Rogue Recovery



Google

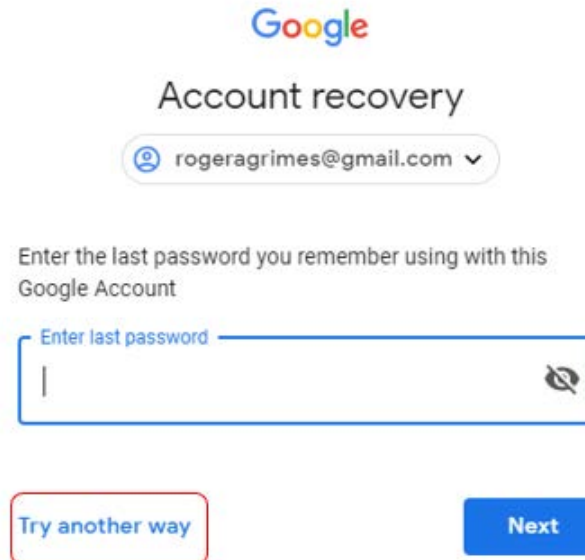
Hi Roger

rogeragrimes@gmail.com ▼

Enter your password

Forgot password?

Next



Google

Account recovery

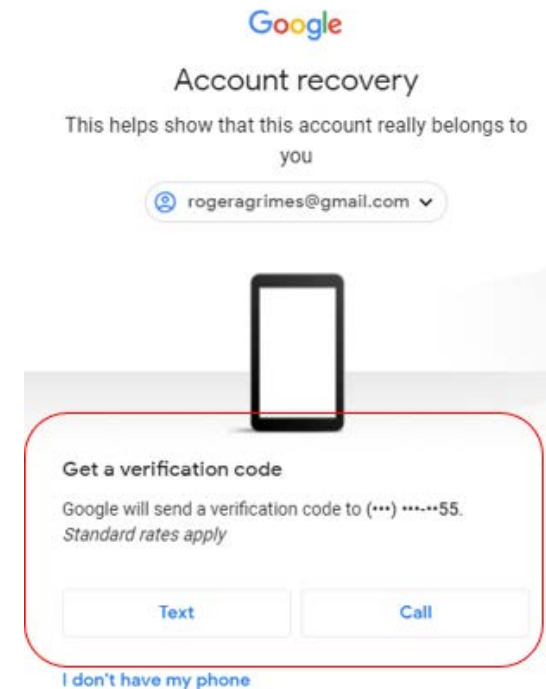
rogeragrimes@gmail.com ▼

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 (...) .....55.  
Standard rates apply

Text Call

[I don't have my phone](#)



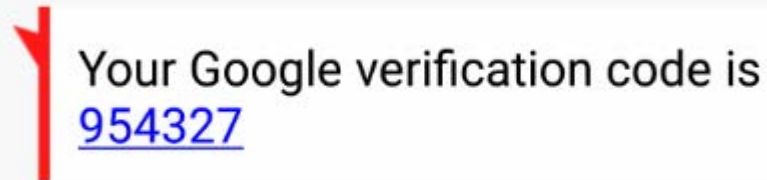
# Rogue Recoveries

## SMS Rogue Recovery

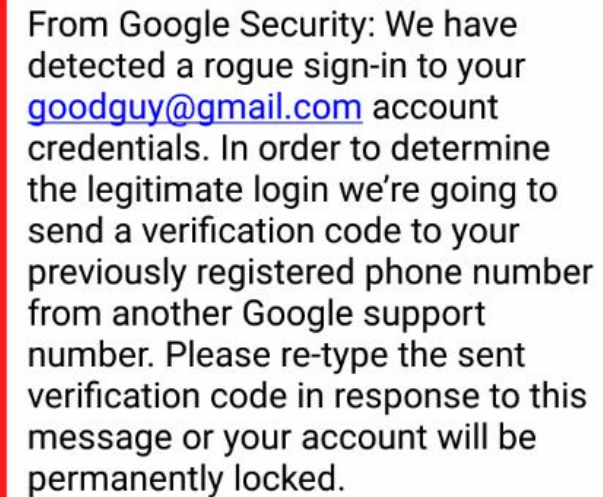
### Hacking Into Your Email Using Recovery Methods

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](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.

[954327](#)

Sent

# Agenda

- Examples of Third-Party Phishing Schemes
- What Doesn't Work
- How to Defend

# What Doesn't Work

- Anti-phishing filters
- Being worried about:
  - Emails from strangers
  - Strange email addresses from people you know
- Blacklists/whitelists
- Reputation services
- Red/Green (second) systems
- DMARC, DKIM, SPF
- Network/Pattern/Anomaly Analysis

# What Doesn't Work

- Educating users about general examples of regular phishing
  - Although you should still do this
  - Just also educate about 3<sup>rd</sup> party phishes

# Agenda

- Examples of Third-Party Phishing Schemes
- What Doesn't Work
- How to Defend



# How to Defend

- Risk Identification
- Tools
- Education
- Policy Changes

# How to Defend

## Risk Identification

- Who is most at risk for these types of attacks?
  - Employees who can move money and pay invoices
  - People with elevated access to systems and data
  - C-Level employees

Give them specific training and simulated phishing testing

# How to Defend

## Look for Malicious Email Rules and Forms

Phishes often create malicious email client rules and forms on 3<sup>rd</sup> party to intercept emails from victim

- Look for any non-default email rules and forms
  - <https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/Get-AllTenantRulesAndForms.ps1>
  - Notruler – <https://github.com/sensepost/notruler>
- Verify that they aren't malicious
- Make sure your event log system looks for new email rules and forms

# How to Defend

## Education

- Share awareness of what's going on
  - Use this slide deck
- Specific simulated phishing campaigns

# How to Defend

## Education

### What Do We Look For?

- Money/gift card/banking info requests
- Strange URLs
- Do URL recognition training
  - “Hovering”
  - Recognizing true domain name



# URL Training

Help Users Understand How to Read URL Domains to Spot the Dubious URL Links

## Microsoft Office-365

Hello roger\_grimes@infoworld.com  
Sorry, due to a problem with your roger\_grimes@infoworld.com subscription, your email has been suspended.  
If you'd like to continue receiving this email, please click the link below to re-verify your email address.

RE-VERIFY

 [https://devopsnw.com/login.microsoftonline.com?userid=roger\\_grimes@infoworld.com](https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com)

This action

Thanks,  
The Microsoft Office

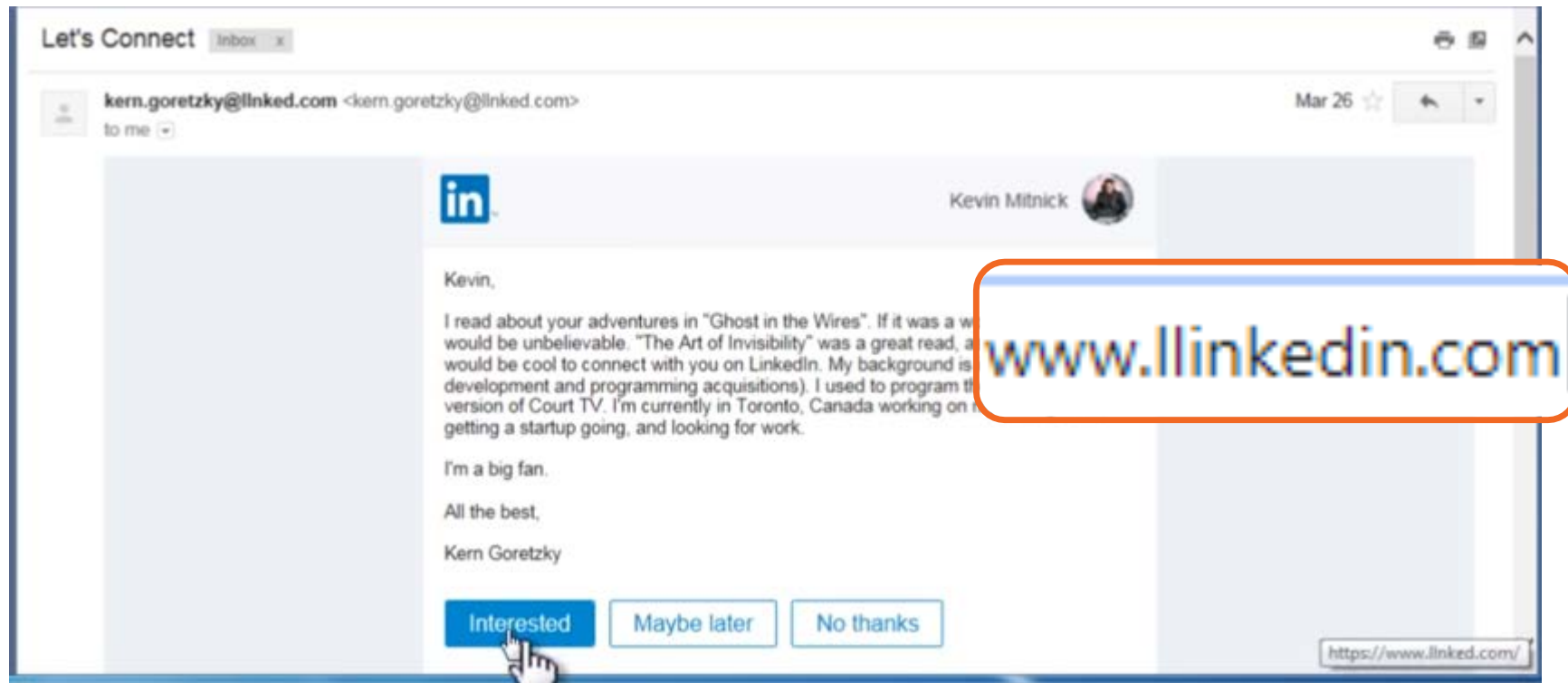
This message was sent from the email address is not monitored. Do not reply to this message.  
[Privacy](#) | [Legal Notices](#)

**We hope to continue serving you.**  
**Microsoft Corporation**  
One MSN Way, Redmond, WA 98052

We respects your privacy, Please read our online [Privacy Statement](#).  
This Message was sent from an unmonitored e-mail address. Please do not reply this message.

# URL Training

Help Users Understand How to Read URL Domains to Spot the Dubious URL Links



# Real-Life Hints

## URL Training

- Help Users Understand How to Read URL Domains to Spot the Dubious URL Links

Bank of America Alert: Unlock Your Account Important Message From Bank Of America®



Bank of America <BankofAmerica@customerloyalty.accounts.com>(Bank of America via shakawaaye.com)  
To Roger Grimes

Update Your Powered By office 365



Office 365 <no-reply1@soft.com>(Office 365 via ds01099.snspreview7.com.au)  
To Roger Grimes

Your Shipping Documents.



MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)  
To roger\_grimes@infoworld.com

Ticket #: 5711310



Microsoftonline <v5pz@onmicrosoft.com>  
To roger\_grimes@infoworld.com



If there are problems with how this message is displayed, click here to view it in a web browser.



# How to Defend

## Education

### What Do We Look For?

- New action requests never requested before
- Strange attachment name or file format
- New action/communication pathways
- Strange Timing (e.g. email arrived at night and is usual in doing so)
- Includes “stressor events”
  - If an email contains one of these, time to slow down and evaluate what we are being asked to do

# How to Defend

## Policy Changes

- Policy needs to support security-aware culture and desired behaviors

# How to Defend

## Policy Changes

### Examples:

- Can't update banking or payment information without prior voice confirmation from a known good contact name and number
- Can't purchase gift cards without voice confirmation
- Mortgagee's must call previously verbally disclosed phone number to verify any escrow transfers
- Let third parties know policies and rules ahead of time



# The KnowBe4 Security Awareness Program WORKS



## Baseline Testing

Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.



## 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, hundreds of templates with unlimited usage, and community phishing templates.



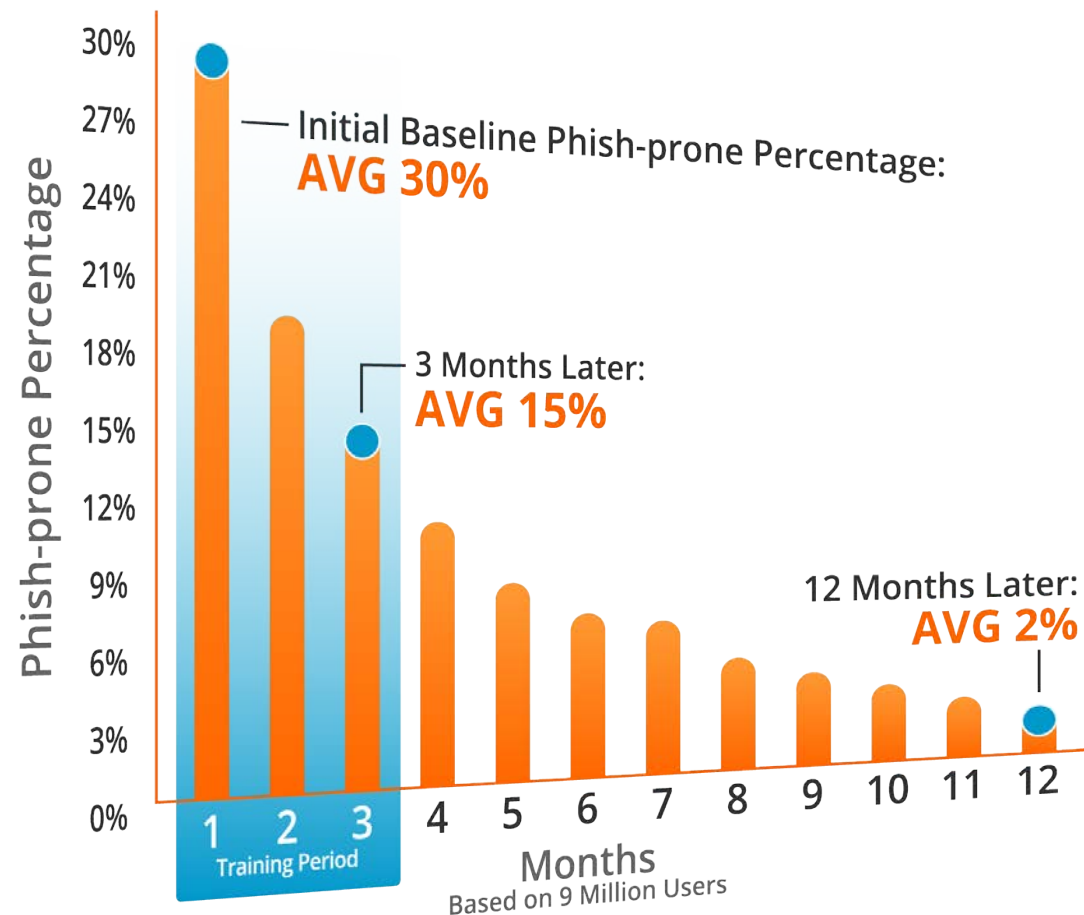
## See the Results

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



# Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)



# 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

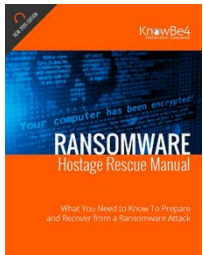


Training Preview



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.



### 12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

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

# Questions?





# Thank You!

**Erich Kron – Security Awareness Advocate**  
**ErichK@KnowBe4.com | @KB4Erich | @ErichKron**

**KnowBe4**  
Human error. Conquered.

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