

Kevin A. McGrail  
kmcgrail@InfraShield.com



# Minimize Social Engineering Exposure



# Introduction

Kevin A. McGrail

Director, Business Growth @ InfraShield.com

Google G Suite TC, GDE & Ambassador

Member, Apache Software Foundation



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



# Security Expertise

Reported FirstPay (& Form 843)

Apache SpamAssassin

KAM.cf

Helped with the first IDS

MIMEDefang

Apology letter from the FBI



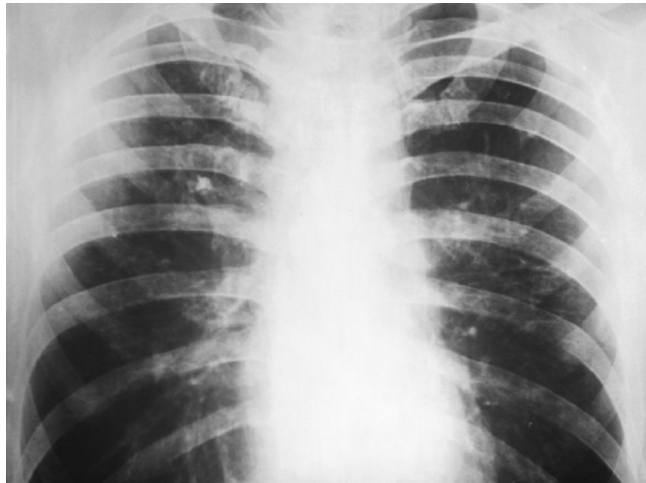
# Tone Setters



# Everyone & Anything \*IS\* a Target

Law firms receive Severance Phish, Payroll Firms receive ACH Phish.  
Even X-rays are targeted:

<https://digitalguardian.com/blog/whats-value-stolen-chest-x-ray-more-youd-think>





# Opportunistic vs. Persistent Adversaries

- Hive/Herd versus Targeted
- Scale of Economies
- Doesn't stay \$20
- Money Handlers are the #1 Target



# Phishing isn't just about Email

- Personal Interactions
- Unexpected Value
- Steganography
- Unintended Leakage
- Social Media
- Job Inquiries
- Invoice Scams
- SMShing
- OSINT







# Spear Phishing on Business Social Media



Invitations (4)

Manage all

	<div><b>Rohit Mishra</b> Computer Operator at SAIC SAIC</div>	Ignore	Accept
	<div><b>Dora Shelly</b> Sales Manager at SAIC SAIC</div>	Ignore	Accept
	<div><b>Subrata Pandit</b> Software Engineer at SAIC SAIC</div>	Ignore	Accept
	<div><b>giakhanh accxi</b> Sales Manager at SAIC SAIC</div>	Ignore	Accept

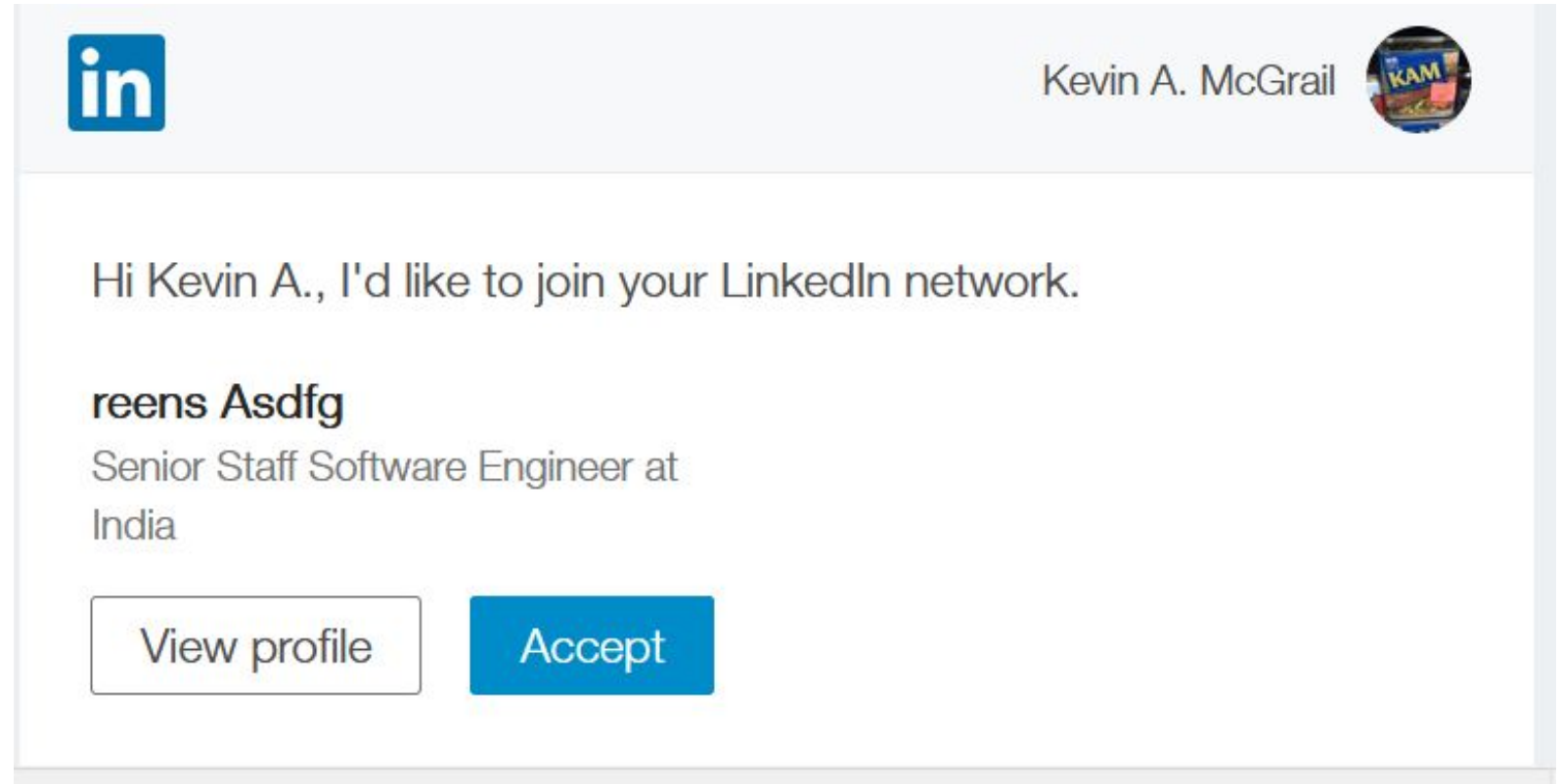
See all 4 invitations





# Some are Quite Silly....

Do I know your  
father, Qwerty  
Asdfg?



# The Risk of Job Inquiries

You have unread messages from **Greg**



**Greg Buckis**

Greetings Sir,  
I was hoping if you would love to explore a promising career opening as VP Finance at Microsoft corporation as I find your profile very interesting, kindly be advised that the afore...  
[see more](#)


<https://nakedsecurity.sophos.com/2019/01/21/attackers-used-a-linkedin-job-ad-and-skype-call-to-breach-banks-defences/>



# “Invoice” Scams

“This notice is not a bill...”

Not all scams are illegal!



Domain Name Expiration Notice  
visit us at [www.idns.ac](http://www.idns.ac)

As a courtesy to domain name holders, we are sending you this notification of the domain name registration that is due to expire in the next few months. When you switch today to Internet Domain Name Services, you can take advantage of our best savings. Your registration for: [redacted] will expire on **December 4, 2018**. Act today!

**Domain name:** [redacted]  
**Reply Requested By:** September 24, 2018

You must renew your domain name to retain exclusive rights to it on the Web, and now is the time to transfer and renew your name from your current Registrar to Internet Domain Name Services. Failure to renew your domain name by the expiration date may result in a loss of your online identity making it difficult for your customers and friends to locate you on the Web.

Privatization of Domain Registrations and Renewals now allows the consumer the choice of Registrars when initially registering and also when renewing a domain name. Domain name holders are not obligated to renew their domain name with their current Registrar or with Internet Domain Name Services. Review our prices and decide for yourself. You are under no obligation to pay the amounts stated below, unless you accept this offer. **This notice is not a bill**, it is rather an easy means of payment should you decide to switch your domain name registration to Internet Domain Name Services.

Term	Period covered	Price
1 year	Until -- Dec 4, 2019	\$45.00
2 years (Recommended)	Until -- Dec 4, 2020	\$80.00 (save \$10)
5 years (Best Value)	Until -- Dec 4, 2023	\$180.00 (save \$45)

The following names are currently available for you to register and secure, protecting your domain name from being duplicated.

Available Domains	Period covered	Price
[redacted]	2 Years	\$80.00
[redacted]	2 Years	\$80.00

For a complete list of our terms and conditions, please visit [www.idns.ac/tos](http://www.idns.ac/tos)

Transfer and renew your domain name online at [www.idns.ac](http://www.idns.ac) 24 hours a day, 7 days a week.

Please detach this stub and include it with your payment.

Check the appropriate boxes of the Domain Names you would like to order.

Expiration Date	Reply Requested By	Renewal Term	Payment	(✓)
December 4, 2018	September 24, 2018	1 Year	\$45.00	
		2 Year	\$80.00	
		5 Year	\$180.00	

Available Domain Names (Optional)

1 Year	\$45.00	<input type="checkbox"/>
2 Year	\$80.00	<input type="checkbox"/>
5 Year	\$180.00	<input type="checkbox"/>

**Total Amount**





KEVIN A. MCGRAIL T116 P1

If paying by credit card, please enter your information below:

Card Number:

Expiry:  /

Please provide a valid email address on the above line





# “Invoice” Scams

“This is an advertisement...”

*Warn your A/P. We see more than a few of these get paid!*



IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED

\*\*\*\*\*AUTO\*\*SCH 5-DIGIT 22031  
Mr. McGrail 6113



IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED

Makes: HONDA, NISSAN, TOYOTA

Attention: Mr. McGrail

Our records indicate that you have not contacted us to have the vehicle service contract for your HONDA, NISSAN, TOYOTA Updated. You are receiving this notice to ensure no lapse in warranty coverage. Warranty expiration is based on the mileage and age of your HONDA, NISSAN, TOYOTA Call now to update your coverage.

Please Call: 1-877-324-0916

Para Espanol: 1-877-282-9764

By neglecting to replace your coverage you will be at risk or being financially liable for any and all repairs after your factory warranty expires. However, you still have time left to activate your service contract on vehicle before it's too late. No vehicle inspection will be required.

Your file on this vehicle will be deleted and you may no longer be eligible for this offer regarding service coverage after 7/3/2018

Personalized Website	<a href="http://CIL9696331.autorepairnetwork.info">http://CIL9696331.autorepairnetwork.info</a>
----------------------	---

SUMMARY OF TERMS

0%	1.5%	2.75%	3.75%	4.5%	7.85%	9.25%	11.99%
APPROVED	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Coverage Explanation	
REQUESTING	Platinum Option: Engine, Transmission, Transfer Unit of 4x4, Drive Axle Assembly, Front End and Rear Suspension, Steering, Air Conditioning Unit, Electronics, Seals, Gaskets, Brake System, and Most mechanical Parts.
1. EXTENSION THROUGH 2023	You may have been selected to receive this special limited time offer from Warranty Services Vehicle Division because of information in your public record consumer auto data file. Final acceptance is subject to your ability to meet our full eligibility requirements. This is an advertisement to obtain coverage.
2. UP TO OR AN ADDITIONAL 100K MILES	
3. PLATINUM / POWERTRAIN	
PHONE: 1-877-324-0916	Call No Later Than: 7/3/2018

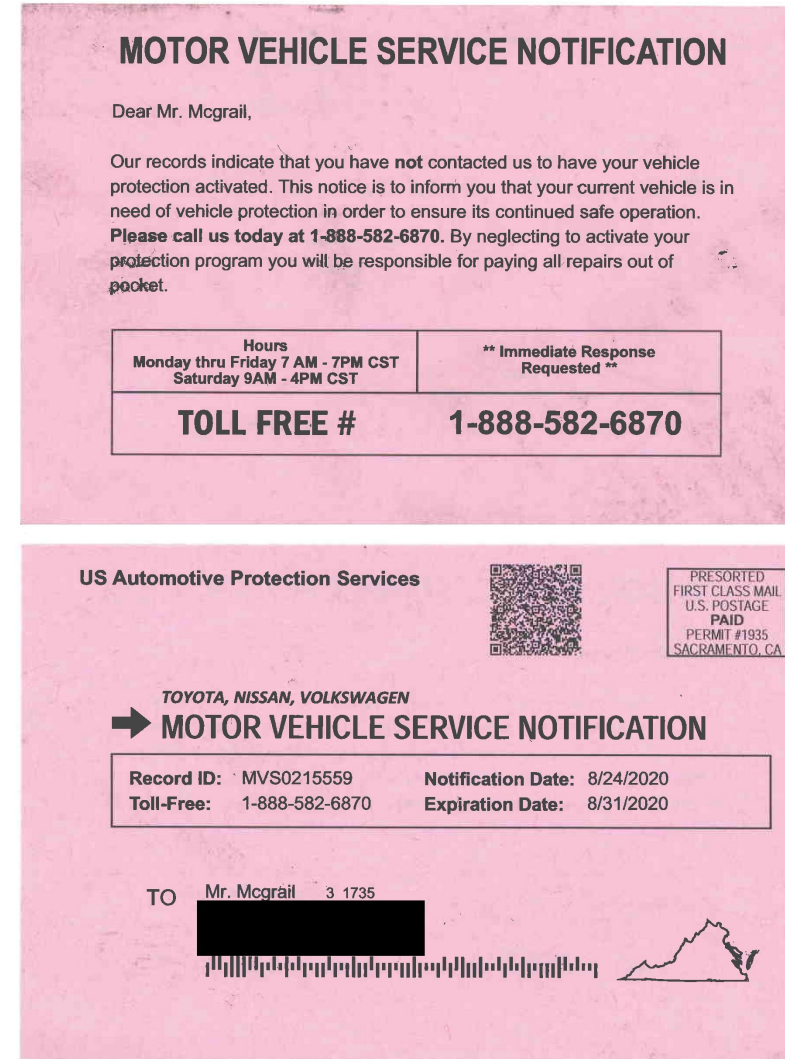
Operating Hours: Monday - Friday 8:00am to 7:00pm CST & Saturday 9:00am - 2:00pm CST





# Maintenance Scams

This one probably  
is illegal...



# Every Industry is a Target... Phish<sup>2</sup>?

Hello Friend

My name is Sir Bismark Thyle .I extend my Happy wishes to you and family in this new decade 2020.

I have been nursing the idea of investment on seafood industry( Yellow fin Tuna Loins and Center Cuts Yellow fin Tuna HGT), as there is a great demand in the field of aquaculture industry here.Today,I was made to understand that there are several routes to the commodity in the markets, some of which facilitate participation for those who are not even professional traders.I need your active advice as a specialist in this field of Agriculture.Include all the financial obligations involves that will qualify me.My private Tel +233204644268 Do treat this message as urgent

Kind Regards

Bismark Thyle





# Psychology of Scams

## Nigerian Prince Scam

Try to separate logic from emotion

Almost always impose a deadline with severe penalties



# Watch Out for Psych-O's

Psych

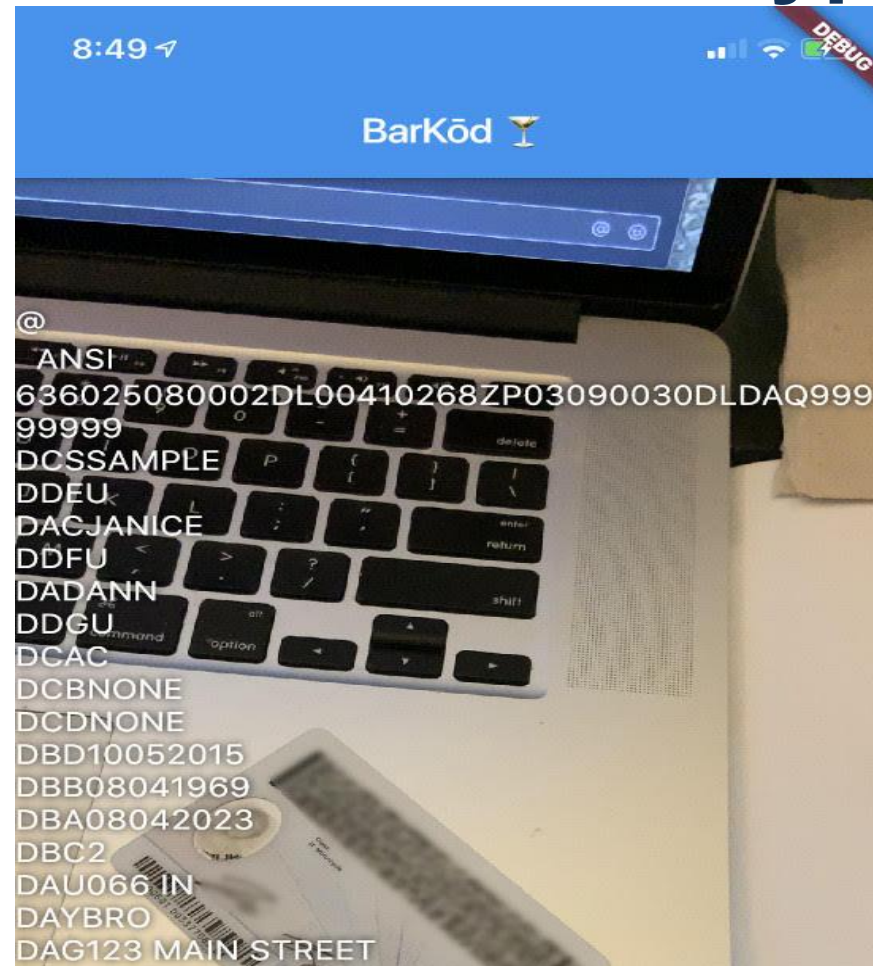
Season 1, Episode 11

He Loves Me, He Loves Me Not, He Loves Me, Oops He's Dead

# psych



# Barcodes on ID are NOT Encrypted



# Hidden Secrets

<https://nakedsecurity.sophos.com/2019/01/11/old-twitter-posts-reveal-hidden-secrets-say-researchers/>

Twitter data before 2015 included metadata! “Before this date, if a user geotagged themselves in a broad area such as a city, the social network embedded their exact GPS coordinates in the tweet’s metadata...”

Posts containing phrases like “at work”, “at home”, or complaints about a doctor leaked Personally Identifiable Information (PII)

**Able to positively identify dozens of anonymous Twitter users!**



# Quill / FedEx Phish

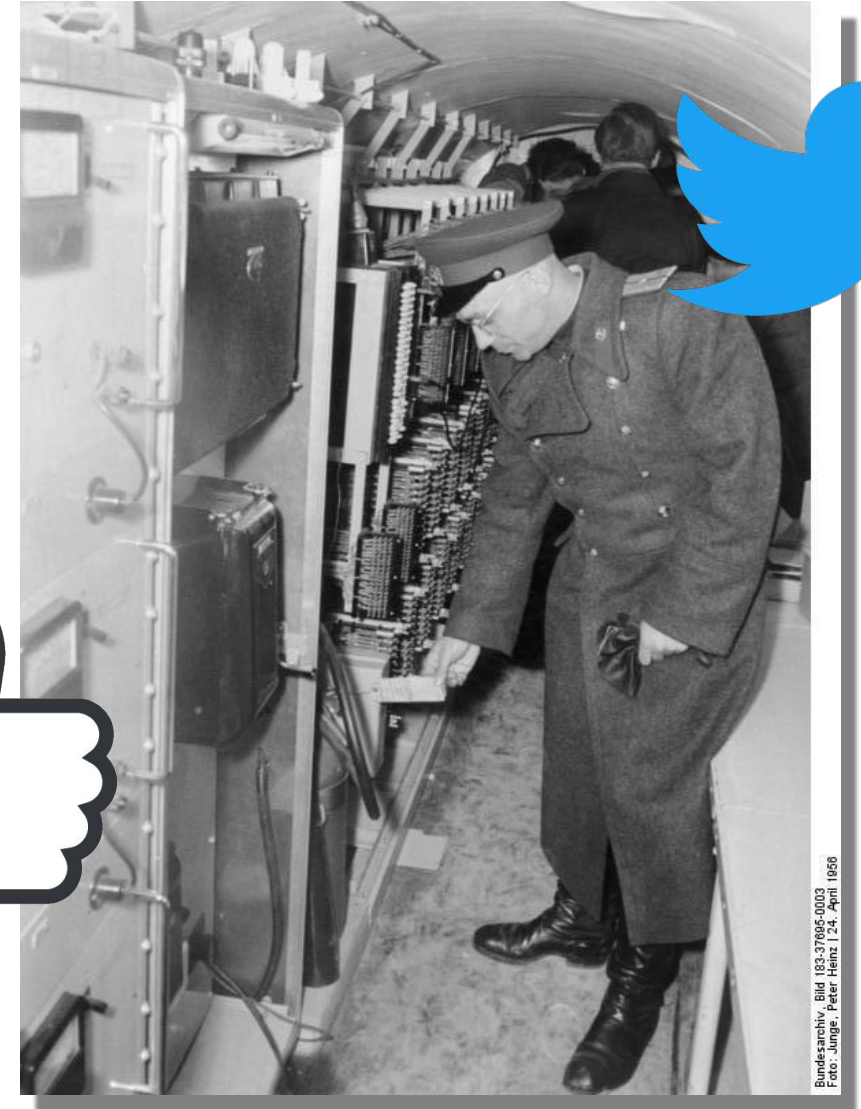
This hack could happen with MANY vendors not just Quill & FedEx but this happened to our customer, WF Wells, in January of 2020

Hack your account, send you normal items, receive a call tag for the items, call tag reroutes the items to the bad guys, NOT the vendor.



# Social Media is a Goldmine

Be sensitive about what you post. Birthdays, parents, addresses, pets, graduations, etc. it all adds up! And it's all archived somewhere...



Bundesarchiv, Bild 183-37605-0003  
Fotograf: Jung, Peter Heinz | 24. April 1950





# Tips to Minimize Exposure



# Beware of Hardware Hacks

<https://www.fastcompany.com/90413945/theres-a-scary-new-reason-not-to-borrow-a-strangers-iphone-cable>

Fast Company | Bad news: A hacker has created a rogue Lightning cable that lets bad guys take over your computer. Worse news: Now it's being mass-produced.

Don't use Unknown Mice/Keyboards

Don't Use Charging Kiosks

Don't Use Public WiFi



# Handling Passwords

## Get rid of password complexity and instead use length

National Institute of Standards and Technology (NIST) Digital Identity Guidelines, [SP 800-63B Section 5.1.1.2](#) paragraph 9, “recommends against the use of composition rules (e.g., requiring lower-case, upper-case, digits, and/or special characters) for memorized secrets. These rules provide less benefit than might be expected...”

## Support LONG passwords

## Passphrases not passwords - xkcd Password Generator

## Don't require periodic password changes

“Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”, SP 800-63B Section 5.1.1.2 paragraph 9

## Hashing AND Salting - haveibeenpwned.com



# Handling Logins

Use Multi-Factor Authentication (MFA)

Password Reset capabilities are a key attack. Reset emails, should be single use and short lifespan. DELETE them when done.

Notify users such as by email when a password is updated/reset.



# Use the Principles of Least Privilege

## Use Principles of Least Privilege (POLP)

These are mistakes you want to make sure are NOT made:

- Turning off Security Features (Anti-virus/SELINUX/etc.)

- Grant ALL on Databases

- Using elevated privileges for general work as laziness

- Using “Shadow IT” to go around controls

When elevated privileges are needed, use as short a window as possible!



# Don't Panic and Have an Incident Response Plan

- Limit damage / Reduce recovery time / Lower costs
- Speed matters (Don't Panic)
- Key phone numbers / account numbers / credentials / list of privileged accounts
- Asset Inventory
- Paper and Electronic Copies of the Plan





# Implement a Moral Compass with Your IT Staff

USENIX / Systems Administrators' Code of Ethics

<https://www.usenix.org/system-administrators-code-ethics>



Q/EH® Qualified/ Ethical Hacker

CEH Certified Ethical Hacker



# Dev to QA to Prod

Have a process for testing new systems from dev to QA to production

Automate what you can!

“If I gave you a fix, how long to implement?”



# Q: Why Do Hackers Love OOM?

☐ Vacation responder off  
☒ Vacation responder on

First day:  ☐ Last day:

Subject:

Message:

Sans Serif | T | B | I | U | A | | | | | | | |

« Plain Text

I am traveling for from August 7th through August 28th. I will be in Costa Rica with Limited Internet Capabilities. In my absence, please contact Bob@MyFirm.com for help!

☐ Only send a response to people in my Contacts



# A: People Overshare

☐ Vacation responder off

☒ Vacation responder on

First day:

☐ Last day:

Subject:

Message:

Sans Serif



« Plain Text

Hi, I am out of the country, please come rob my house! Oh and now is a great time to try and attack my accounts and things since I might not see the notices. And Bob might be a great guy to send an email impersonating me.

☐ Only send a response to people in my Contacts

☐ Only send a response to people in PCCC Document Share



# There is a Quick Fix

The screenshot shows the Outlook Web App interface for setting up automatic replies. The left sidebar contains navigation links: options, account, organize email (selected), groups, site mailboxes, settings, phone, block or allow, and apps. The main content area is titled 'automatic replies' and includes tabs for 'inbox rules', 'automatic replies', and 'delivery reports'. Under the 'automatic replies' tab, there are sections for 'Send automatic replies' (with a checkbox for 'Send replies only during this time period' and time pickers for 'Start time' and 'End time'), 'Send a reply once to each sender inside my organization' (with a font size selector set to 12), and 'Send automatic reply messages to senders outside my organization' (with radio buttons for 'Send replies only to senders in my Contacts list' and 'Send replies to all external senders'). A callout box highlights the 'Send automatic reply messages to senders outside my organization' section, showing the checked 'Send automatic reply messages to senders outside my organization' checkbox and the three radio button options. Below the callout box, the text 'Send a reply once to each sender outside my organization with the following message:' is visible. A 'save' button is located at the bottom left of the settings area.

automatic replies - Outlook Web

https://webmail.parkersburgwv.gov/ecp/?rfr=owa&owaparam=modurl%3D0&p=account

Outlook Web App

Kevin McGrail

options

account

organize email

groups

site mailboxes

settings

phone

block or allow

apps

inbox rules automatic replies delivery reports

Send automatic replies

Send replies only during this time period:

Start time: Sun 7/14/2019 11:00 AM

End time: Mon 7/15/2019 11:00 AM

Send a reply once to each sender inside my organization

Calibri 12 B I U

Send automatic reply messages to senders outside my organization

Send replies only to senders in my Contacts list

Send replies to all external senders

Send a reply once to each sender outside my organization with the following message:

save



# Think Evil

Start with Why:

Threat Modelling is important.

**MITRE** ATT&CK to understand your adversaries and their TTP  
(Tactics, Techniques & Procedures)

Palo Alto Networks Unit 42 Playbooks

Payment Card Industry Data Security Specification (PCI-DSS) - SAQ

Read more Spy Novels





# Solutions to Consider

InfraShield cyberphysical security - <https://www.InfraShield.com/>

Policy, Implementation, Training, Assessments, Attestation, Remediation, and Recovery

Recorded Future

<https://www.recordedfuture.com/open-source-intelligence-definition/> -

Security policies based on Who and What is Attacking you.

Stop the #1 Vector: Email

INKY Phishing Prevention - <https://inky.com/>

Raptor Email Security - <https://www.pccc.com/>



# Thanks!

## Slides will be on my LinkedIn & [mcgrail.com/downloads](https://mcgrail.com/downloads)

Thanks to CASC, the Soter Group and Recorded Future for their input & ideas. Thanks to WF Wells, Victor M. Glassberg & ASMFC for their permission to use their real-world phishing examples.

### Image Credits:

Barkod Image courtesy of John Lifsey, used with permission

KAM photo taken by Ted King, used with permission

Company logos used to represent the firms and do not imply any approval

Operation Gold Bundesarchiv, Bild 183-37695-0003 / Junge, Peter Heinz / CC-BY-SA 3.0

Chest Xray from the CDC Public Domain

Psych Logo from Wikipedia

Keep Calm Poster & Exit Sign from Public Domain

Angela Merkel Photo from Bundesregierung/Kugler



Kevin A. McGrail  
[www.linkedin.com/in/kmcgrail](https://www.linkedin.com/in/kmcgrail)

