

Kevin A. McGrail
kmcgrail@InfraShield.com

Internet Safety: Liars and Phishers and Bad Actors, Oh My!



QUANTICO

Presented by:



About the Speaker

Kevin A. McGrail
Director, Business Growth



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



Security Expertise

USMC Cyber Aux Member

Apache SpamAssassin

KAM.cf

Helped with the first IDS

MIMEDefang

Phone Lines Cut

Apology from the FBI



What Makes InfraShield Special?

Used to securing high-value, high-target critical infrastructure

\$40M cyber range for proving our strategies

OT & IT Cyber Expertise





ASHIELD

Today's Goals

What is Phishing?

How to Recognize Signs of Phishing

Laugh (Preferably with Me, Rather than at Me)

Real World Advice

What is Phishing?

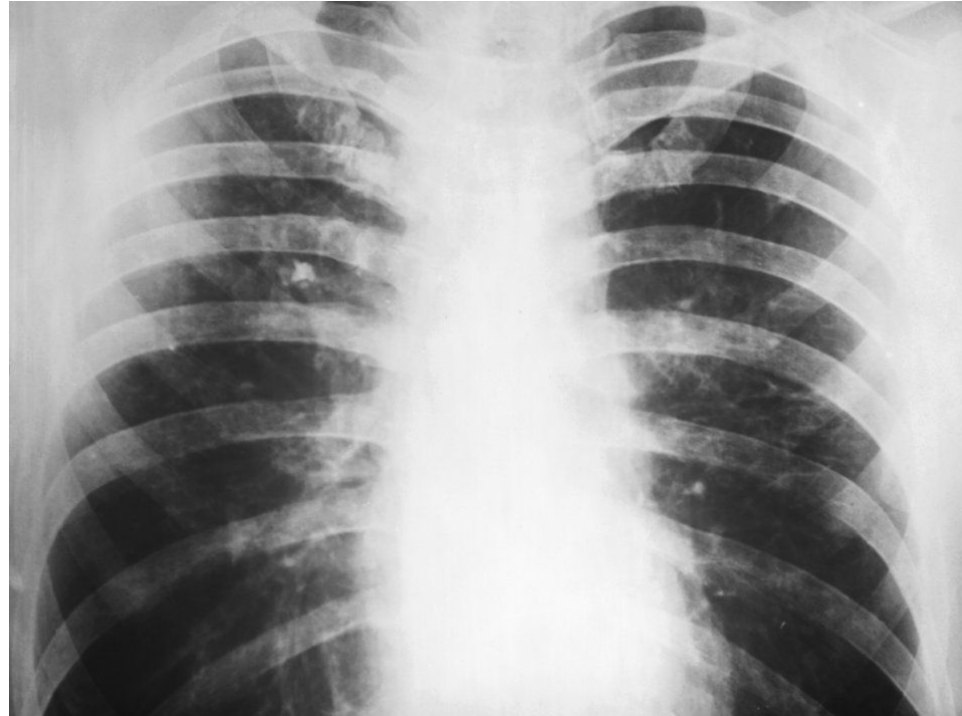
Why me?



I'm **Not** a Target!



Everyone & Anything is a Target!



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

Phishing isn't just about Email



QUANTICO

Personal Interactions

Unexpected Value

Steganography

Unintended Leakage

Social Media

Job Inquiries

Invoice Scams



Watch Out for Psych-O's

Psych

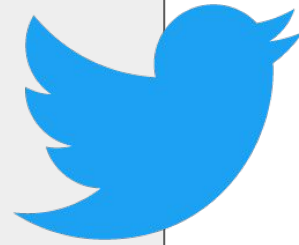
Season 1, Episode 11

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

psych

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 103 37605 0003
Foto: Jungo - Peter Heinz | 24. April 1956

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!

Florida Man Challenge

Have you heard of the Florida Man Challenge?

Did anyone here do it?

What are the risks involved?

Q: Why Do Hackers Love OOM?

Vacation responder off
 Vacation responder on

First day: Last day:

Subject:

Message:

Sans Serif | ↑↓ | **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 - | ↑T - | **B** *I* U A - | ↻ 📷 | ☰ - | ☰ ☰ ☰ ☰ ☰ ☰ ☰ ☰ | ☰ ☰ | *I*x

« 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 configuring automatic replies. The browser address bar shows the URL: <https://webmail.parkersburgwv.gov/ecp/?rfr=owa&owaparam=modurl%3D0&p=account>. The page title is "automatic replies - Outlook Web". The user is identified as "Kevin McGrail".

The "automatic replies" settings are visible, including:

- 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:
 - Font: Calibri, Size: 12
- 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:
 - Font: Calibri, Size: 12





A blue "save" button is located at the bottom left of the settings area.

A callout box highlights the "Send replies to all external senders" option, which is currently unselected. The text "Send a reply once to each sender outside my organization with the following message:" is visible below the callout box.

Spear Phishing on Business Social Media



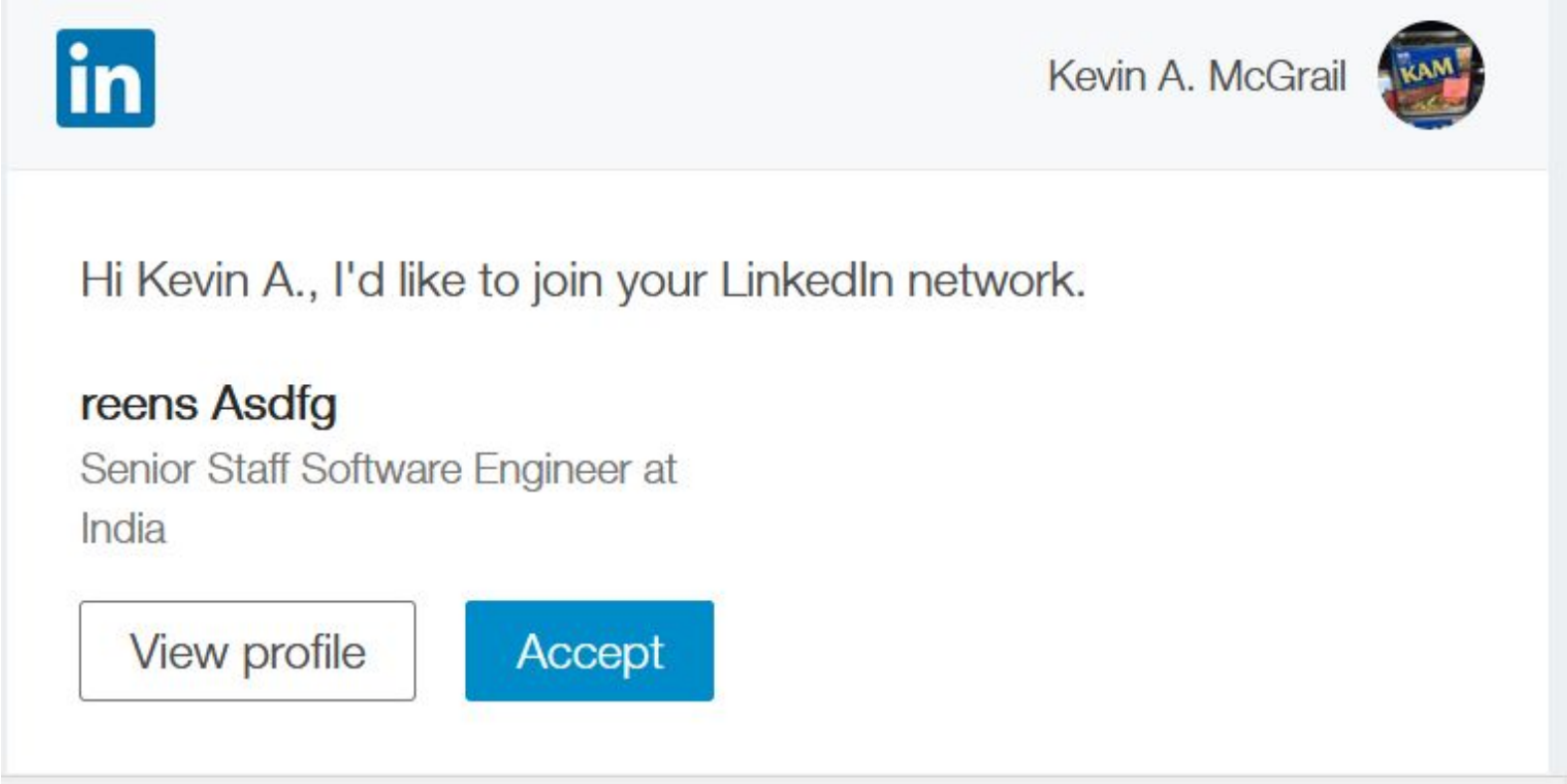
Invitations (4) Manage all

	Rohit Mishra Computer Operator at SAIC SAIC	Ignore	Accept
	Dora Shelly Sales Manager at SAIC SAIC	Ignore	Accept
	Subrata Pandit Software Engineer at SAIC SAIC	Ignore	Accept
	giakhanh accxi Sales Manager at SAIC SAIC	Ignore	Accept

[See all 4 invitations](#)


Some are Quite Silly....

Do I know your father,
Qwerty Asdfg?







The screenshot shows a LinkedIn interface. At the top left is the LinkedIn logo. At the top right, the name 'Kevin A. McGrail' is displayed next to a circular profile picture containing the letters 'KAM'. The main content area shows a connection request from 'reens Asdfg', who is identified as a 'Senior Staff Software Engineer at India'. Below the name are two buttons: 'View profile' and 'Accept'.

<3 the <3's



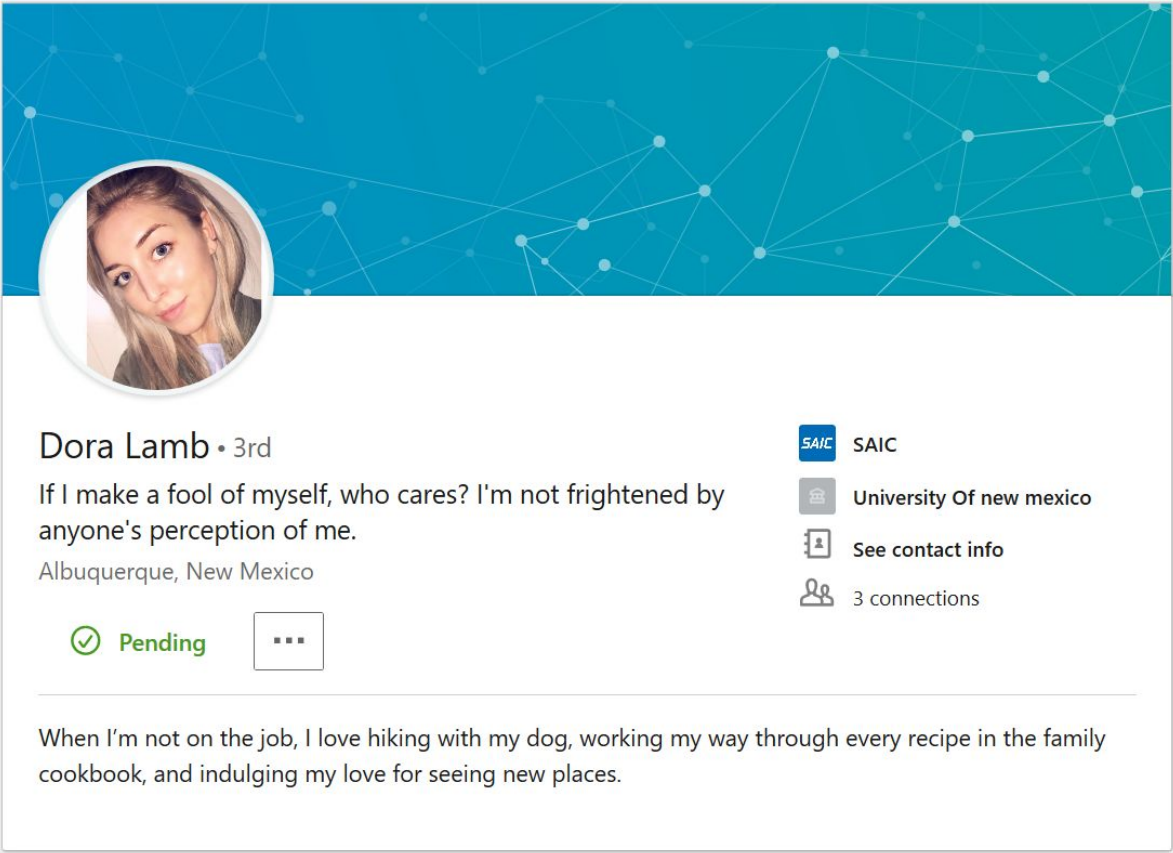
Mandy Bullen • 1st
Front-End Developer at SAIC
Albuquerque, New Mexico Area

[Message](#) [More...](#)

-  SAIC
-  Univerasity OF new mexico
-  See contact info
-  See connections (21)

Everyone has a purpose in life and a unique talent to give to others. And when we blend this unique talent with service to others, we experience the ecstasy and exultation of own spirit, which is the ultimate goal of all goals.



Sometimes we see patterns...





Dora Lamb • 3rd


If I make a fool of myself, who cares? I'm not frightened by anyone's perception of me.


Albuquerque, New Mexico

 Pending 

 SAIC

 University Of new mexico

 See contact info

 3 connections

When I'm not on the job, I love hiking with my dog, working my way through every recipe in the family cookbook, and indulging my love for seeing new places.

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/>

LI to PDF to URL Shortener

They use these
techniques to:

A) Make the message
look more legitimate

B) Evade scanners

Steve Chiama Business Coach Northern Virginia • 6:59 AM
Good morning,

Attached is a business project we are working on. Kindly review so we can discuss further as I'll be needing more capable hands.

Thanks,

Steve.

PDF PJT2019_CBO.pdf
168 KB Download

OneDrive

This document has been shared with you. <https://bit.ly/2JaqcEQ> sender view document below.

VIEW ATTACHMENT HERE

This document was sent to you by using the One Drive Electronic file share service. To see document click on "View PDF"

Do Not Share This Email
This email contains important documents. Please do not share this email, link, or access code with others.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

“Invoice” Scams

“This notice is not a bill...”

Pay no attention to the man behind the curtain...

Not all scams are illegal!

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

Transfer and renew your domain name online at 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	<input type="checkbox"/>
		2 Year	\$80.00	<input type="checkbox"/>
		5 Year	\$180.00	<input type="checkbox"/>

Available Domain Names (Optional)

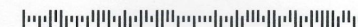
- 1 Year \$45.00
- 2 Year \$80.00
- 5 Year \$180.00

Total Amount

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

Card Number:

Expiry: ____/____/____



KEVIN A. MCGRAIL

T116 P1

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!



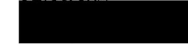
Warranty Services
Extended Coverage Department



Owner ID # : CIL9696331
Contact Phone: 1-877-324-0916
Vehicle Make: HONDA, NISSAN, TOYOTA
Program Term Deadline: 7/3/2018

IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED

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



Call to verify the above information
Read below for more information



IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED

Owner ID # : CIL9696331
Coverage Status: AVAILABLE
Program Term Deadline: 7/3/2018

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	http://CIL9696331.autorepairnetwork.info
----------------------	---

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	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.
REQUESTING	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.
1. EXTENSION THROUGH 2023	
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

Not a Risk in 2020... But...

Conference Hotel Pirates

Now Email Phishing



#1 Vector

Examples



91%

The percentage of compromises that occur because of a spear phishing email.

Source: Cofense (previously Phishme) 2016 Study on Enterprise Phishing



Credential Phishing

Dear LinkedIn User

As part of our effort to improve your experience in LinkedIn access across our consumer services, we're updating LinkedIn Services Agreement and Privacy.

Click the link below to update your account.

<http://workwp.ir/a/a/sign.htm>

Your account will be De-Activated if you do not update.

This notice Ends WED September 26, 2018

We apologize for any inconvenience.

Thank you for your cooperation.

Sincerely,

LinkedIn Service Provider

Copyright ? 2018 Information

Company. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.



Watch Out for Impersonators!



Phil Steitz via [apache.org](#)

to Kevin ▾

Okay. I need you to set up a same-day payment to the account details below

Amount \$19,840

Bank Name: Wells Fargo

Name on Account: HE

Account Number:3303

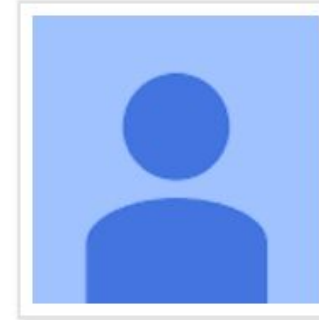
Routine Number:0260

Address:[475 6th Ave, New York, NY 10011](#)

E-mail me the payment confirmation after you have it done

Phil Steitz

executive.office2@zoho.com



Contact info Emails



The Wrong Approach

While accurate, it's too simplistic and shows only basic examples:

<https://securityboulevard.com/2019/05/your-account-has-been-locked-7-telltale-signs-of-a-phishing-scam/>

https no longer safe; Malicious URL attacks using HTTPS surge across the enterprise

<https://www.zdnet.com/article/social-engineering-attacks-surge-across-the-enterprise/>

https is not an indicator of bad or good actors. Tools like letsencrypt make it too simple to implement and good guys mess up

The Wrong Approach - Part 2

Obfuscation techniques using shorteners or google/box/microsoft files appear OK

Hovering is BAD

Escalate Escalate Escalate

Use a box with a browser on a simple ChromeOS or Linux box to do checking of potential bad forwards using WebMail. Don't have it? Consider VirtualBox and an installation of Ubuntu or CentOS.

Think Evil



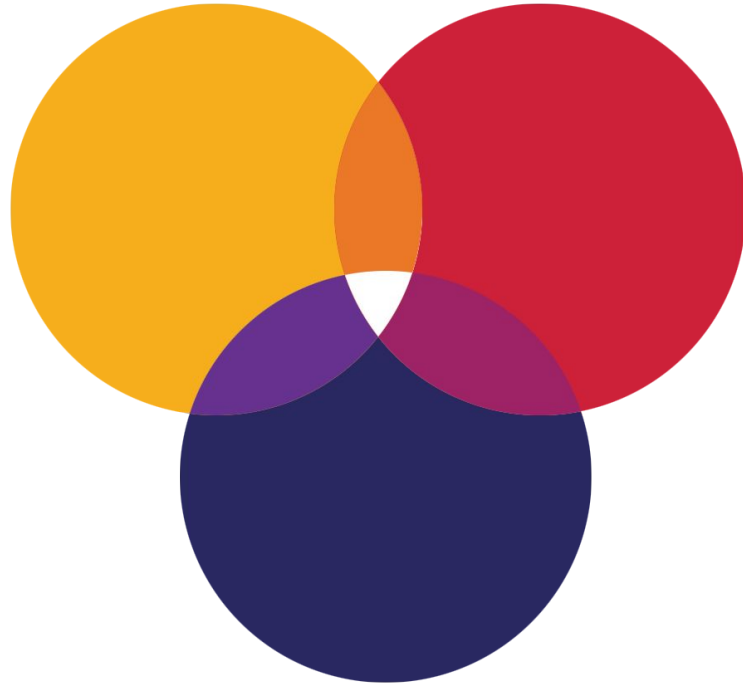
GANs

Anime Art

Security Data Sharing



Bad Actors are More Evil than KAM



Please Don't...

Password Change Sign Up sheet

If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.

Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scouter49\$	Steele4U2
Iz Jones	PHONE	89621	4281
Jack H	email	Password	Password 2
Big Ed	facebook	redst@p	mnmkr
Sam Adams	Pike Pass		beerlover1981

Come See Me
- Shawn



Generative Adversarial Networks (GAN)

<https://thispersondoesnotexist.com/image>



Think Evil

https://nips2017creativity.github.io/doc/High_Quality_Anime.pdf

<https://news.ycombinator.com/item?id=19144280>



Figure 1: Generated samples with random prior.



Figure 2: Generated images with fixed noise part and random attributes.



Figure 3: Generated images with fixed conditions (silver hair, long hair, blush, smile, open mouth, blue eyes) and random noise part.



Figure 4: Interpolation between images.

Data Sharing & Unintended Consequences

Another Worrying Trend:

Q: What's a consistently overused security question?

A: Your Mother's Maiden Name.

Q: How many married women can you find on social media because they add their maiden name?

A: Sigh...

Limit Social Media sharing & restrict Out of Office Messages

Tools to Combat Phishers



Passphrases

Entropy

Multi-Factor Authentication

Credit Watch

Silly Security Tips

My Advice

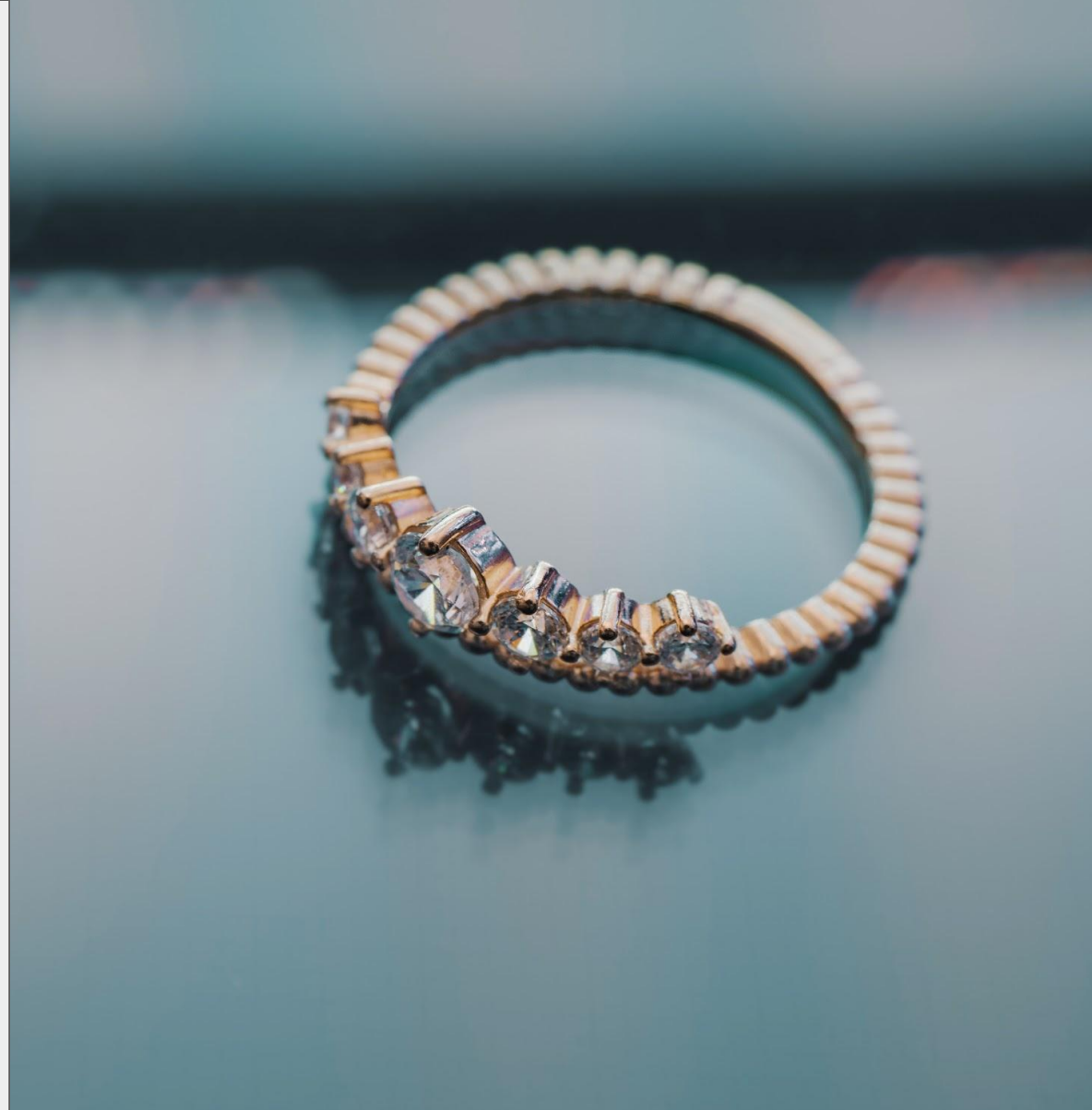


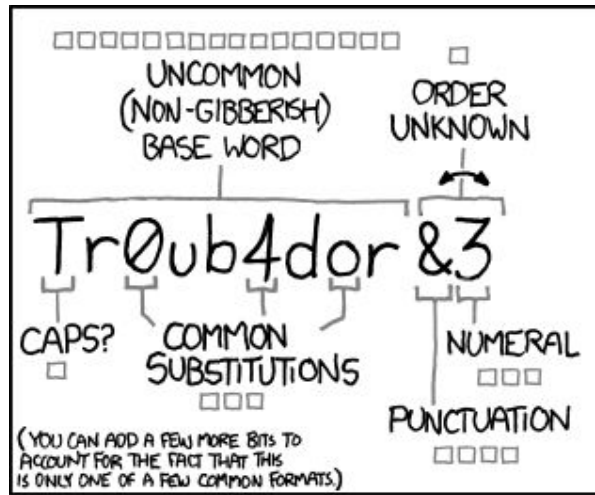
Passphrases not passwords

Passwords you have to write down
are less secure!

NIST 800-63 Password Guidelines
is now revised: minimum 8 to a
MINIMUM MAXIMUM of 64, no
sequences but no special char
requirements.

MickeyMinniePlutoHueyDeweyLoui
eDonaldGoofyRichmond





~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

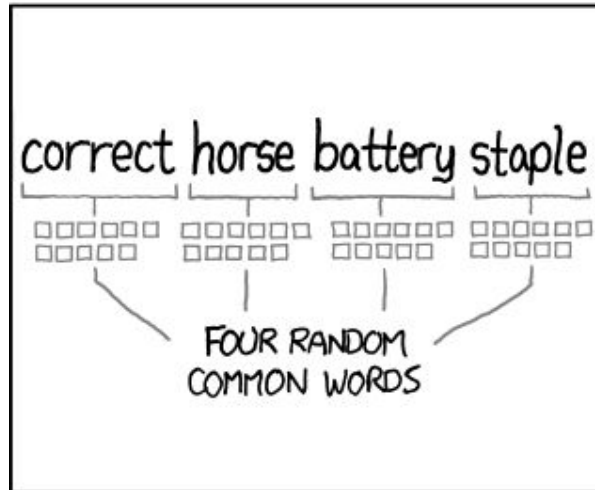
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

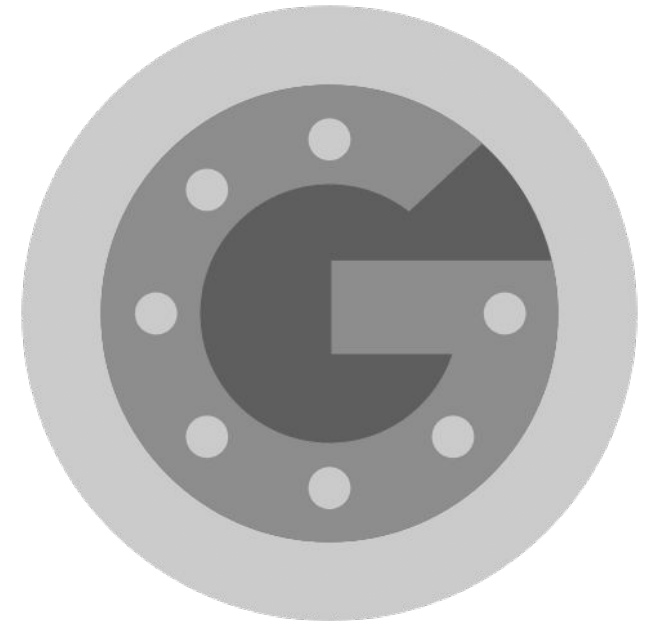
CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

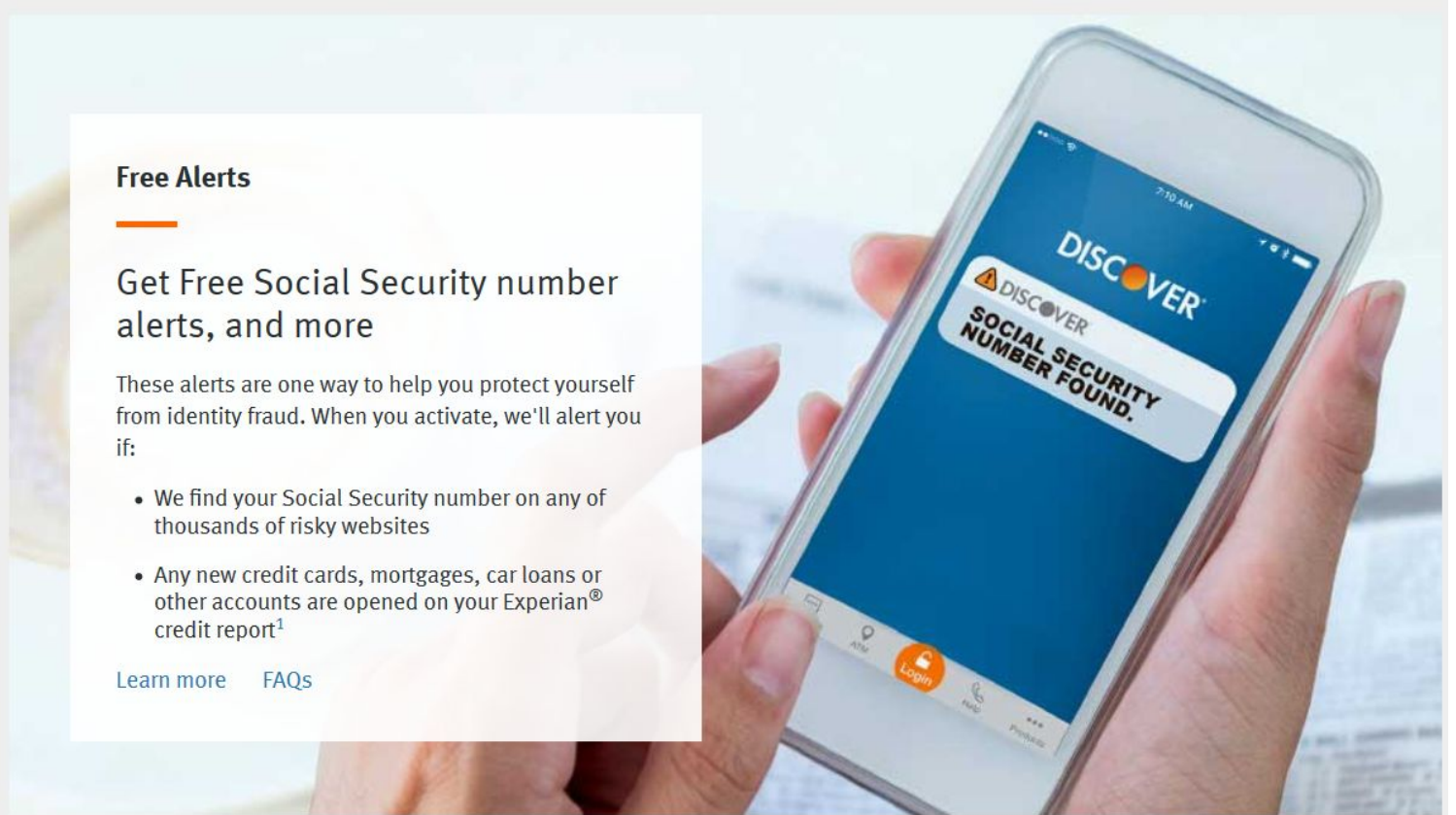
Password Length is Better Than Password Complexity!!

Use Multi-Factor Authentication



Monitor Your Credit

<https://refer.discover.com/s/pwdup>



Top 5 XKCD Security Tips

1. Change your password manager monthly
2. Install a secure font
3. Use a 2-factor smoke detector
4. Change your maiden name regularly
5. Put strange USB drives in a bag of rice overnight

SECURITY TIPS

(PRINT OUT THIS LIST AND KEEP IT
IN YOUR BANK SAFE DEPOSIT BOX.)

- DON'T CLICK LINKS TO WEBSITES
- USE PRIME NUMBERS IN YOUR PASSWORD
- CHANGE YOUR PASSWORD MANAGER MONTHLY
- HOLD YOUR BREATH WHILE CROSSING THE BORDER
- INSTALL A SECURE FONT
- USE A 2-FACTOR SMOKE DETECTOR
- CHANGE YOUR MAIDEN NAME REGULARLY
- PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
- USE SPECIAL CHARACTERS LIKE & AND %
- ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
- USE A BURNER'S PHONE
- GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
- IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.

Be a Strong Link

You **CANNOT** identify all scams. **Use Your Help Desk!**

Anytime you have a concern, **Take 10 Seconds** to Separate Emotion from Logic.

Preparing for the Worst



QUANTICO



Have I Been Pwned?

haveibeenpwned.com

';--have i been pwned?

Keep Calm and Have an Incident Response Plan

Limit damage / Reduce recovery time /
Lower costs

Speed matters

Key phone numbers / account numbers /
credentials / list of privileged accounts

Asset Inventory

Paper and Electronic Copies of the Plan



Discussing Scams

Use ***munge*** or similar to deactivate links when discussing dangerous things

Phish example for for Steve Chiama:

Seeing a new process on LI but using images, or pdfs or links to OneDrive/Google Drive that are fake.

Message on linkedin which has a PDF leading to a One Drive link that is actually to bit.ly/*munge*2JaqcEQ that lands on https://destingulfgate*munge*.icu

Psychology



Psychology of Scams

Nigerian Prince Scam

Try to separate logic from emotion

Almost always impose a deadline with severe penalties

Opportunistic vs. Persistent Adversaries

Hive versus Targeted

Scale of Economies

Doesn't stay \$20

Paranoid KAMland: Engadget: How a trivial cell phone hack is ruining lives.

<https://www.engadget.com/2019/06/28/cell-phone-hack-is-ruining-lives-identity-theft/>

Being a Better Administrator



Users Can Be a Strong Link

Users CANNOT identify all scams. Encourage Help Desk Use!

Look for “Tip of the Iceberg” issues & pay attention to users who file good trouble tickets.

Encourage users to get those 10 seconds they need to separate the Emotion from the Logic.



How to Be the Best Administrator

LISA/SAGE IT Ten Commandments:

https://www.pccc.com/base.cgim?template=sage_code_of_ethics

Users can do no wrong

<https://www.itweb.co.za/content/JBwErvn5wIYq6Db2>

Our job is to protect users from the bad guys (and themselves)

“The goal of cyber is to minimize mean time to detect and mean time to resolve”,
CSO of Raytheon

Administrative Training Resources

[Imgtfy.com](http://imgtfy.com)

[XKCD.com](http://xkcd.com)

BOFH (<http://bofh.bjash.com/bofh/bofh1.html>)

The IT Crowd (<https://www.netflix.com/title/70140450>)

Shadow IT is Real

Embrace new ideas ...before users do so outside your control...



Offboarding

Make sure exiting employees have their accounts disabled!

EXIT

 BetterCloud

Don't Require 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



NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce

Spam is about Consent
NOT about Content

Money Handlers are the Biggest Targets

A few types of fraud to discuss

CxO Fraud

Cloning

Domain Spoofing

Rogue Access point like ATTWIRELESS

Malicious Text Messages (SMISHING?)

Phishing

Spear Phishing

Whale Phishing

QR Code Phishing

(<https://www.bleepingcomputer.com/news/security/phishing-security-controls-fully-bypassed-using-qr-codes/>)

Security Alerts

(<https://www.scmagazine.com/home/security-news/phishing/phishing-campaign-impersonates-email-alerts-from-dhs/>)

Pow-Wow Exercise

State Department Wi-Fi Example

Think about X-Rays example and be broad in this exercise:

How/What/Who/When/Why do you think you will be attacked?

If you were evil, how would you attack/steal/cripple your infrastructure?

Surveillance 2.0 and FSB Disclosure

<https://www.nytimes.com/2019/07/03/technology/personaltech/fingerprinting-track-devices-what-to-do.html>

<https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/#45ddda316b11>

NOTE: Government Blockchain Association event 1Q Next Year at US Capitol.
Will be speaking on de-anonymizing cryptocurrency

Closing



Q&A

Escalate

Thanks

Credits



Q&A

Suggested Questions:

I talk fast. Anything you'd like to go back or go over?

How did I get so good looking?

What is my Skincare regimen?

Is that me in a Megapode chicken suit?



Thanks!



Kevin A. McGrail
www.linkedin.com/in/kmcgrail



Credits

Image Credits:

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

Chest Xray from the CDC Public Domain

KAM photo taken by Ted King, used with permission.

Facebook, LinkedIn & Twitter Logos Brand Resources of their Respective Companies

Psych Logo from Wikipedia

Pineapple Logo free from UIHere

Anime Photo Used with Permission

XKCD comics CC BY-NC 2.5 from <https://xkcd.com/936/> & <https://xkcd.com/1820/>

Rings Photo by FOX from Pexels

Keep Calm Poster & Exit Sign from Public Domain

Shadow IT picture courteous of Noble Ackerson, used with permission.

Special thanks to Paul Rockwell & ThisPersonDoesNotExist.com