INFRASHIELD

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

Open Source Software & Internet Security

Kevin A. McGrail
kmcgrail@infrashield.com

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

Introduction

Who am I?

Agenda:

1 - What is the Apache Software Foundation
2 - Apache Strategies
3 - The Apache Way
4 - Internet Security

MAPLE LEAF
READY TO EAT · PRÊT À MANGER
KAM
LUNCHEON MEAT / PAIN DE VIANDE
455
TENEUR ÉLEVÉE EN PROTÉINES
340 g

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

INFRASHIELD

Part 1: What is the ASF?

Who?

The Apache Software Foundation is a 501(c)(3) Charity often referred to as just Apache or the ASF.

501(c)(3) Charity not a 501(c)(6) Trade Organization

We’re known for the HTTP server and the Apache Software License.

ASF Mission

To provide software for the public good.

*We do this by providing
services and support for many
diverse software project
communities of individuals AT NO CHARGE.*

The Apache License

The ASLv2 is known for its permissive, business-friendly stance with patent grants and without copyleft provisions.

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

POWERED BY APACHE™

Powered by Apache

80% of the world's websites use our software

Every Smartphone in the world uses our software

Every plane in US airspace is tracked w/our software

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

Projects.Apache.org & Apache.org/logos

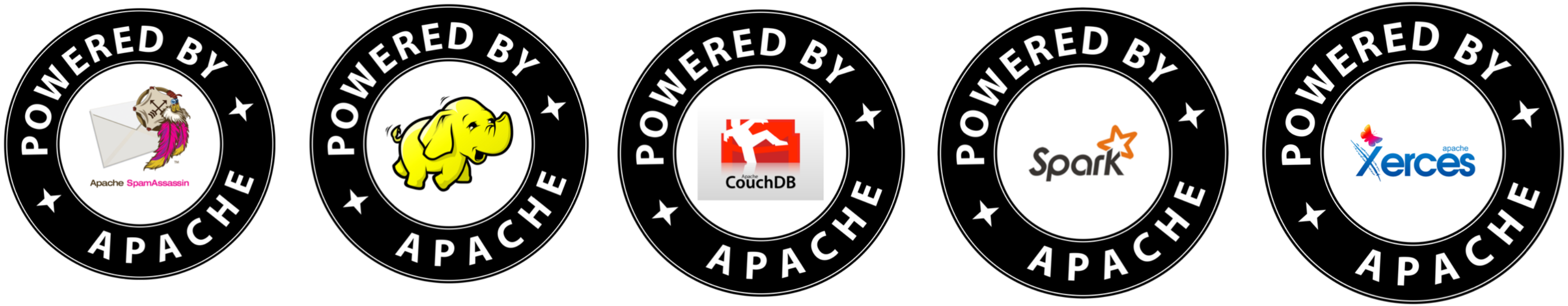
There are currently 350+ open source initiatives at the ASF:

- 199 committees managing 322 project
- 5 special committees*
- 51 incubating podlings

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

From A to Z

Apache ActiveMQ, Cloudstack, CouchDB, Fineract, Hadoop, HTTP, Kafka, Lucene, modperl, Solr, SpamAssassin, Spark, Tomcat, Xerces + a lot more!



I Cheated with Xerces

Xerces = "Zerk-cees"

“It was chosen by looking up interesting words in the dictionary, and then running them through a name check...”

POWERED BY ★ APACHE ★

apache Xerces

THE APACHE® SOFTWARE FOUNDATION
http://www.apache.org/

POWERED BY APACHE

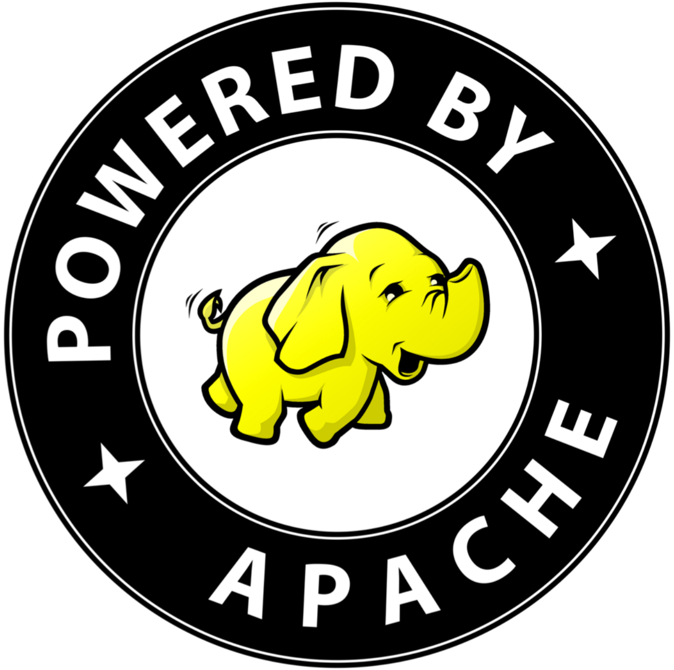
Apache Zookeeper

Not really cheating!

“ZooKeeper is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services.”

Apache Hadoop

Quiz: What’s in a name?



Big Data

“Big data is data sets that are so voluminous and complex that traditional data-processing application software are inadequate to deal with them. “ Wikipedia

Apache has 48 projects under Big Data!

Quiz: Why did they really call it Big Data?

Apache Bigtop

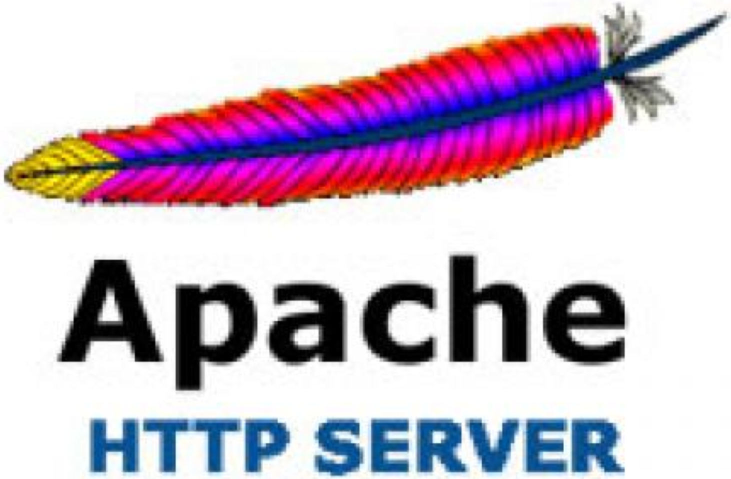
Bigtop is a project for the development of packaging and tests of the Apache Hadoop ecosystem.

POWERED BY APACHE
BIGTOP

When?

Incorporated

March 26, 1999



Part 2: Apache Strategies

What are We?

Not a democracy - elitists w/no innate right to vote

Not capitalists - you cannot buy a seat on our board.

Not a monarchy - Kings and Pawns side by side

Meritocracy

What we are is a Meritocracy. To be able to have a say, you have to prove your worth in a system of merit **as judged by the community.**

Meritocracy is a key part of The Apache Way.

Inclusion

Merit has no basis on Age, Sex, Religion, Ethnicity, Race, Country of Origin, Sexual Preference, Social Status, Income Level, Lineage, and/or Physical / Cultural Traits*.

* NOTE: We do take into serious account whether you are a Cat or Dog person.

Why?

The Foundation supports the projects and the projects support the foundation...

#1 - Resources

#2 - Legal Protection

#3 - Recognition

#4 - Community

Part 3: The Apache Way

The Apache Way

People typically hate the Apache Way for a few years

No One Way is THE Apache Way - YATAWP

The Apache Way - Charity

The ASF is a decentralized organization that supports communities to produce software at no charge for the public good.

The Apache Way - Community

We value Communities over Code

Support minority voices by trying to build support rather than rule.

The Apache Way - Consensus

+1, 0, -1

Lazy Consensus

72-hour window

Consensus ≠ Unanimity

https://www.apache.org/foundation/voting.html

The Apache Way - Meritocracy

Power is earned through merit

The most merit is earned by people with ideas who also put those ideas into action

JFDI

The Apache Way - Meritocracy

Everyone at Apache is an individual

With a meritocracy, the biggest risk is turning into a dictatorship but we like to think of ourselves as BDFL*

*We won't send fully armed battalion to remind you of our love.

The Apache Way - Transparency

If it didn't happen on list...

Discussed, decided and ARCHIVED

Reversible baby steps

Speaking of Mailing Lists (DNFTEC)

DO NOT FEED

THE ENERGY CREATURE

Source: Tim Freeman, 28 May 1996

http://www.cryonet.org/cgi-bin/dsp.cgi?msg=6284

The Apache Way - Pragmatic

Visible & Reusable Code

Risk Mitigation

Control your Destiny - Never EOL

The Apache Way - Pragmatic

No Copyleft Principle

ASLv2 is Pro-Business

“Start with the Apache License and if I ever feel bad about that, switch to GPLv3. The other way around would not be possible after thousands of idealist programmers committed their improvements.”

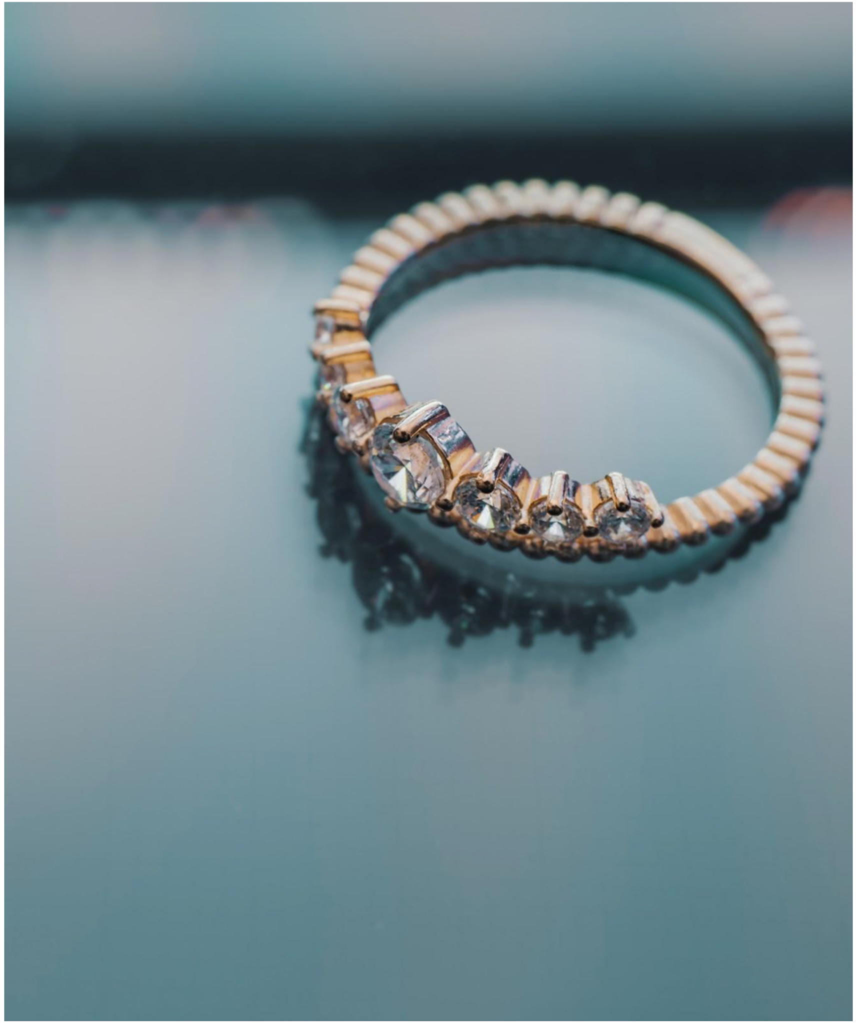
Dreas van Donselaar of SpamExperts

The Apache Way - Pragmatic

"If we ever have to go through an M&A process, the GPL license will turn up on a disclosure report. When it does, the potential acquirer will cite it as a significant risk. If we have to go back to the project owner and request documentation of permission at that time, they'll have us over a barrel."

INFRASHIELD

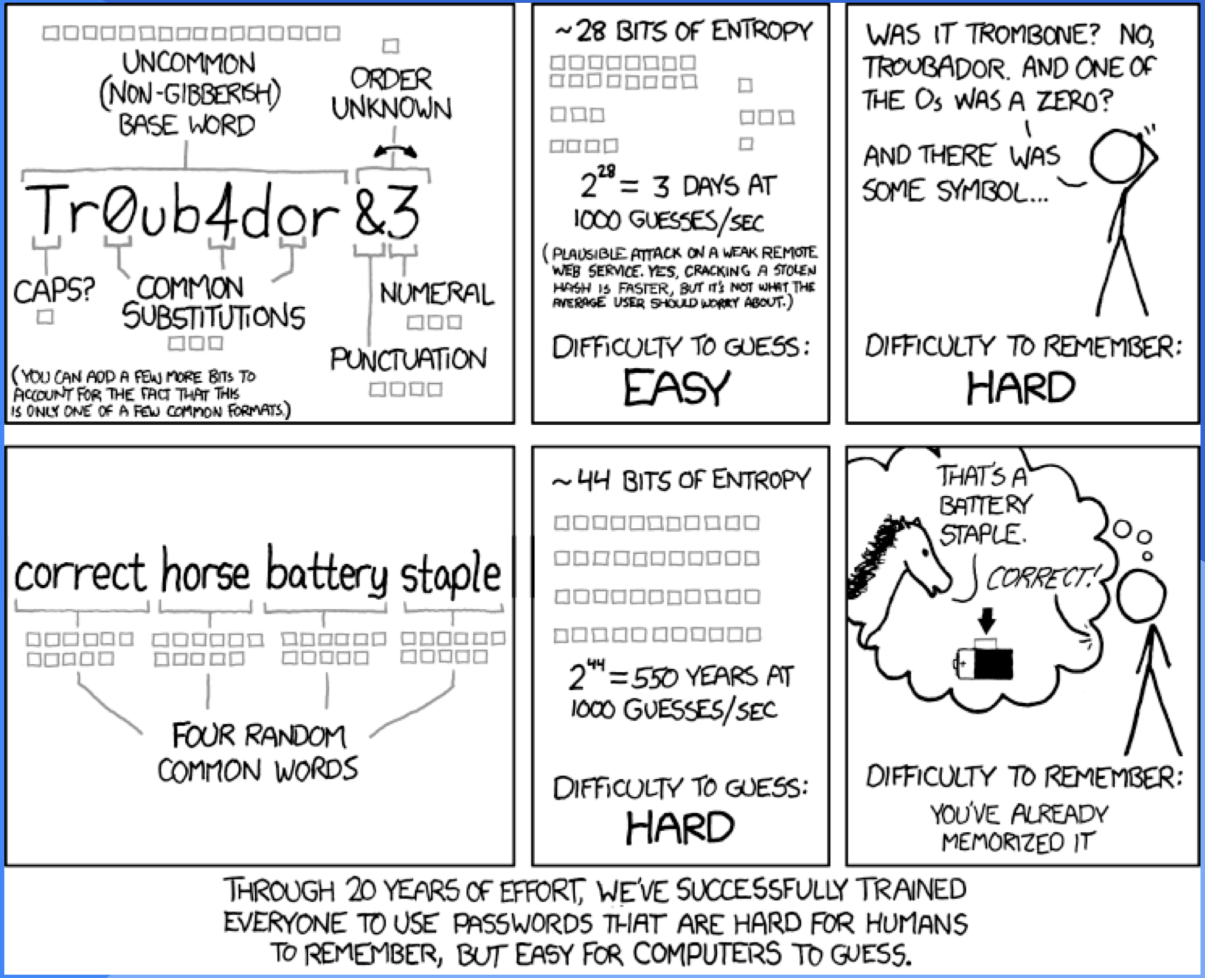
Part 4: Internet Security



Passphrases
not passwords

Google Cloud

Password Length is Better Than Password Complexity!!


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

> “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

Don’t Require Password Changes

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

Google Cloud

Use Unique Passwords!!

haveIbeenpwned.com

Base Password + Cipher (pig latin/Caesar/middle letters of site)

You can't uncompromise biometrics.

Use MFA

82% Reduction in support costs

$16 Cost for Thetis FIDO U2F Key on Amazon

0 Number of exploits reported by Google Employees since they switched to keys

$1,000 The hourly rate for a 3 person incident response team from PCCC

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.

#11, #12 & 13

dmarcian

virtru

A - Setup DKIM & SPF

B - Setup DMARC

C - Look at Dmarcian and Virtru

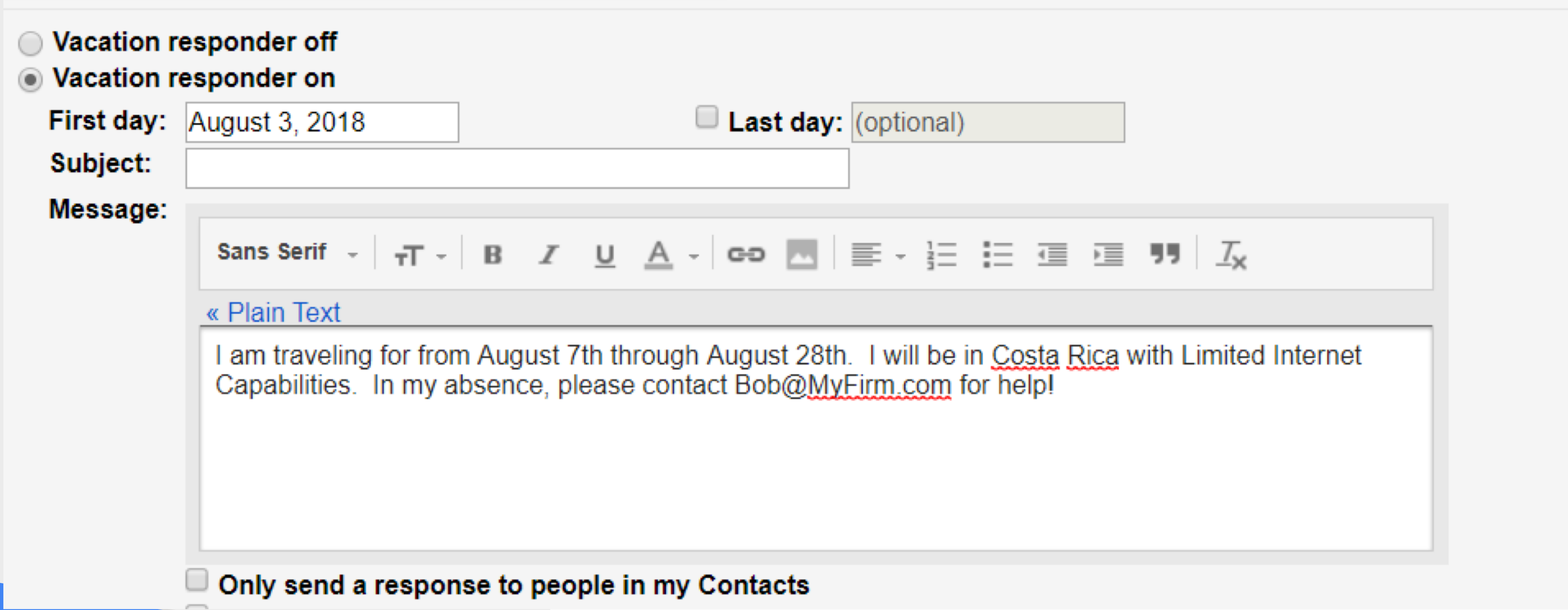
Know your #1 Vector!

91%

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

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

Hackers Love OOM



○ Vacation responder off

● Vacation responder on

First day: August 3, 2018

□ Last day: (optional)

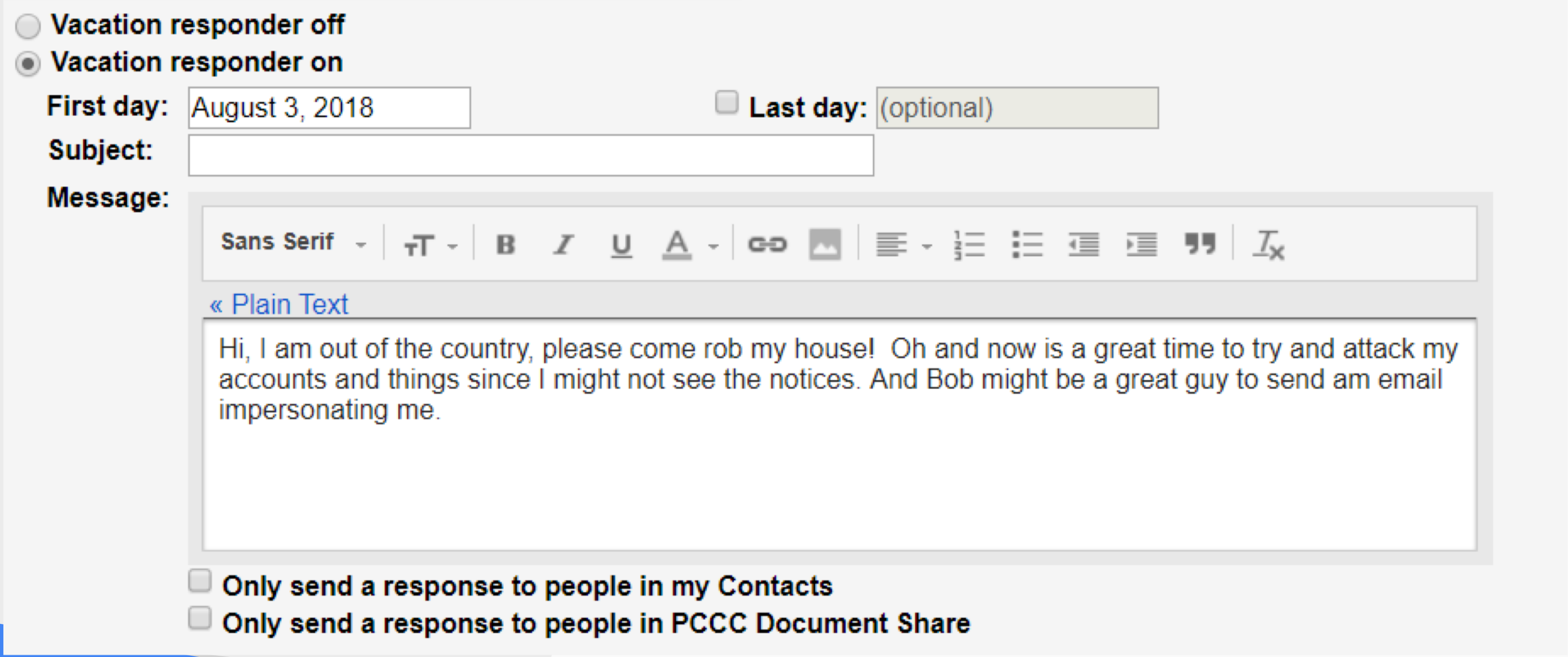
Subject:

Message:

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

Here’s why...



○ Vacation responder off

● Vacation responder on

First day: August 3, 2018 □ Last day: (optional)

Subject:

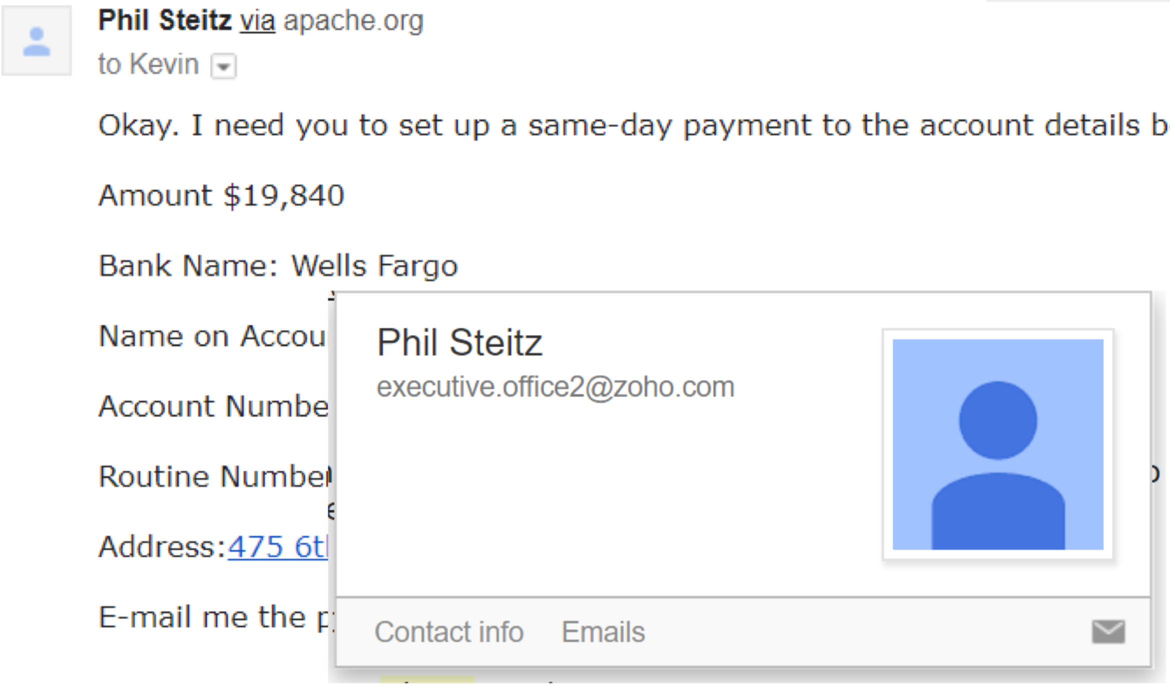
Message:

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 am email impersonating me.

□ Only send a response to people in my Contacts

□ Only send a response to people in PCCC Document Share

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 Accou

Account Numbe

Routine Number

Address:475 6t

E-mail me the p

Phil Steitz

executive.office2@zoho.com

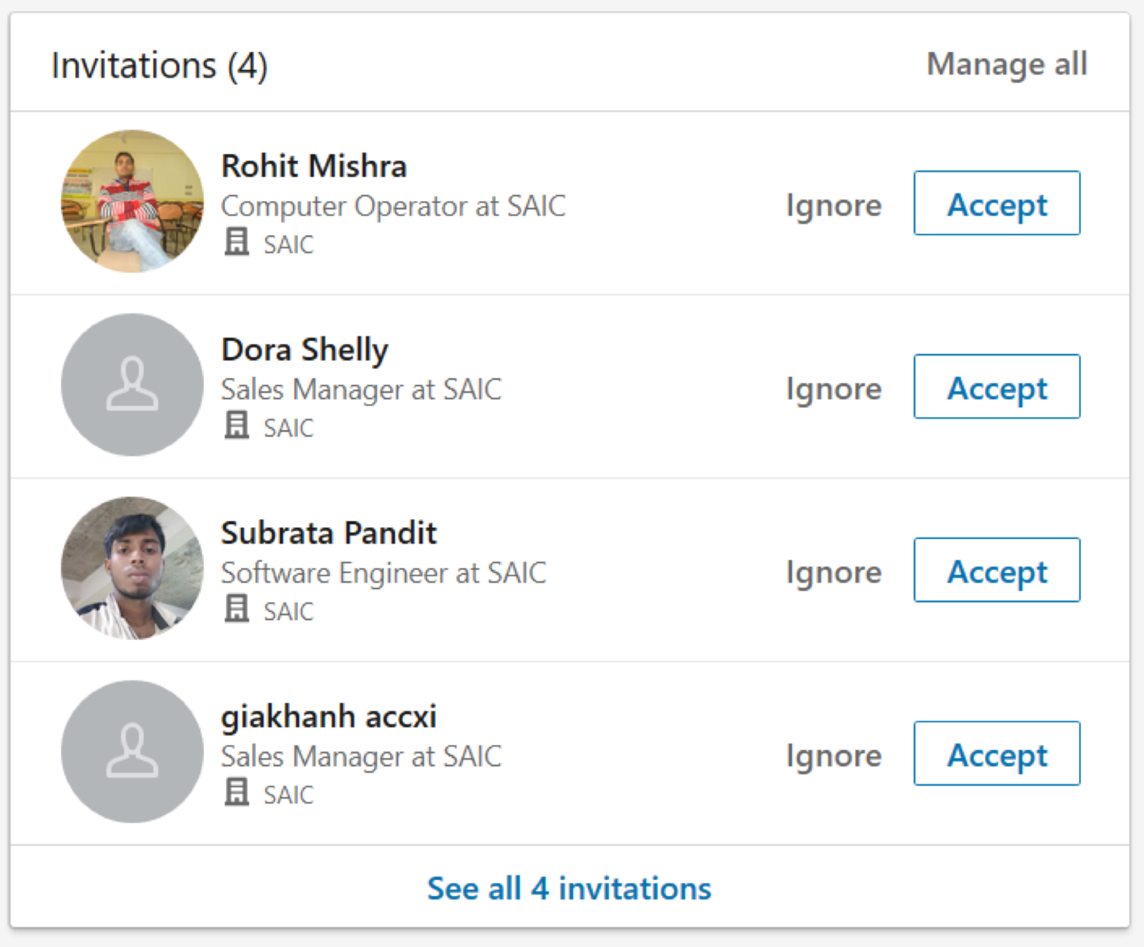
Social Media is a Goldmine

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

#17

Bundesarchiv, Bild 183-37695-0003
Foto: Junge, Peter Heinz | 24. April 1956

Business Social Media Spear Phishing



Invitations (4)

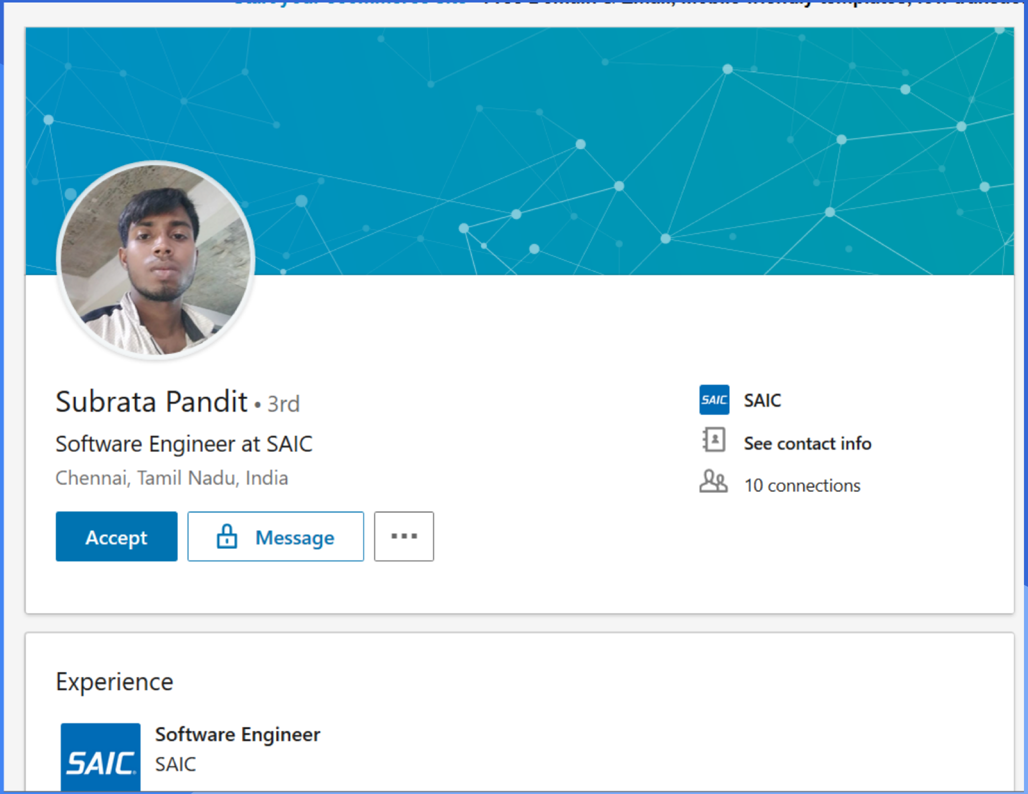
Rohit Mishra
Computer Operator at SAIC
SAIC

Dora Shelly
Sales Manager at SAIC
SAIC

Subrata Pandit
Software Engineer at SAIC
SAIC

giakhanh accxi
Sales Manager at SAIC
SAIC

Worrisome that he has 10 connections…
he had 0… who has he compromised?



Subrata Pandit • 3rd

Software Engineer at SAIC

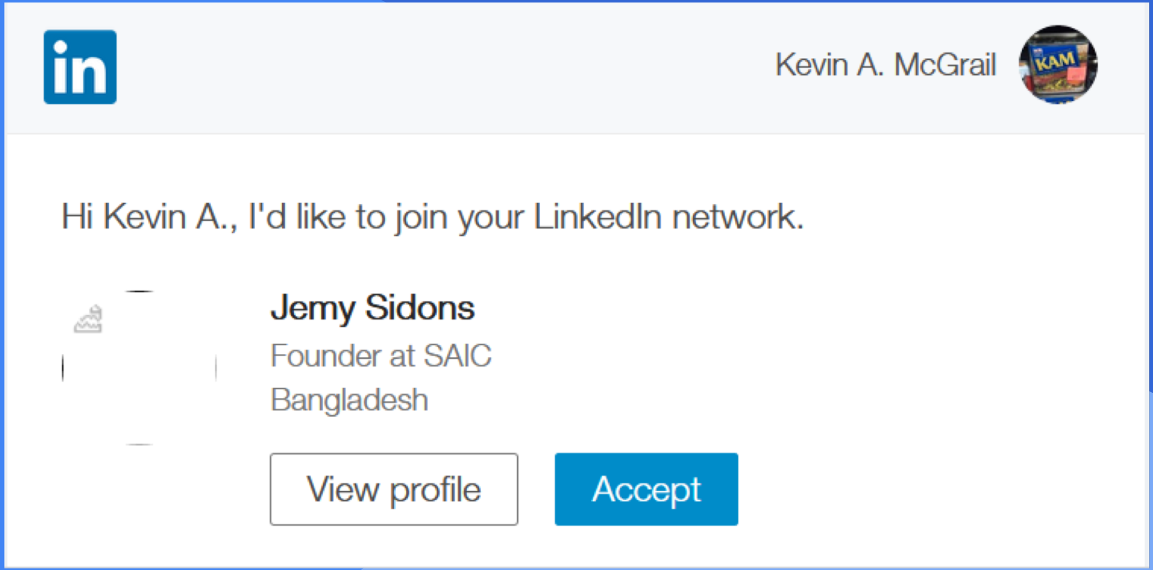
Chennai, Tamil Nadu, India

Experience

Software Engineer
SAIC

https://www.linkedin.com/in/barry-mcguire/

SAIC was founded in 1969...



Kevin A. McGrail

Hi Kevin A., I'd like to join your LinkedIn network.

Jemy Sidons

Founder at SAIC

Bangladesh

Keep Calm and Have an Incident Response Plan

KEY GOALS:
Limit damage / Reduce recovery time / Lower costs

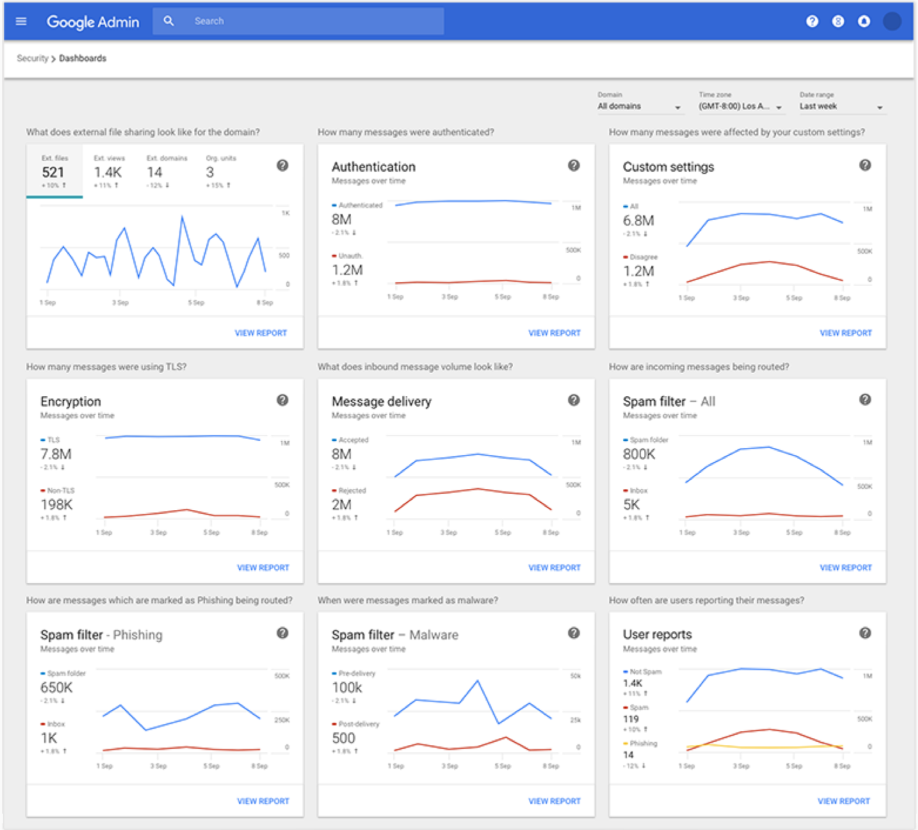
Speed matters

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

Asset Inventory

Paper and Electronic Copies of the Plan

Monitor, AI, NV & Autonomous Response



Google Admin

Security > Dashboards

Domain: All domains · Time zone: (GMT-8:00) Los A... · Date range: Last week

What does external file sharing look like for the domain?

How many messages were authenticated?

Authentication
Messages over time

How many messages were affected by your custom settings?

Custom settings
Messages over time

How many messages were using TLS?

Encryption
Messages over time

What does inbound message volume look like?

Message delivery
Messages over time

How are incoming messages being routed?

Spam filter – All
Messages over time

How are messages which are marked as Phishing being routed?

Spam filter - Phishing
Messages over time

When were messages marked as malware?

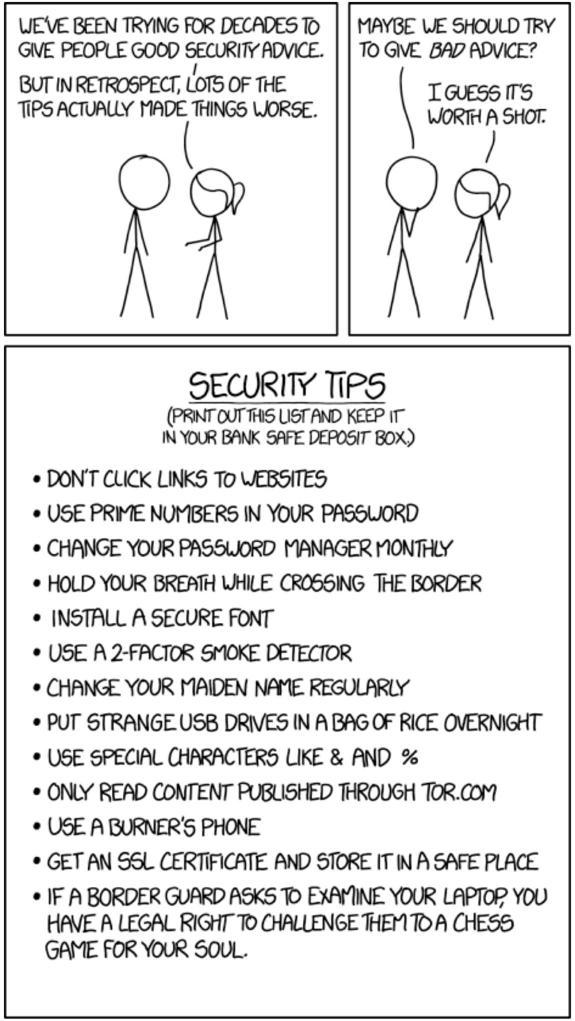
Spam filter – Malware
Messages over time

How often are users reporting their messages?

User reports
Messages over time

Explain “Why?”

Or just use Cunningham’s law...


WE'VE BEEN TRYING FOR DECADES TO GIVE PEOPLE GOOD SECURITY ADVICE.
BUT IN RETROSPECT, LOTS OF THE TIPS ACTUALLY MADE THINGS WORSE.
MAYBE WE SHOULD TRY TO GIVE *BAD* ADVICE?
I GUESS IT'S WORTH A SHOT.
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.

Quis Custodiet Ipsos Custodes?

USENIX / Systems Administrator’s Code of Ethics
https://www.usenix.org/system-administrators-code-ethics

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Sage Advice from a U.S. Founding Father

If you aren't paying for it, you ARE the product.

100
ONE HUNDRED DOLLARS
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
LG 04727792 ★
G7
FRANKLIN
SERIES 2009 A

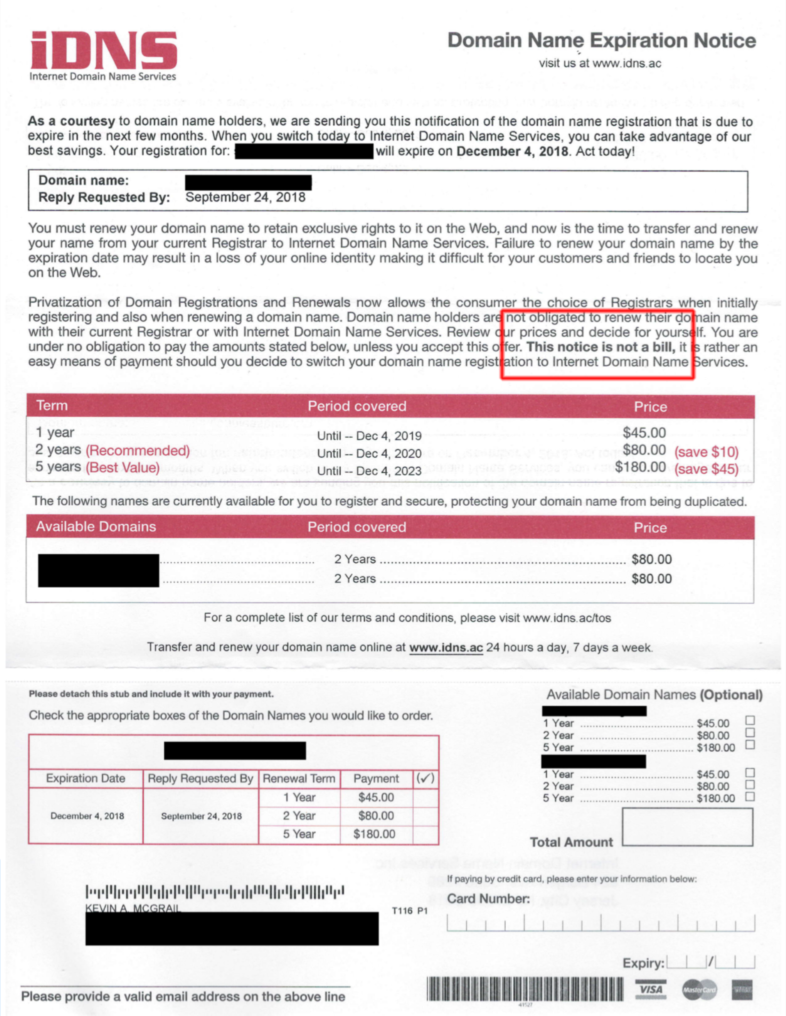
Too good to be true? It probably is...

B Franklin

“Invoice” Scams

“This notice is not a bill…”

Pay no attention to the man behind the curtain…



iDNS
Internet Domain Name Services

Domain Name Expiration Notice

visit us at 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
	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.

[redacted]				
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)**

[redacted]

1 Year	$45.00	□
2 Year	$80.00	□
5 Year	$180.00	□

[redacted]

1 Year	$45.00	□
2 Year	$80.00	□
5 Year	$180.00	□

Total Amount □

KEVIN A. MCGRAIL
[redacted]

T116 P1

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

Card Number:

Expiry: /

41527

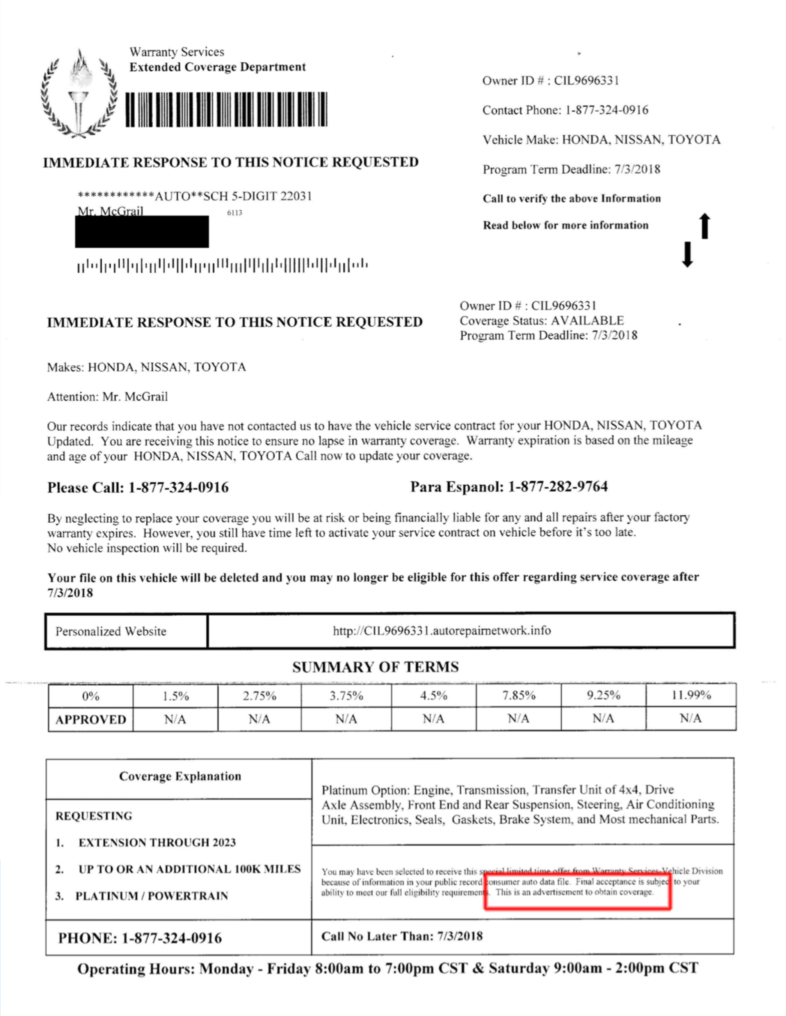
VISA MasterCard

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

IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED

************AUTO**SCH 5-DIGIT 22031
Mr. McGrail 6113
[redacted]

Owner ID # : CIL9696331

Contact Phone: 1-877-324-0916

Vehicle Make: HONDA, NISSAN, TOYOTA

Program Term Deadline: 7/3/2018

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 **1. EXTENSION THROUGH 2023** **2. UP TO OR AN ADDITIONAL 100K MILES** **3. PLATINUM / POWERTRAIN**	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.
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

Offboarding

Make sure exiting employees have their accounts disabled!

BetterCloud

Zero Trust Networks

Based on a poem by Rudyard Kipling, it refers to the Who, What, Why, When, Where and How.

"I KEEP six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest. ..."
From: http://www.kiplingsociety.co.uk/poems_serving.htm

As opposed to a 5-tuple for TCP/IP Layer 3 Firewalls that use Source IP/Port, Destination IP/Port & Protocol.

Thank You!

INFRASHIELD

kmcgrail@infrashield.com

www.linkedin.com/in/kmcgrail

Image Credits:
KAM - Photo by Ted King
XKCD comics CC BY-NC 2.5 from https://xkcd.com/936/ & https://xkcd.com/1820/
KAM photo taken by Ted King, used with permission.
Rings Photo by FOX from Pexels
Angela Merkel Photo from Bundesregierung/Kugler
Chain Photo by Miguel Á. Padriñán from Pexels
Operation Gold Bundesarchiv, Bild 183-37695-0003 / Junge, Peter Heinz / CC-BY-SA 3.0
Facebook & Twitter Logos Brand Resources of their Respective Companies
Lightbulb image by Pixabay CC0 License
Escape Plan Free Template from Edrawsoft.com
Keep Calm Poster, Obverse of 100$ Bill, Ben Franklin Signature & Exit Sign from Public Domain
Security Code Fail taken by Xavier Mertens, used with permission