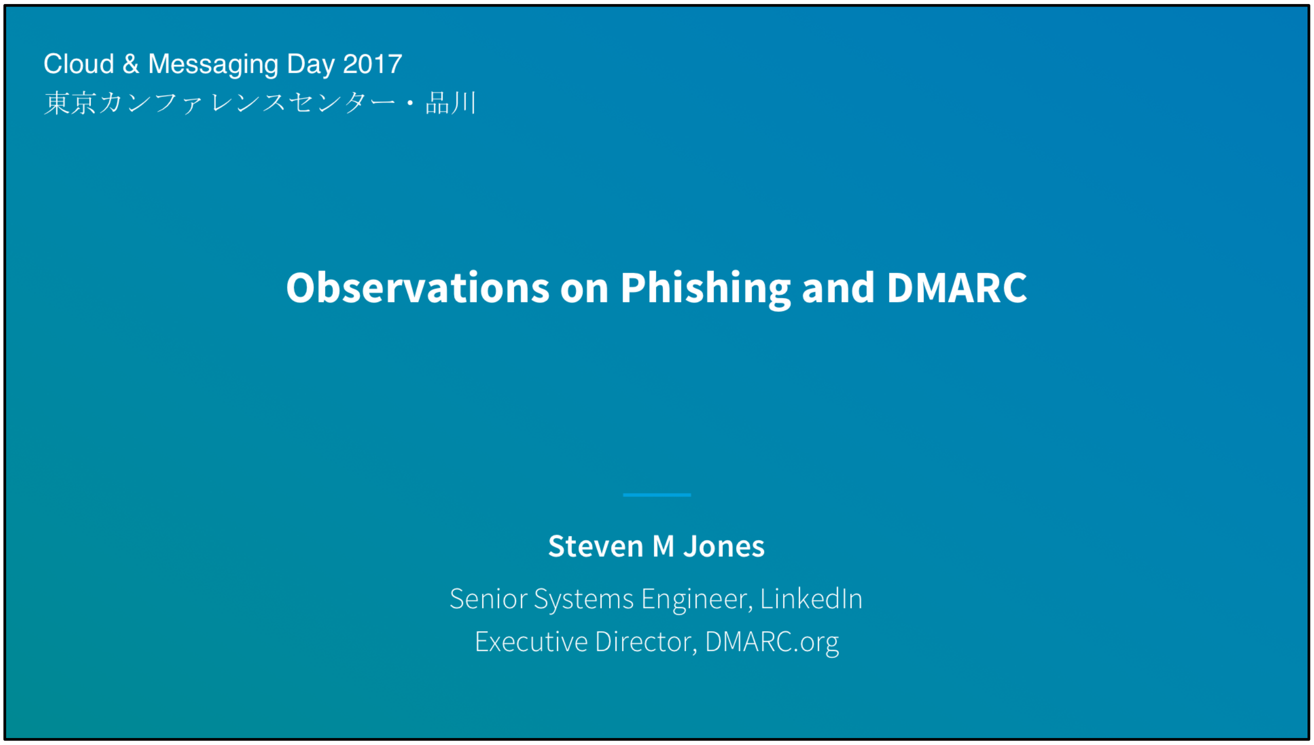
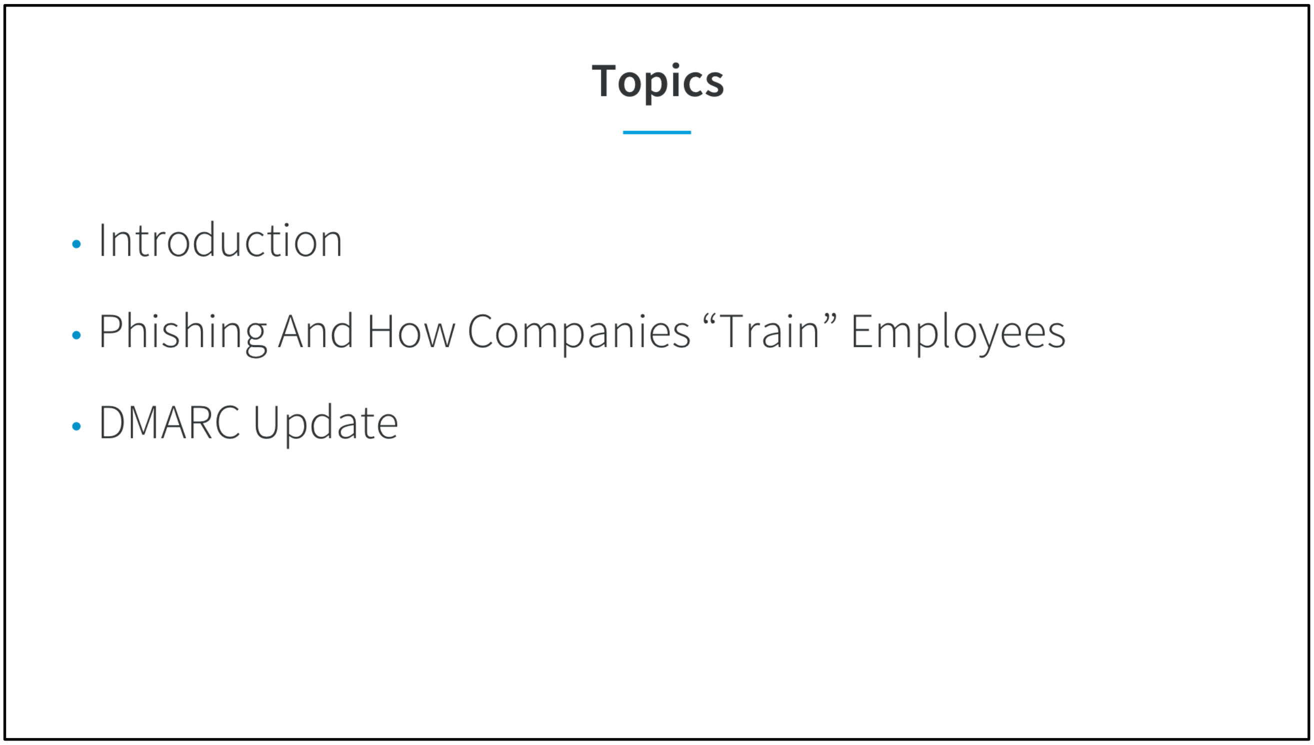


Cloud & Messaging Day 2017
東京カンファレンスセンター・品川

Observations on Phishing and DMARC

Steven M Jones

Senior Systems Engineer, LinkedIn
Executive Director, DMARC.org



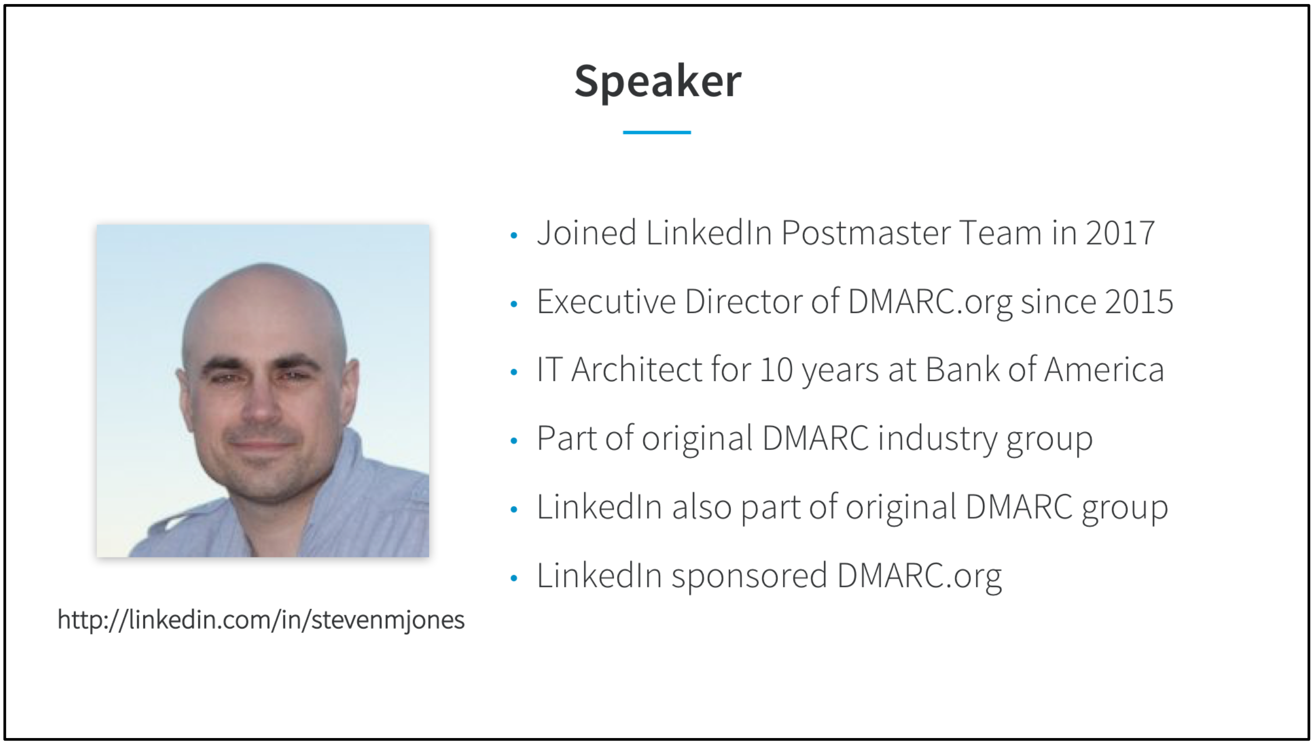
Topics

- Introduction
- Phishing And How Companies “Train” Employees
- DMARC Update

A few words about DMARC.org, LinkedIn, and Japan

A disturbing observation about company email and phishing

An update on DMARC and email authentication

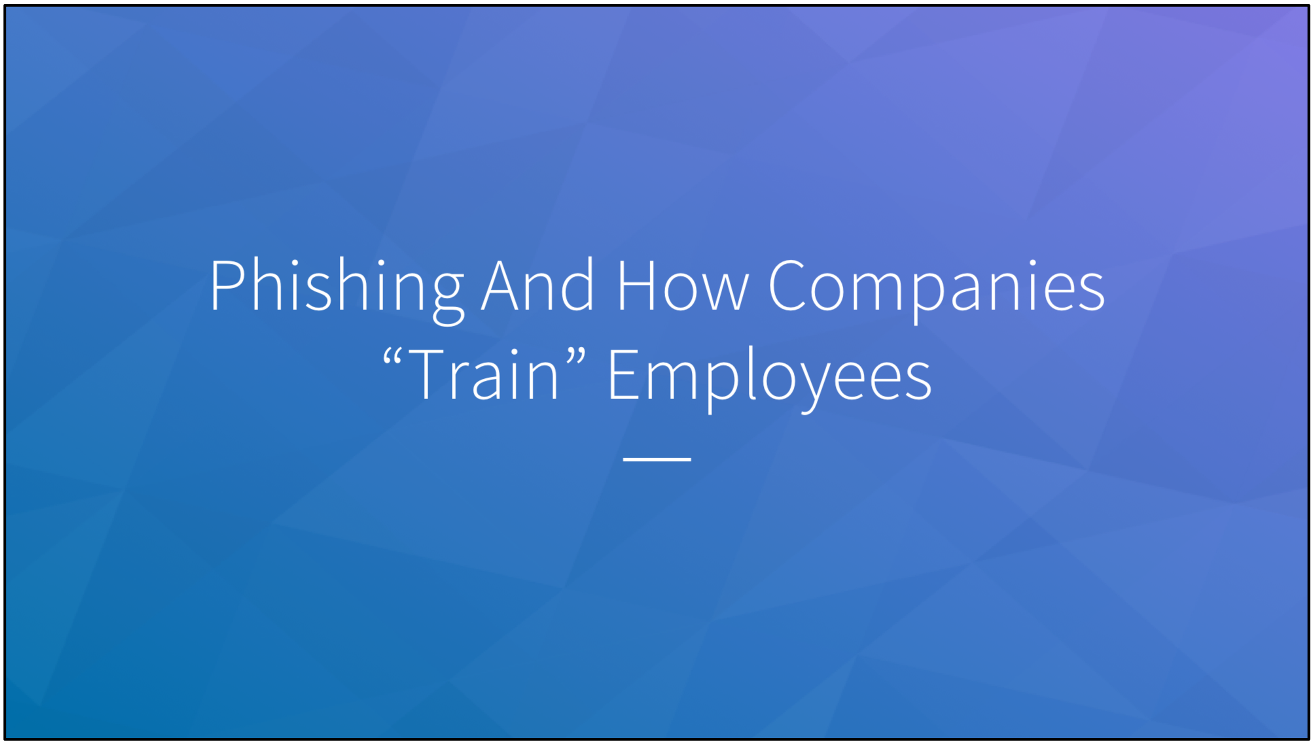


Speaker

- Joined LinkedIn Postmaster Team in 2017
- Executive Director of DMARC.org since 2015
- IT Architect for 10 years at Bank of America
- Part of original DMARC industry group
- LinkedIn also part of original DMARC group
- LinkedIn sponsored DMARC.org

http://linkedin.com/in/stevenmjones

“LinkedIn and Microsoft were both part of the original DMARC project. LinkedIn supported DMARC.org as a non-profit, so it was natural to transition to a full-time position that allows me to continue working on DMARC.org”



Phishing And How Companies “Train” Employees

Companies Hiring Vendors to Phish Employees

Companies developed policies to protect email sent to their customers.

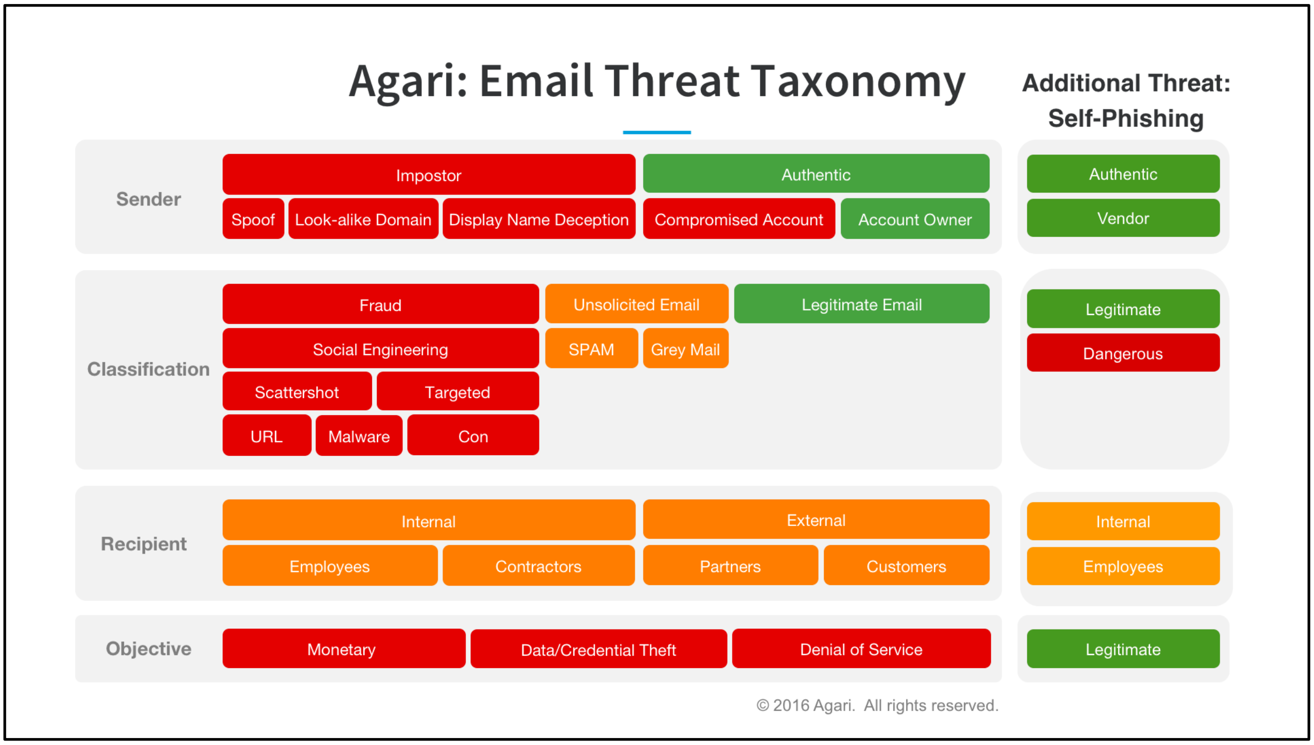
But companies have not done this with communications to their employees.

In the United States employee retirement savings, health insurance, paychecks, and many other services are “outsourced” to other companies.

These companies communicate directly with company employees.

The email communications these companies send do not meet the standards developed for consumer communications – no SPF, no DKIM, no DMARC.

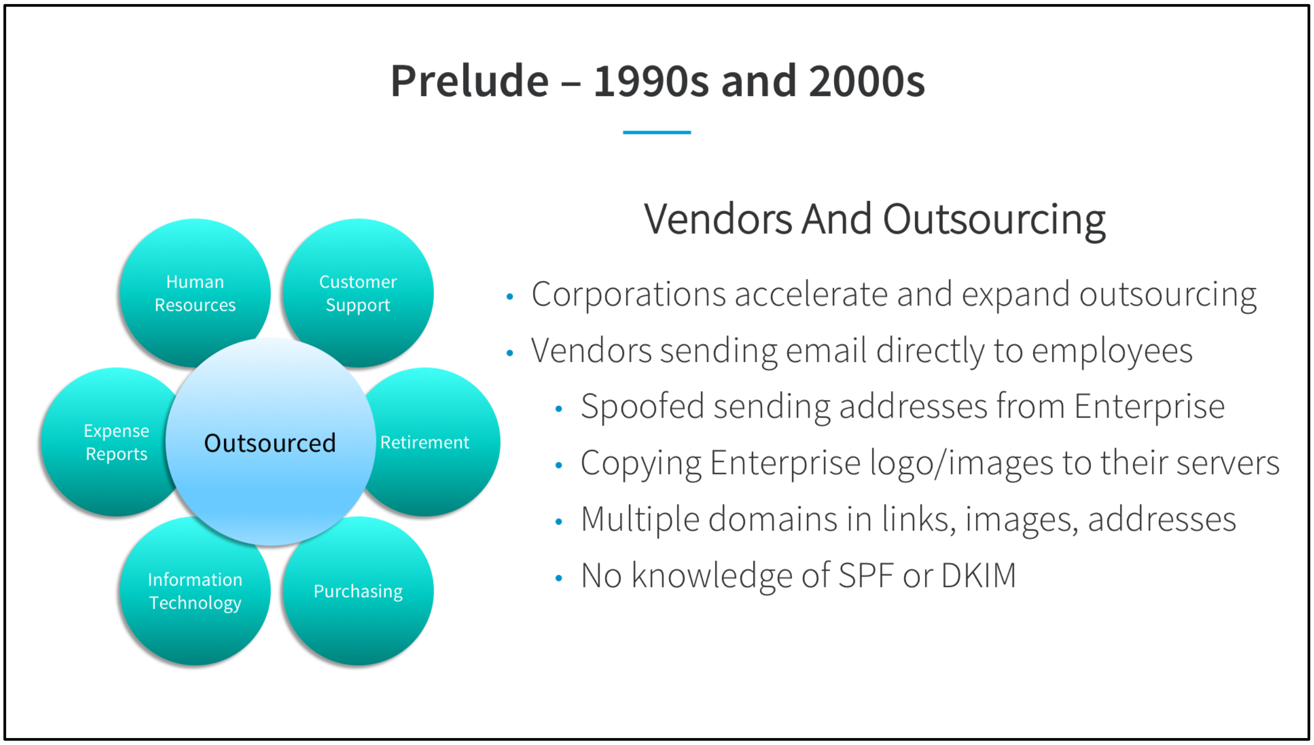
So companies have essentially hired companies to phish their employees, and contradict their anti-phishing training, telling them to trust these messages.



Agari: Email Threat Taxonomy

		Additional Threat: Self-Phishing
Sender	Impostor Spoof · Look-alike Domain · Display Name Deception Authentic Compromised Account · Account Owner	Authentic Vendor
Classification	Fraud Social Engineering Scattershot · Targeted URL · Malware · Con Unsolicited Email SPAM · Grey Mail Legitimate Email	Legitimate Dangerous
Recipient	Internal Employees · Contractors External Partners · Customers	Internal Employees
Objective	Monetary · Data/Credential Theft · Denial of Service	Legitimate

Dr. Markus Jacobsson of Agari has developed this taxonomy to describe all the ways malicious email is constructed. This is a very useful model, but it leaves out the threat of legitimate messages sent from a vendor that confuse employees – and contradict their anti-phishing training - by looking like phishing messages.



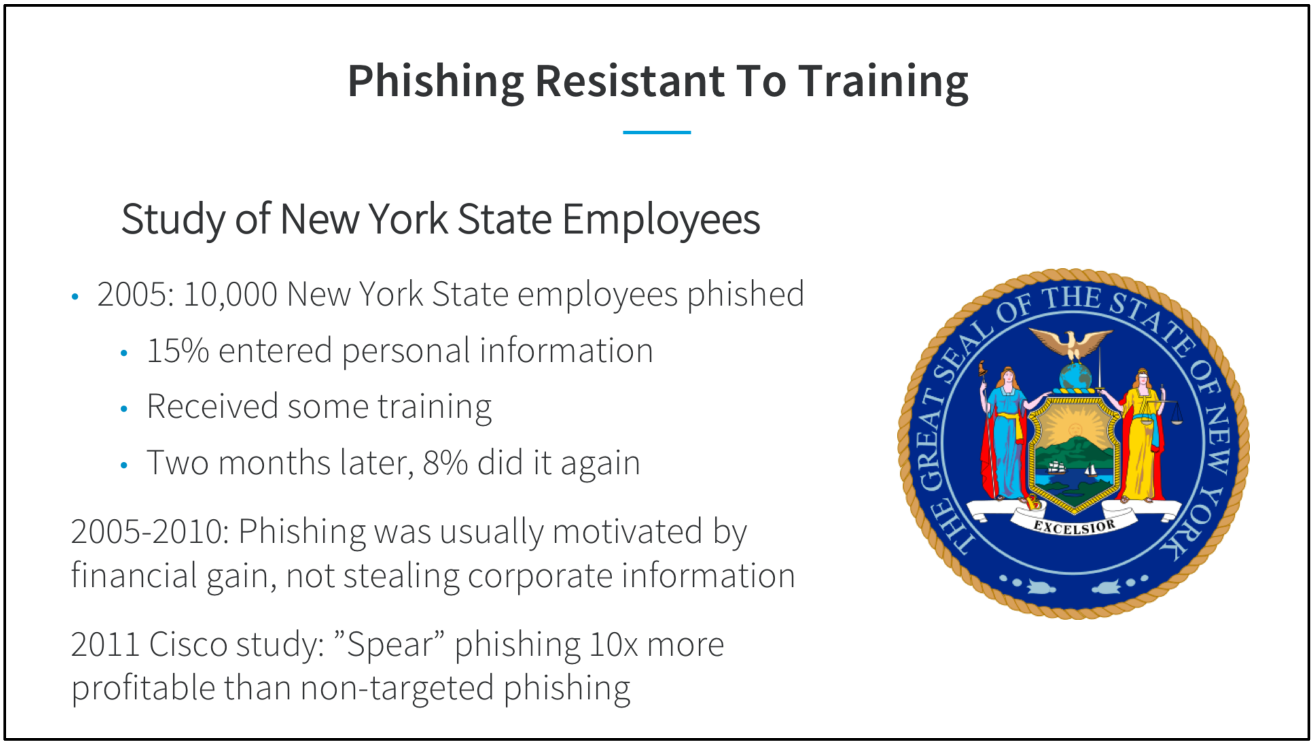
Prelude – 1990s and 2000s

Human Resources
Customer Support
Expense Reports
Outsourced
Retirement
Information Technology
Purchasing

Vendors And Outsourcing

- Corporations accelerate and expand outsourcing
- Vendors sending email directly to employees
  - Spoofed sending addresses from Enterprise
  - Copying Enterprise logo/images to their servers
  - Multiple domains in links, images, addresses
  - No knowledge of SPF or DKIM

In mid-2000s we would routinely discover new outsourced projects when the in-house contact complained that their vendor’s messages were being blocked by anti-spam filters.



Phishing Resistant To Training

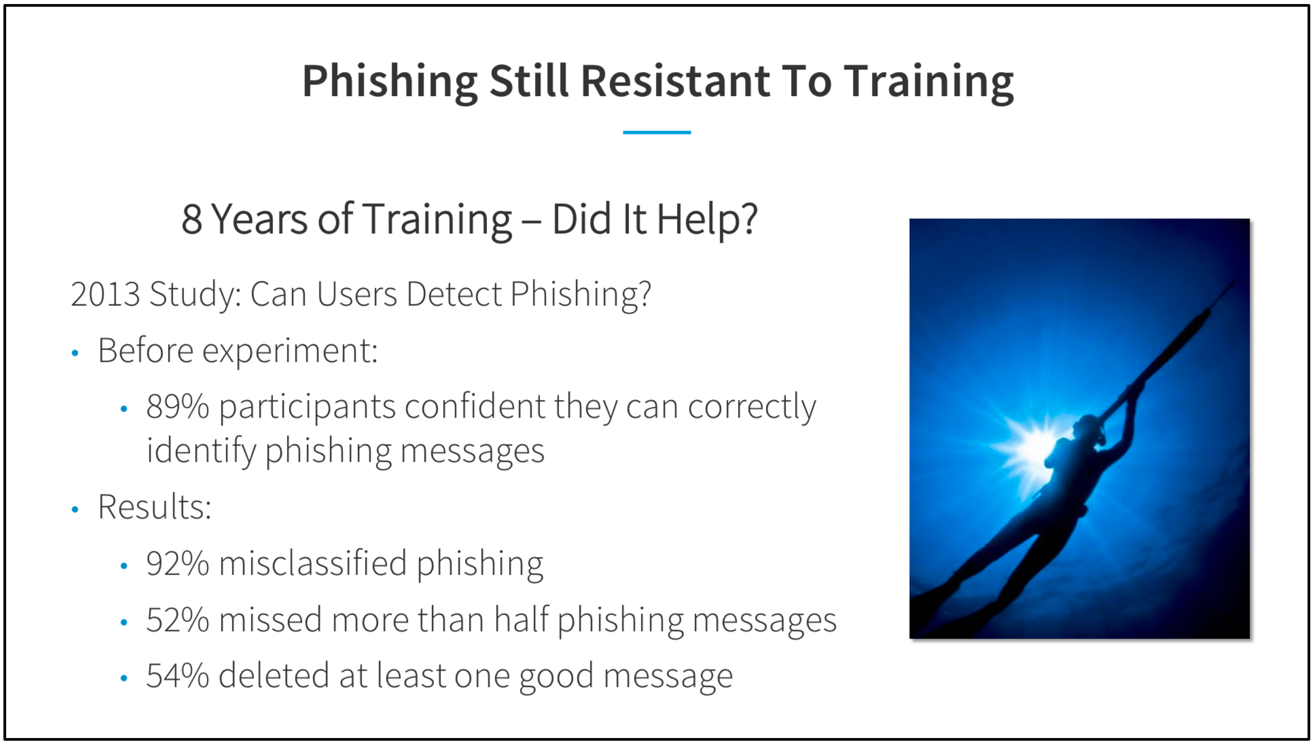
Study of New York State Employees

- 2005: 10,000 New York State employees phished
  - 15% entered personal information
  - Received some training
  - Two months later, 8% did it again

2005-2010: Phishing was usually motivated by financial gain, not stealing corporate information

2011 Cisco study: ”Spear” phishing 10x more profitable than non-targeted phishing

NYState study: https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/IEEESecurityPrivacy-SpearPhishing-Jan-Feb2014.pdf
* Cisco phishing story from 2005
Cisco spear phishing study: https://www.darkreading.com/mobile/targeted-attacks-10-times-more-profitable-than-mass-campaigns/d/d-id/1135960



Phishing Still Resistant To Training

8 Years of Training – Did It Help?

2013 Study: Can Users Detect Phishing?

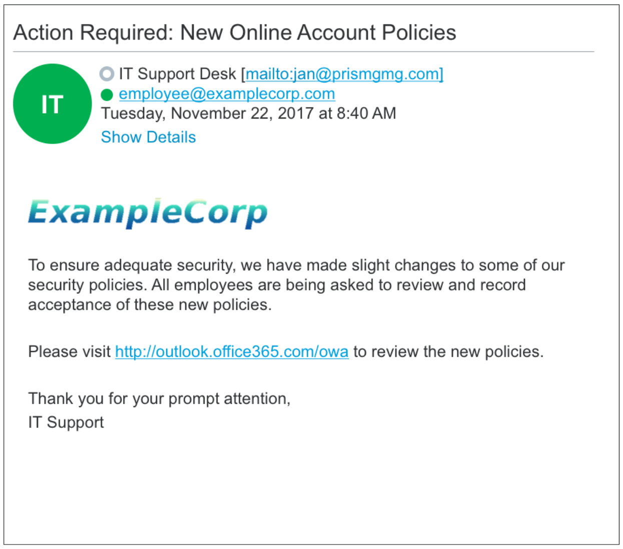
- Before experiment:
  - 89% participants confident they can correctly identify phishing messages
- Results:
  - 92% misclassified phishing
  - 52% missed more than half phishing messages
  - 54% deleted at least one good message

Source: A paper presented at the 2013 International Human Factors and Ergonomics Society Annual Meeting about phishing emails. https://www.welivesecurity.com/2013/07/25/overconfident-introverted-study-reveals-personality-traits-of-perfect-phishing-victims/

Why Is Phishing So Successful

- Some aspects are due to human nature
  - We are busy and distracted at work
  - Messages “look right”
- Some problems companies increase through their actions
  - Companies don’t see the confusion these vendors cause
  - No internal communications policy (company → employee)
  - Different departments using different outsourced vendors
  - Addresses and links using multiple, external domains
  - Anti-phishing training is a tedious, once-a-year obstacle to work

Which Is Phishing, Which Is Outsourced?



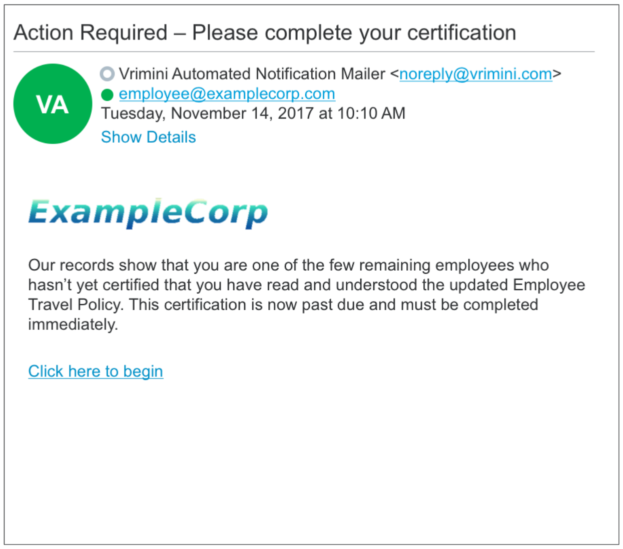
Action Required: New Online Account Policies

○ IT Support Desk [mailto:jan@prismgmg.com]
● employee@examplecorp.com
Tuesday, November 22, 2017 at 8:40 AM

To ensure adequate security, we have made slight changes to some of our security policies. All employees are being asked to review and record acceptance of these new policies.

Please visit http://outlook.office365.com/owa to review the new policies.

Thank you for your prompt attention,
IT Support



Action Required – Please complete your certification

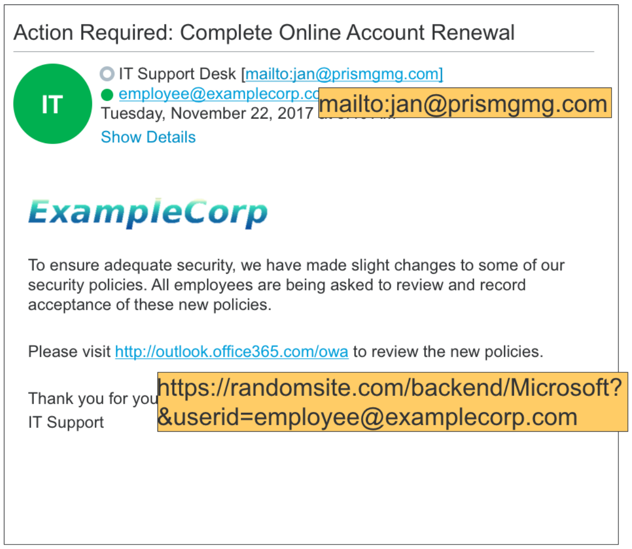
○ Vrimini Automated Notification Mailer <noreply@vrimini.com>
● employee@examplecorp.com
Tuesday, November 14, 2017 at 10:10 AM

Our records show that you are one of the few remaining employees who hasn't yet certified that you have read and understood the updated Employee Travel Policy. This certification is now past due and must be completed immediately.

Click here to begin

We have changed the company names, but these are both examples based on real messages received by company employees.

This Is Phishing



Action Required: Complete Online Account Renewal

IT

○ IT Support Desk [mailto:jan@prismgmg.com]
● employee@examplecorp.co
Tuesday, November 22, 2017
Show Details

mailto:jan@prismgmg.com

ExampleCorp

To ensure adequate security, we have made slight changes to some of our security policies. All employees are being asked to review and record acceptance of these new policies.

Please visit http://outlook.office365.com/owa to review the new policies.

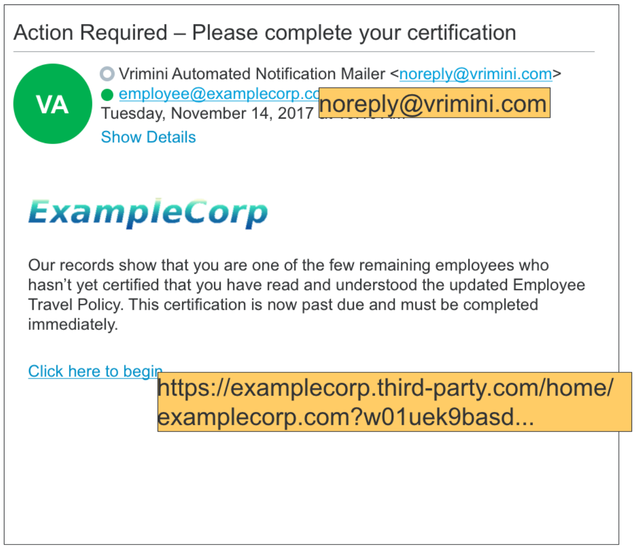
Thank you for you

IT Support

https://randomsite.com/backend/Microsoft?&userid=employee@examplecorp.com

- From: address is external
- Urgent Call-To-Action
- Uses expected company logo
- Link goes to external site
- Link displayed doesn’t match target
- Link domain doesn’t match From:

This Is Outsourced



Action Required – Please complete your certification

VA

○ Vrimini Automated Notification Mailer <noreply@vrimini.com>
● employee@examplecorp.co
Tuesday, November 14, 2017
Show Details

noreply@vrimini.com

Our records show that you are one of the few remaining employees who hasn't yet certified that you have read and understood the updated Employee Travel Policy. This certification is now past due and must be completed immediately.

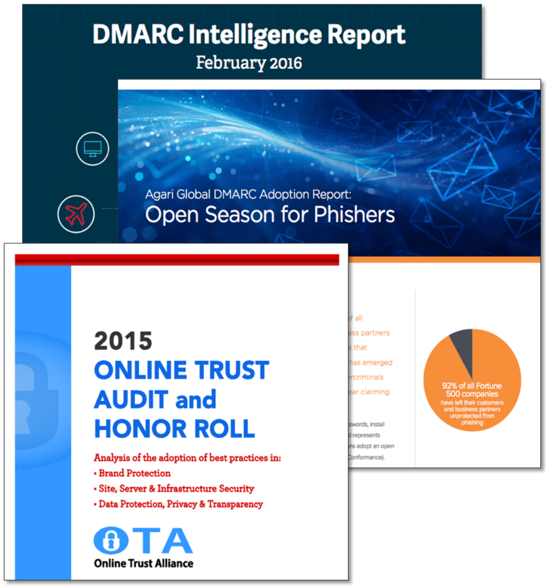
Click here to begin

https://examplecorp.third-party.com/home/examplecorp.com?w01uek9basd...

- From: address is external
- Urgent Call-To-Action
- Uses expected company logo
- Link goes to external site
- Link doesn't show URL
- Link shown doesn't match target
- Link domain doesn't match From:

This legitimate campaign frequently reported as phishing!
This practice – and problem – did not develop overnight. But we must start to pay attention to securing these communications, just as we have started securing communications to customers.

Phishing is Growing (So Is DMARC)



DMARC Intelligence Report

February 2016

Agari Global DMARC Adoption Report:

Open Season for Phishers

f all
ss partners
 that
has emerged
rcriminals
ar claiming

swords, install
d represents
s adopt an open
Conformance).

92% of all Fortune 500 companies
have left their customers and business partners unprotected from phishing

2015

ONLINE TRUST AUDIT and HONOR ROLL

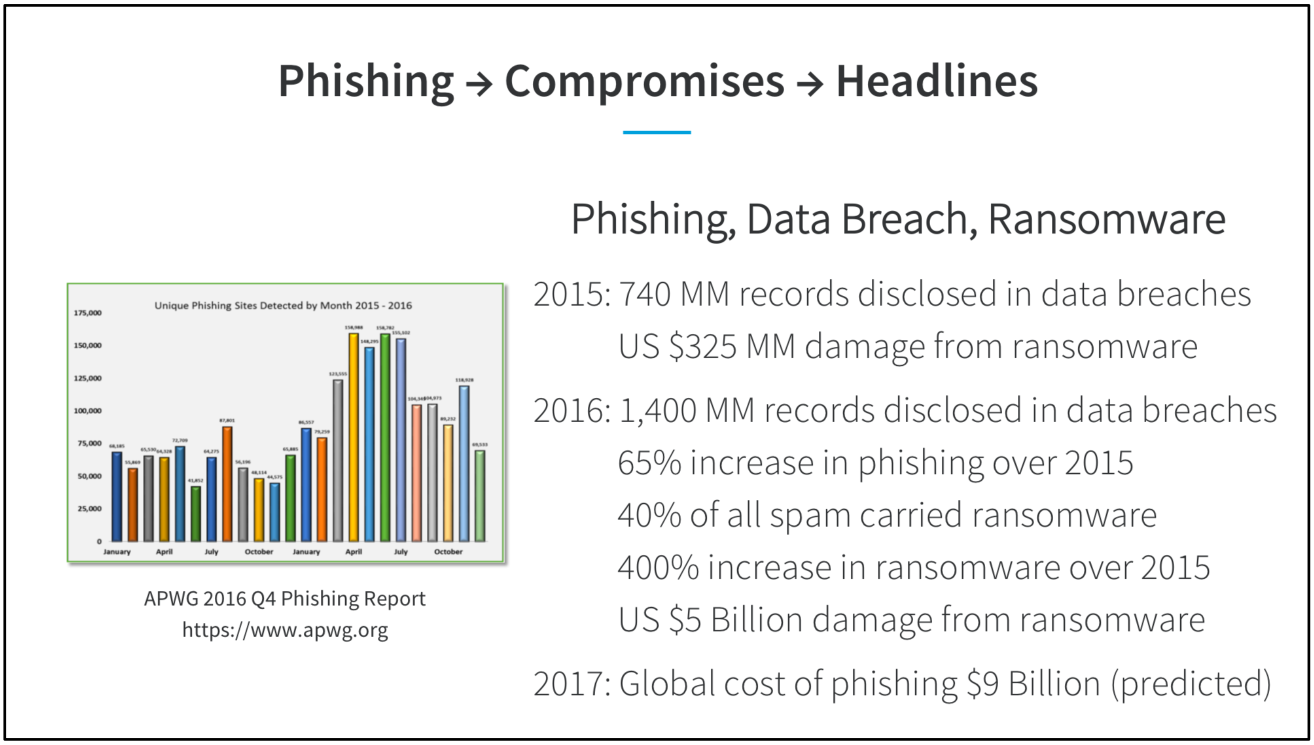
Analysis of the adoption of best practices in:

- Brand Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

OTA

Online Trust Alliance

- Annual reports have tracked growth of spam & phishing for many years
- Phishing a greater threat than spam
- Industry analysts (Gartner) add email authentication to their buying guides
- Growth of DMARC 2012 - 2015
- Recent focus on DMARC “reject”
- Will they focus on internal communications in 2018?


Unique Phishing Sites Detected by Month 2015 - 2016
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
68,185
55,869
65,530
64,328
72,709
41,852
64,275
87,801
56,196
48,114
44,575
65,885
86,557
79,259
123,555
158,988
148,295
158,782
155,102
104,348
104,973
89,232
118,928
69,533
January
April
July
October
January
April
July
October

Phishing → Compromises → Headlines

APWG 2016 Q4 Phishing Report
https://www.apwg.org

Phishing, Data Breach, Ransomware

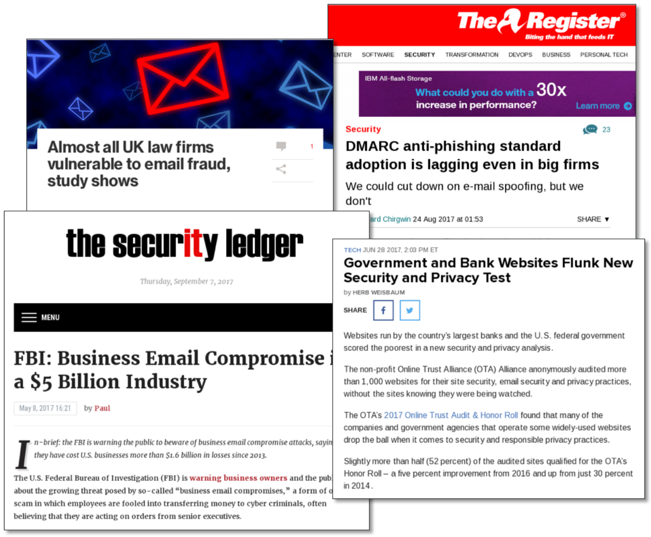
2015: 740 MM records disclosed in data breaches
US $325 MM damage from ransomware

2016: 1,400 MM records disclosed in data breaches
65% increase in phishing over 2015
40% of all spam carried ransomware
400% increase in ransomware over 2015
US $5 Billion damage from ransomware

2017: Global cost of phishing $9 Billion (predicted)

2013 phishing figure: https://www.phishingusertraining.com/the-cost-of-phishing/
2015-2016 data breach: http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf
2016 phish figures: https://blog.barkly.com/phishing-statistics-2016
2017 phish cost figure: https://www.rsa.com/en-us/blog/2016-12/2017-global-fraud-cybercrime-forecast
APWG 2016Q1 report: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf
Ransomware stats: http://invenioit.com/security/ransomware-statistics-2016/
400% ransomware: https://www.scmagazine.com/ransomware-attacks-will-double-in-2017-study/article/634560/
Ransomware damage costs: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

News Articles Calling For Solutions



Almost all UK law firms vulnerable to email fraud, study shows

1

The Register®
Biting the hand that feeds IT

ENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

IBM All-flash Storage
What could you do with a 30x increase in performance? Learn more

Security

23

DMARC anti-phishing standard adoption is lagging even in big firms

We could cut down on e-mail spoofing, but we don't

ard Chirgwin 24 Aug 2017 at 01:53

SHARE ▾

the security ledger

Thursday, September 7, 2017

MENU

FBI: Business Email Compromise i a $5 Billion Industry

May 8, 2017 16:21 by Paul

In-brief: the FBI is warning the public to beware of business email compromise attacks, sayin they have cost U.S. businesses more than $1.6 billion in losses since 2013.

The U.S. Federal Bureau of Investigation (FBI) is warning business owners and the pub about the growing threat posed by so-called "business email compromises," a form of o scam in which employees are fooled into transferring money to cyber criminals, often believing that they are acting on orders from senior executives.

TECH JUN 28 2017, 2:03 PM ET

Government and Bank Websites Flunk New Security and Privacy Test

by HERB WEISBAUM

SHARE f 🐦

Websites run by the country's largest banks and the U.S. federal government scored the poorest in a new security and privacy analysis.

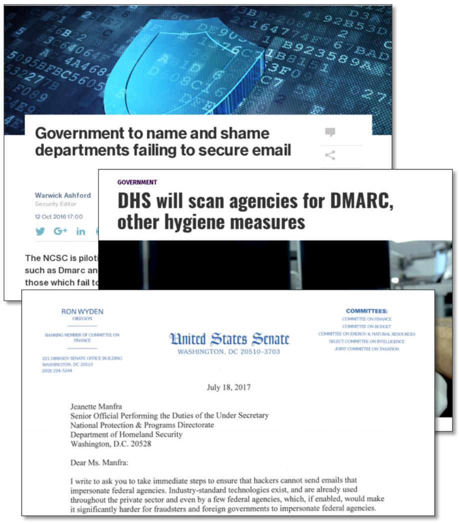
The non-profit Online Trust Alliance (OTA) Alliance anonymously audited more than 1,000 websites for their site security, email security and privacy practices, without the sites knowing they were being watched.

The OTA's 2017 Online Trust Audit & Honor Roll found that many of the companies and government agencies that operate some widely-used websites drop the ball when it comes to security and responsible privacy practices.

Slightly more than half (52 percent) of the audited sites qualified for the OTA's Honor Roll – a five percent improvement from 2016 and up from just 30 percent in 2014.

- The Press Has Noticed!
- Crime is accelerating, leading news
- Email is often the vector for attacks
- Industry and press push for solutions, asking why DMARC isn't used more widely
- Increase in data breaches, and press focus on it, will change focus of all companies

Government Views Evolving



Government to name and shame departments failing to secure email

Warwick Ashford
Security Editor
12 Oct 2016 17:00

The NCSC is piloti
such as Dmarc an
those which fail to

GOVERNMENT

DHS will scan agencies for DMARC, other hygiene measures

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

July 18, 2017

Jeanette Manfra
Senior Official Performing the Duties of the Under Secretary
National Protection & Programs Directorate
Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Manfra:

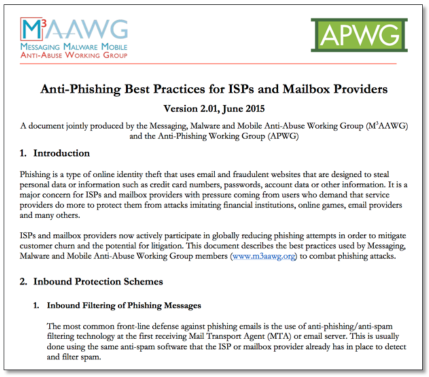
I write to ask you to take immediate steps to ensure that hackers cannot send emails that impersonate federal agencies. Industry-standard technologies exist, and are already used throughout the private sector and even by a few federal agencies, which, if enabled, would make it significantly harder for fraudsters and foreign governments to impersonate federal agencies.

- Dutch, German agencies moved early
- US and Australian agencies followed
- UK sets national policy in November 2016
- FTC and NIST make strong recommendations
- Senator Wyden calls for US government adoption
- October: US DHS announces DMARC requirement

What Should Companies Do?

Stop Acting Like Phishers

- Consistent use of domains
- All images and links in same domain as From:
- Using SPF, DKIM, and DMARC
- Preferably no clickable links
  - Short Intranet links (“go/this-service”)
- Communicate policies to employees
  - “We will never ask you to click a link to reset your password.”



M^{3}AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

APWG

Anti-Phishing Best Practices for ISPs and Mailbox Providers

Version 2.01, June 2015

A document jointly produced by the Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) and the Anti-Phishing Working Group (APWG)

1. Introduction

Phishing is a type of online identity theft that uses email and fraudulent websites that are designed to steal personal data or information such as credit card numbers, passwords, account data or other information. It is a major concern for ISPs and mailbox providers with pressure coming from users who demand that service providers do more to protect them from attacks imitating financial institutions, online games, email providers and many others.

ISPs and mailbox providers now actively participate in globally reducing phishing attempts in order to mitigate customer churn and the potential for litigation. This document describes the best practices used by Messaging, Malware and Mobile Anti-Abuse Working Group members (www.m3aawg.org) to combat phishing attacks.

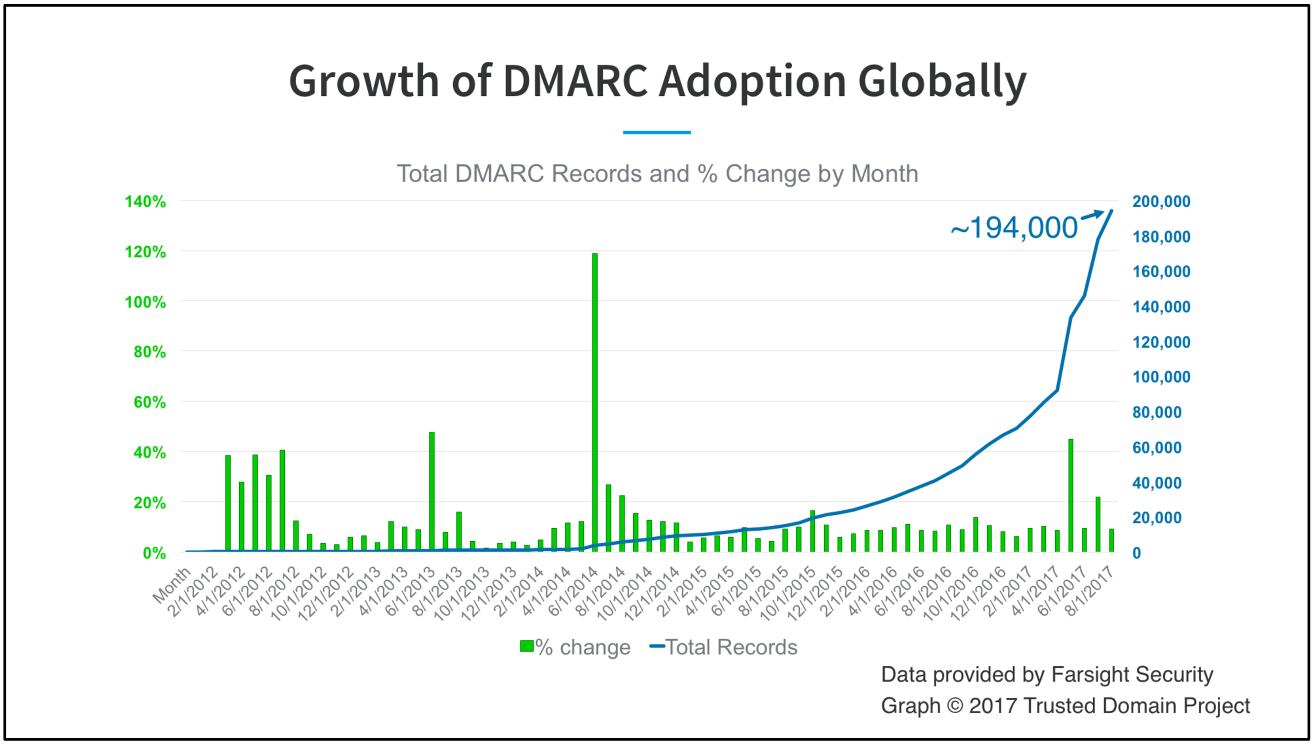
2. Inbound Protection Schemes

1. Inbound Filtering of Phishing Messages

The most common front-line defense against phishing emails is the use of anti-phishing/anti-spam filtering technology at the first receiving Mail Transport Agent (MTA) or email server. This is usually done using the same anti-spam software that the ISP or mailbox provider already has in place to detect and filter spam.

https://www.m3aawg.org/published-documents

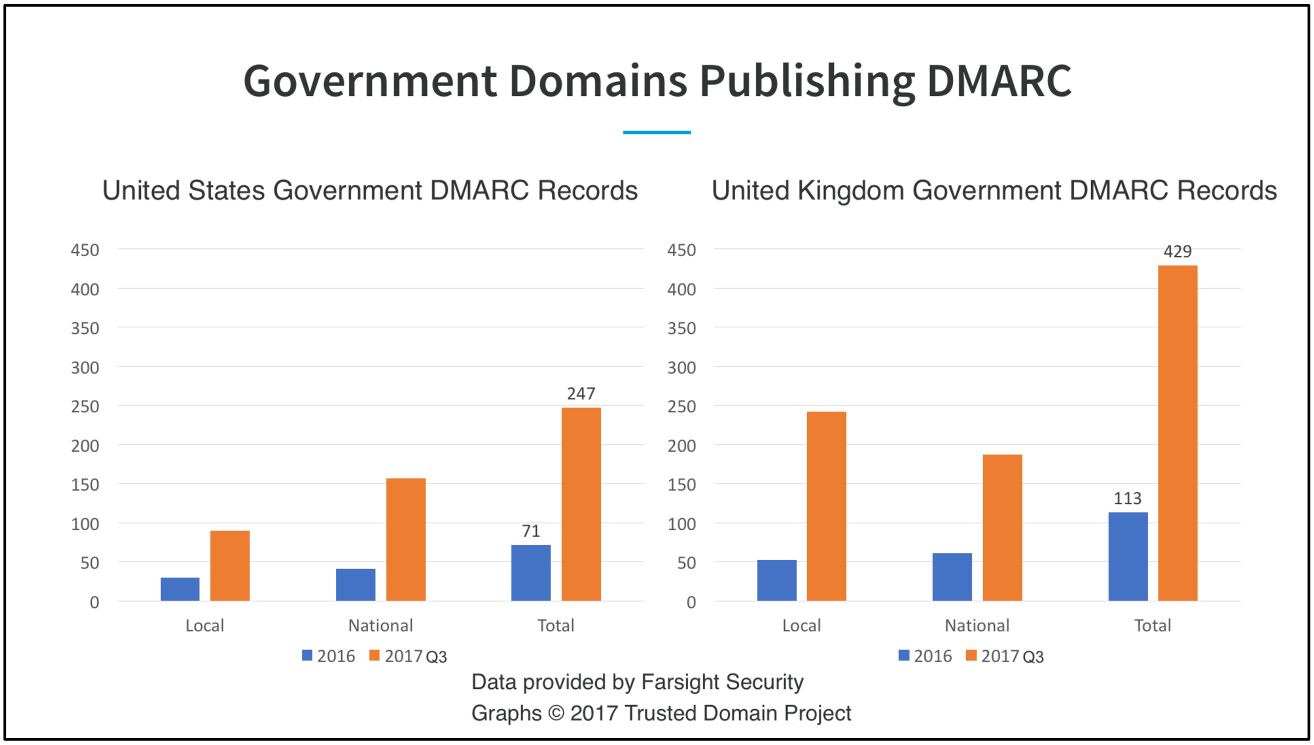
DMARC Update



Growth of DMARC Adoption Globally

Data provided by Farsight Security
Graph © 2017 Trusted Domain Project

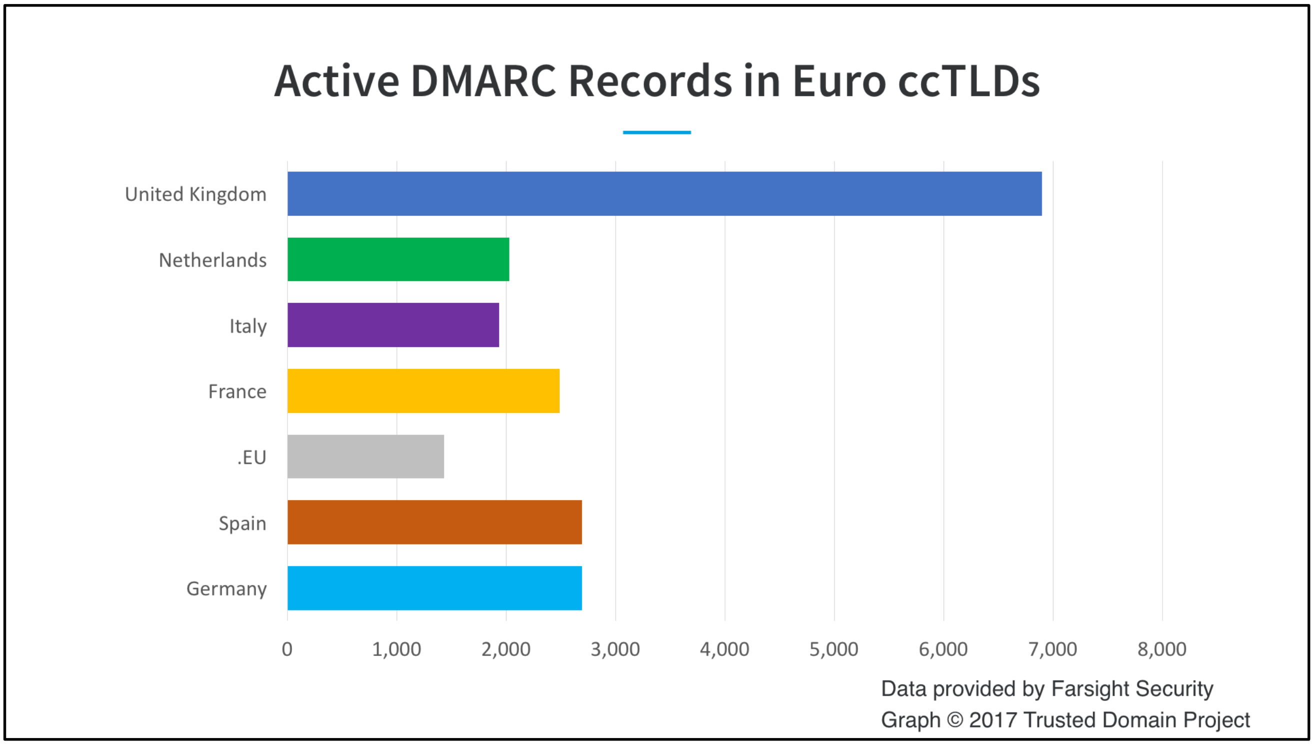
Only 62,000 ending same quarter in 2016. We only include domains that are still publishing DMARC records.
For the graph above, our figure for 2016-09 reflects domains that first published a DMARC record from 2012-01 through 2016-09, and which are still published as of 2017-10. Therefore the figure shown in the graph for 2016-09 is 48,838 – however, when these same records were checked in 2016-10, the total was roughly 62,000. Between 2016-10 and 2017-10, roughly 13,000 domains that had published DMARC records before 2016-10 withdrew their records, lowering the total observed in 2017-10.



Government Domains Publishing DMARC

Data provided by Farsight Security
Graphs © 2017 Trusted Domain Project

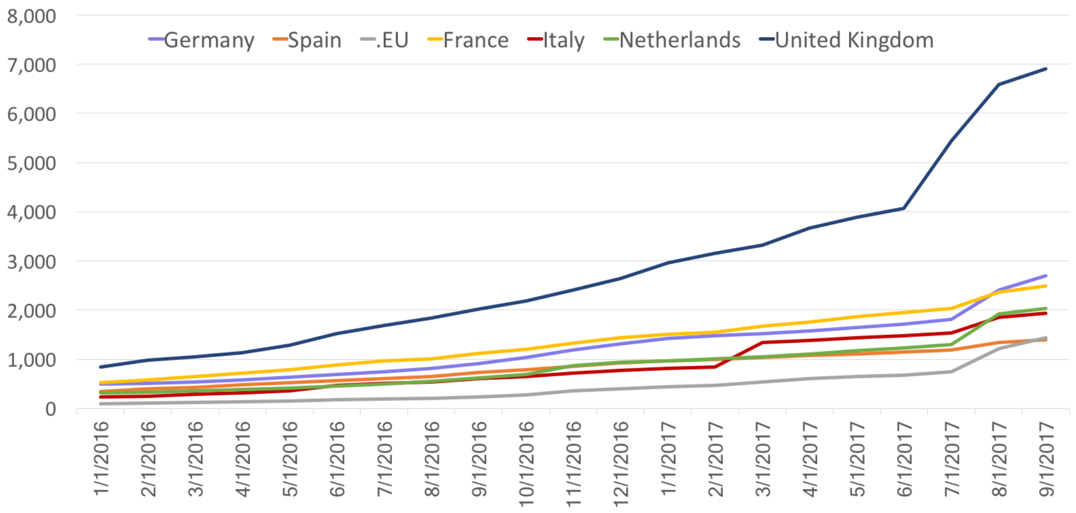
United States ~350% 2017 versus 2016
United Kingdom 380% 2017 versus 2016



Active DMARC Records in Euro ccTLDs

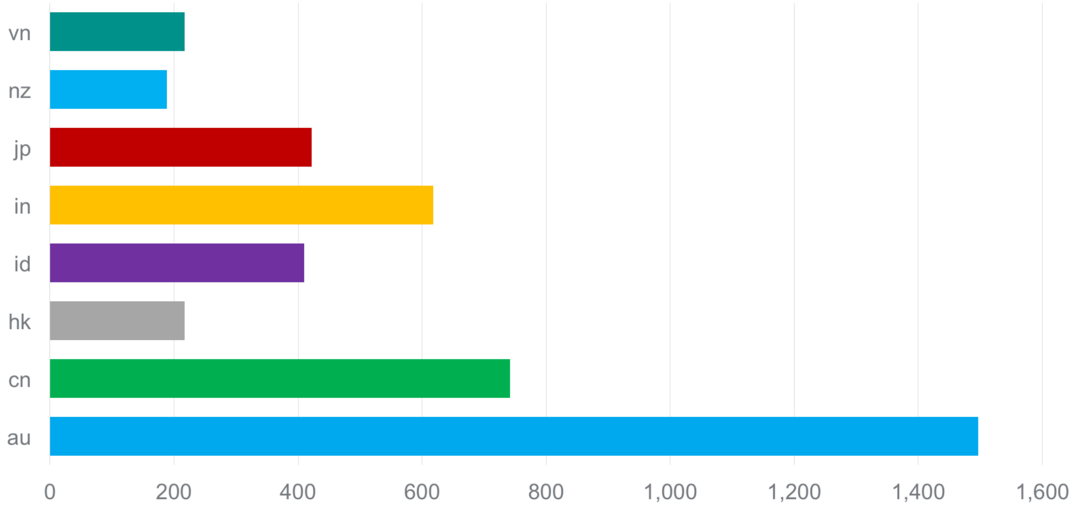
Data provided by Farsight Security
Graph © 2017 Trusted Domain Project

Active DMARC Records in European ccTLDs



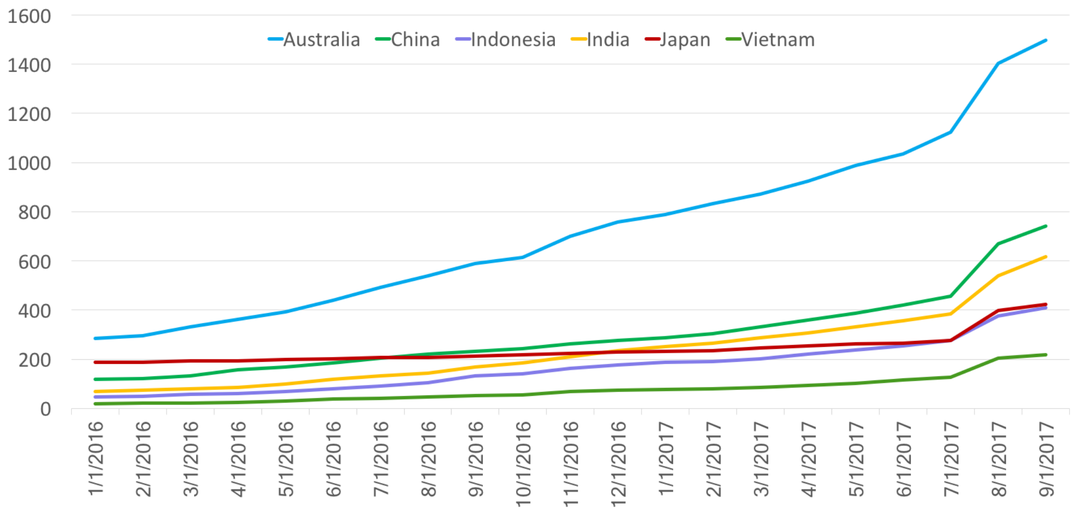
Data provided by Farsight Security
Graph © 2017 Trusted Domain Project

Active DMARC Records in Asia ccTLDs



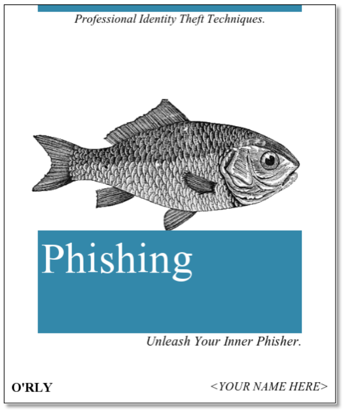
Data provided by Farsight Security
Graph © 2017 Trusted Domain Project

Active DMARC Records in Asian ccTLDs

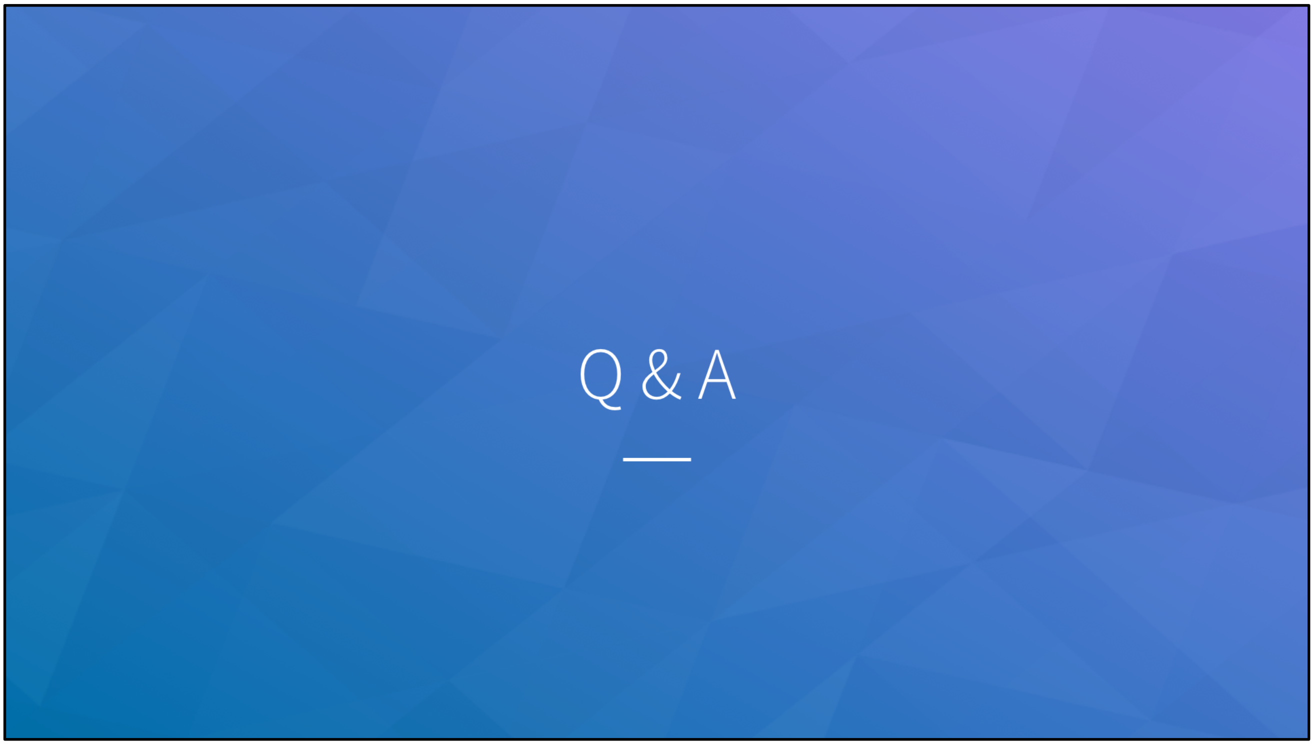


Data provided by Farsight Security
Graph © 2017 Trusted Domain Project

Predictions


Professional Identity Theft Techniques.
Phishing
Unleash Your Inner Phisher.
O'RLY
<YOUR NAME HERE>

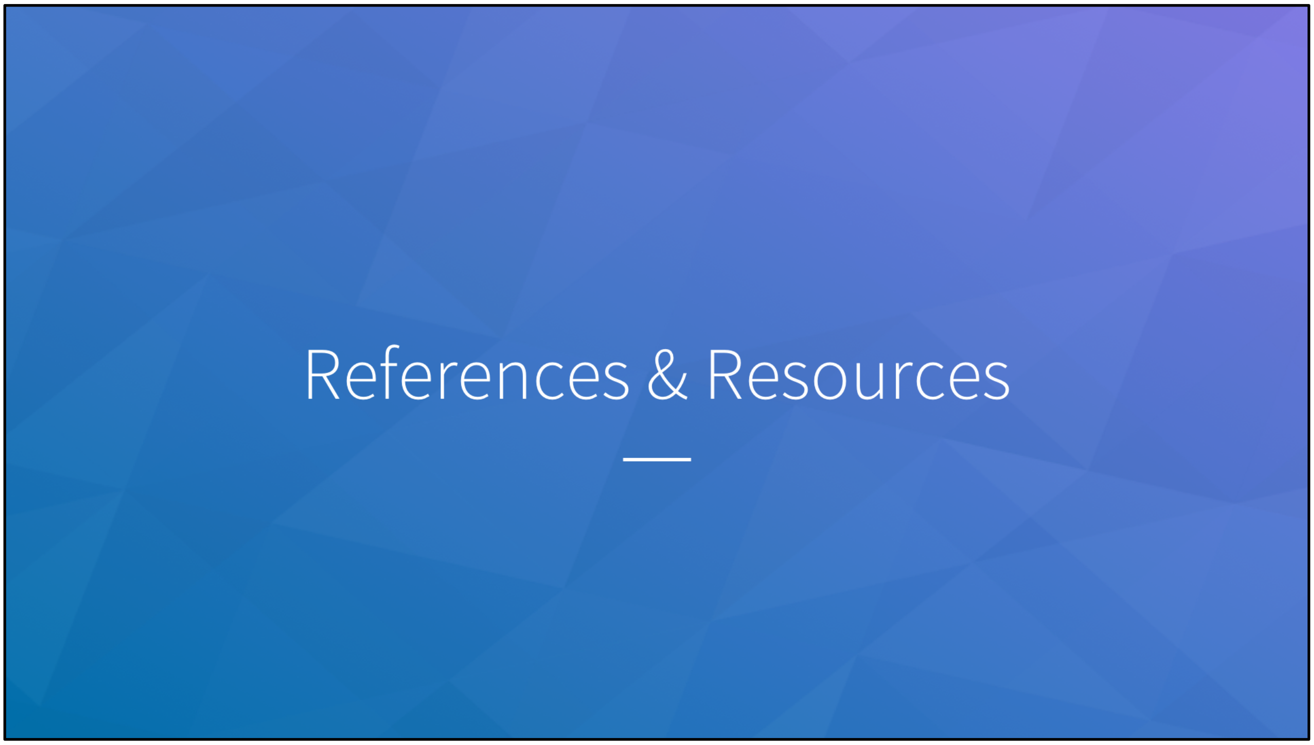
- Phishing will continue to grow, spam steady or declines
- More governments will recommend/require DMARC
- ARC protocol will help address limitations of DMARC
  - OpenARC implementation ships in 2017 Q4
- Global ISPs resume motion toward "No Auth, No Entry"
  - Google, Microsoft
- More visual indicators of authentication for end users
- DMARC adoption up 300% through 3Q2017,
  but perhaps 200% in 2018 due to increased scale



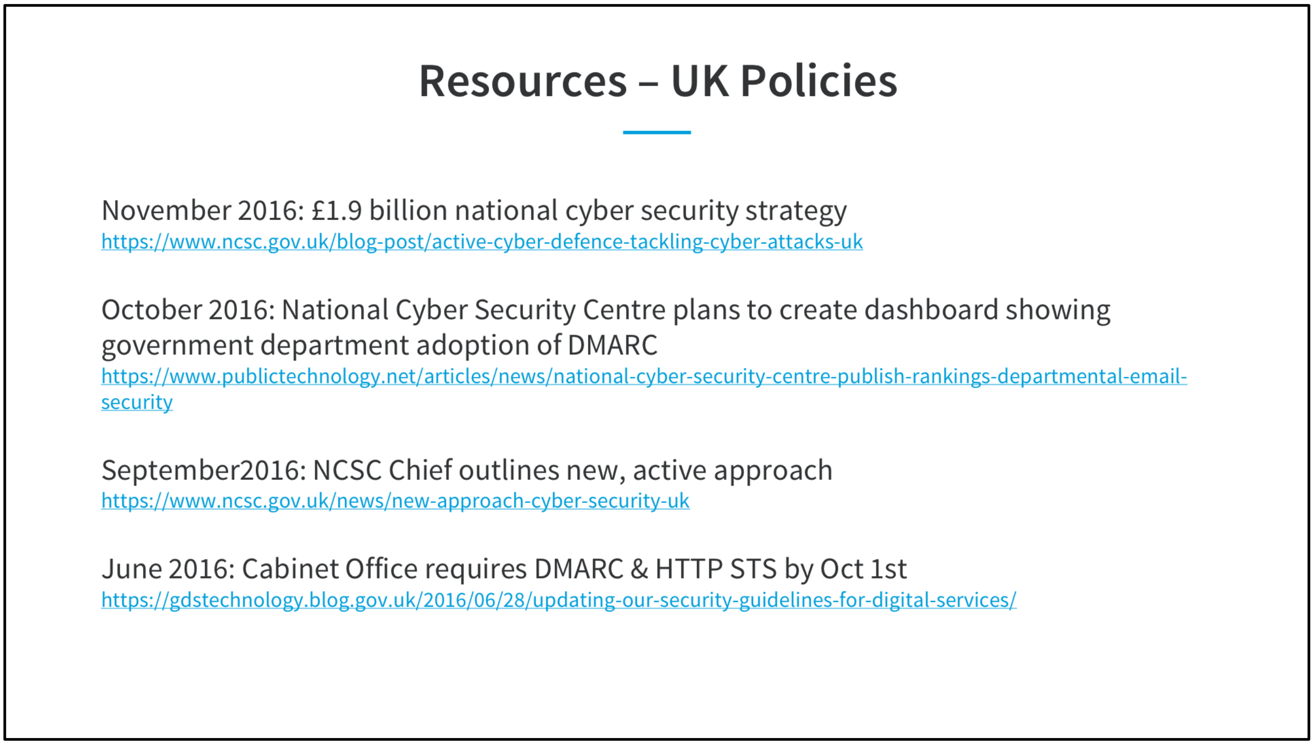
Q & A

ありがとうございました

Thank you



References & Resources



Resources – UK Policies

November 2016: £1.9 billion national cyber security strategy
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

October 2016: National Cyber Security Centre plans to create dashboard showing government department adoption of DMARC
https://www.publictechnology.net/articles/news/national-cyber-security-centre-publish-rankings-departmental-email-security

September2016: NCSC Chief outlines new, active approach
https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

June 2016: Cabinet Office requires DMARC & HTTP STS by Oct 1st
https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/

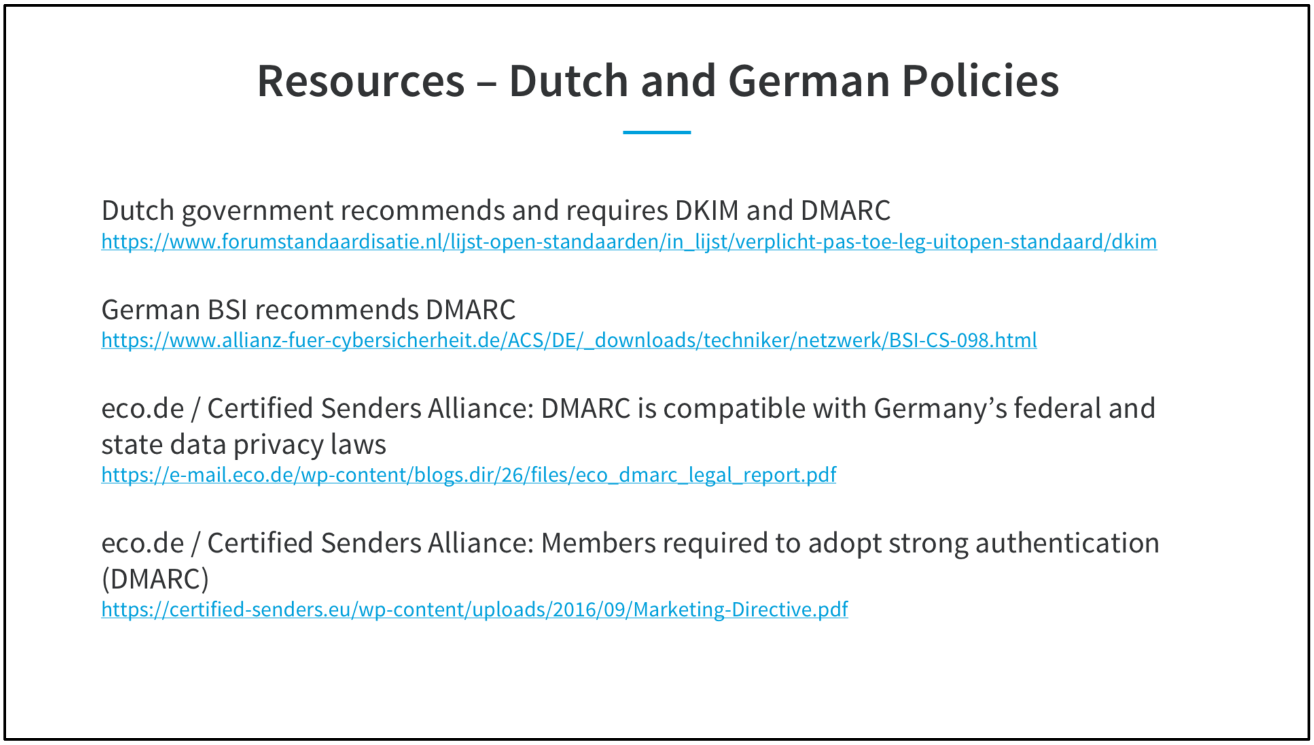
Resources – US Policies

October 2017: DHS Issues Binding Operational Directive 18 (BOD-18) re: DMARC, HTTPS
https://cyber.dhs.gov/
https://www.infosecurity-magazine.com/news/dhs-mandates-dmarc-https/

July 2017: US Senator Ron Wyden's Letter to DHS
https://www.wyden.senate.gov/download/letter-to-dhs-regarding-dmarc

March 2017: FTC - "Use Email Authentication"
https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication

April 2016: NIST Special Publication 800-177: Trustworthy Email
https://csrc.nist.gov/presentations/2016/nist-sp-800-177-trustworthy-email



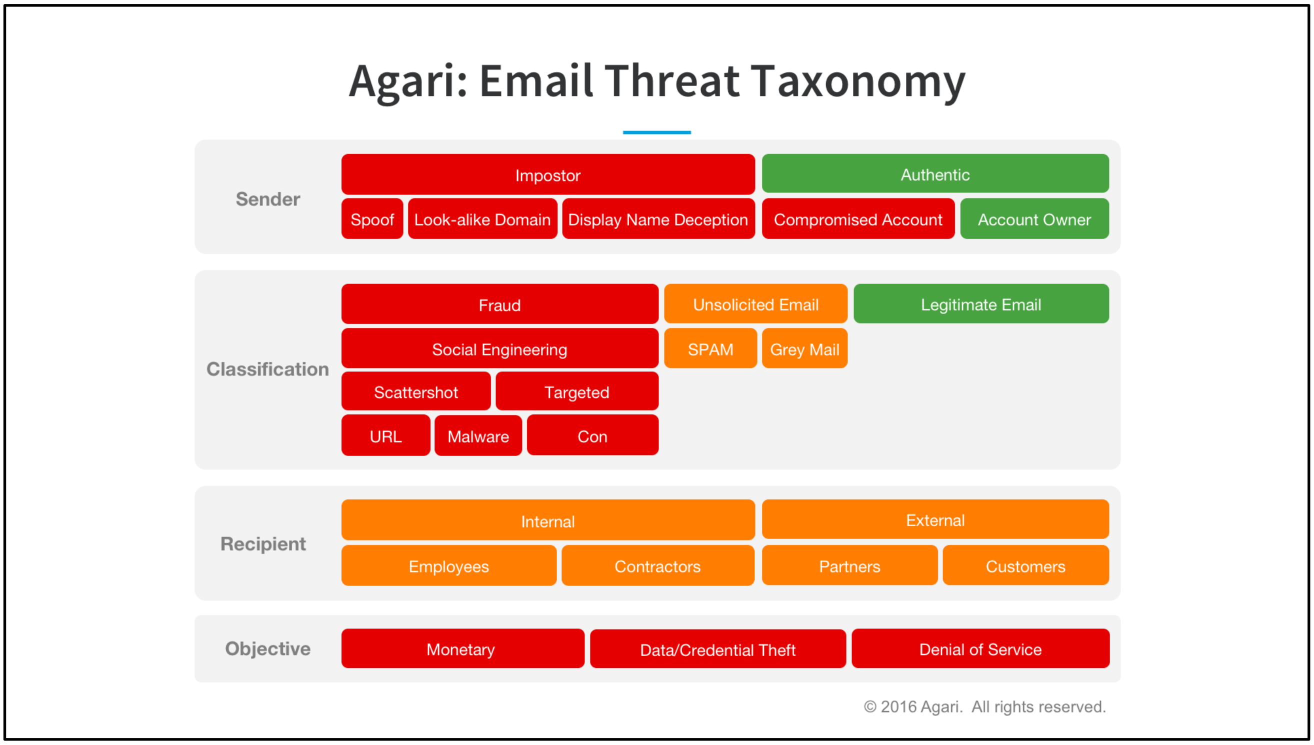
Resources – Dutch and German Policies

Dutch government recommends and requires DKIM and DMARC
https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uitopen-standaard/dkim

German BSI recommends DMARC
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-098.html

eco.de / Certified Senders Alliance: DMARC is compatible with Germany's federal and state data privacy laws
https://e-mail.eco.de/wp-content/blogs.dir/26/files/eco_dmarc_legal_report.pdf

eco.de / Certified Senders Alliance: Members required to adopt strong authentication (DMARC)
https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Directive.pdf



Agari: Email Threat Taxonomy

Sender

- Impostor
  - Spoof
  - Look-alike Domain
  - Display Name Deception
- Authentic
  - Compromised Account
  - Account Owner

Classification

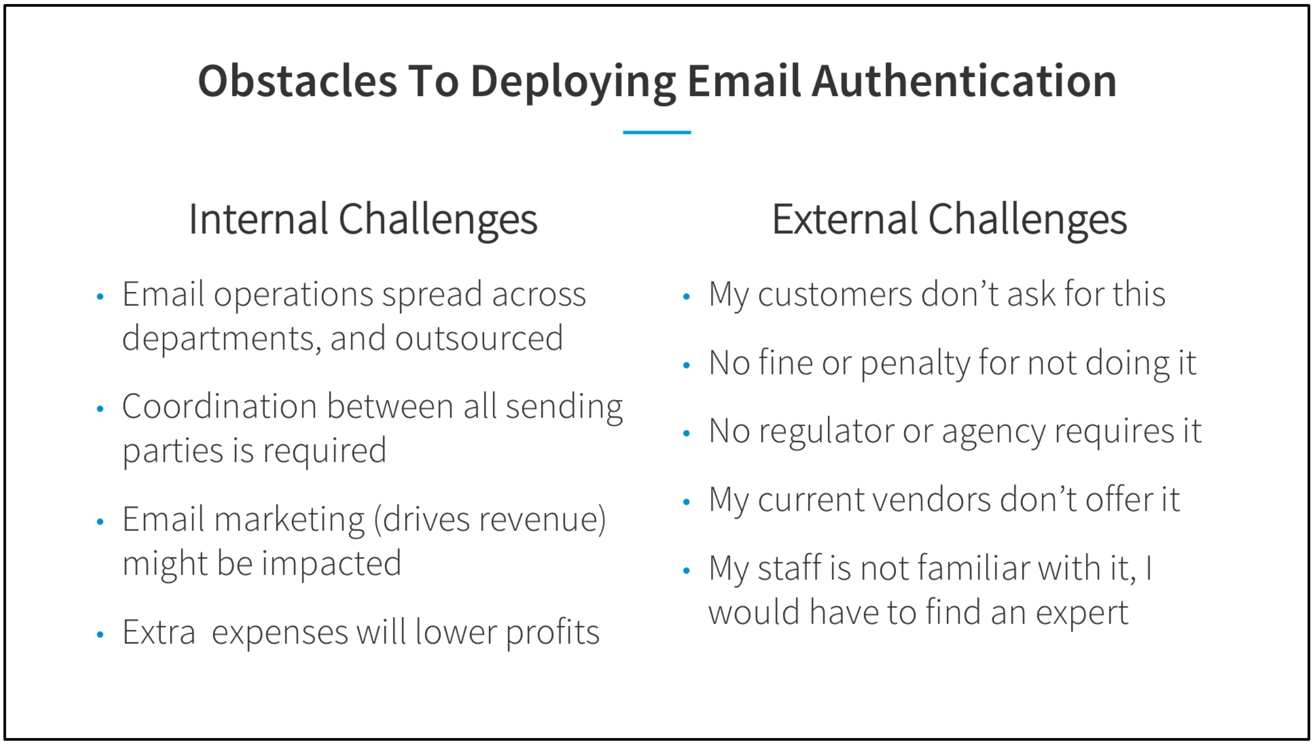
- Fraud
  - Social Engineering
    - Scattershot
    - Targeted
      - URL
      - Malware
      - Con
- Unsolicited Email
  - SPAM
  - Grey Mail
- Legitimate Email

Recipient

- Internal
  - Employees
  - Contractors
- External
  - Partners
  - Customers

Objective

- Monetary
- Data/Credential Theft
- Denial of Service



Obstacles To Deploying Email Authentication

Internal Challenges

- Email operations spread across departments, and outsourced
- Coordination between all sending parties is required
- Email marketing (drives revenue) might be impacted
- Extra expenses will lower profits

External Challenges

- My customers don’t ask for this
- No fine or penalty for not doing it
- No regulator or agency requires it
- My current vendors don’t offer it
- My staff is not familiar with it, I would have to find an expert