RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: **TECH-W03**

Curbing Email Threats & Spear Phishing – The Promise & Results with DMARC

MODERATOR:

Craig Spiezle
Executive Director & President
Online Trust Alliance
@otalliance

OTA Online Trust Alliance

PANELISTS:

Pat Peterson
Chief Executive Officer, Agari

AGARI

J. Trent Adams
Sr. Internet Security Advisor, PayPal

PayPal

John Scarrow
General Manager, Online Security Services
Microsoft Corporation

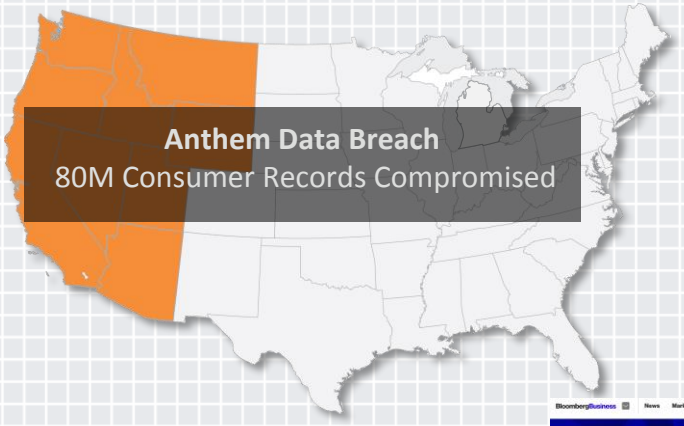
Microsoft

Overview

- **Problem & challenge – Email as a threat vector**
- **Email Authentication Overview – All Published RFC's**
  - **SPF** – *Authorizing the servers*
  - **DKIM** – *Authenticating the message*
  - **DMARC** – *Policy and Reporting*
- **Case Studies; Where Are we Today?**
- **Apply What You have Learned**

Problem

Attack Impact



Anthem Data Breach
80M Consumer Records Compromised

THE 1-2 PUNCH

18% success rate of phishing
14.5 Million Victims

25th February - ATTORNEY GENERALS ISSUES WARNING IN 10 STATES

400 Brands, 50% New Targeted by Malicious Email Every Quarter

What is DMARC?

- Domain-based Message Authentication, Reporting & Conformance”
- Specification to help reduce the potential for email-based abuse by solving a couple of long-standing operational, deployment, and reporting issues related to email authentication protocols.
- Standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms

Email Authentication Overview

SPF

- **Authenticates Message Path**
- Authorized senders in DNS

DKIM

- **Authenticates Message Content**
- Public encryption keys in DNS

DMARC

Consistency
A method to leverage the best of **SPF** and **DKIM**

Policy
Senders can declare how to process unauthenticated email

Visibility
Reports on how receivers process received email

Aggregated Insights
Telemetry into your mail streams (RUA)

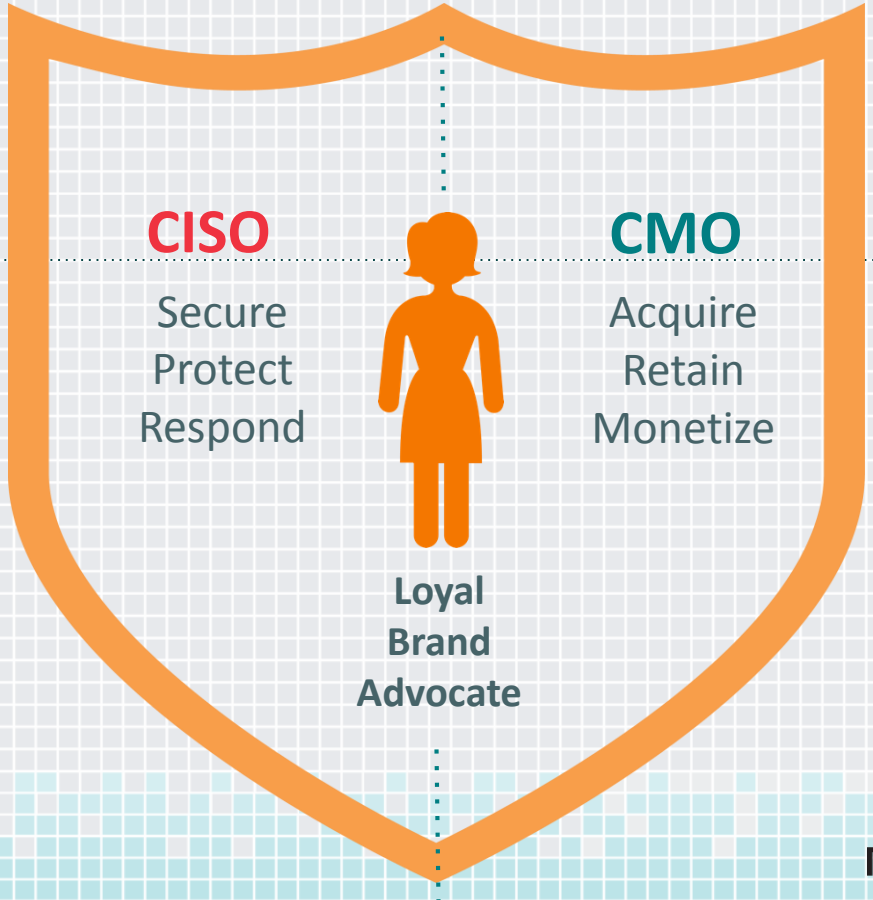
Failure & Spoofed email reports
(RUF)

DMARC – Who should care

83%

of CISO's that agree **brand protection** is their responsibility.

– CSO magazine's annual State of the CSO survey

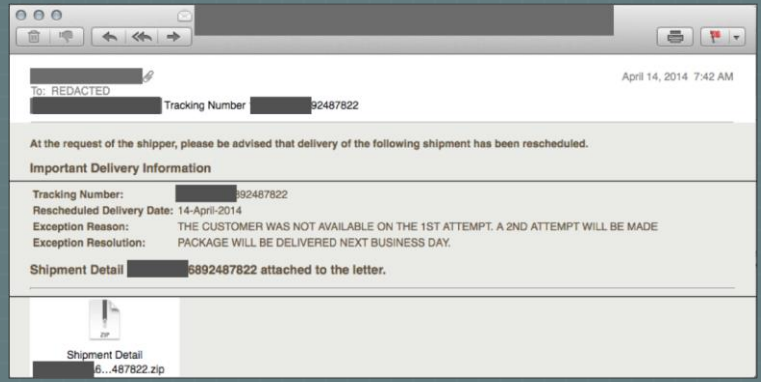


42%

of consumers less likely to do business with you following an email attack

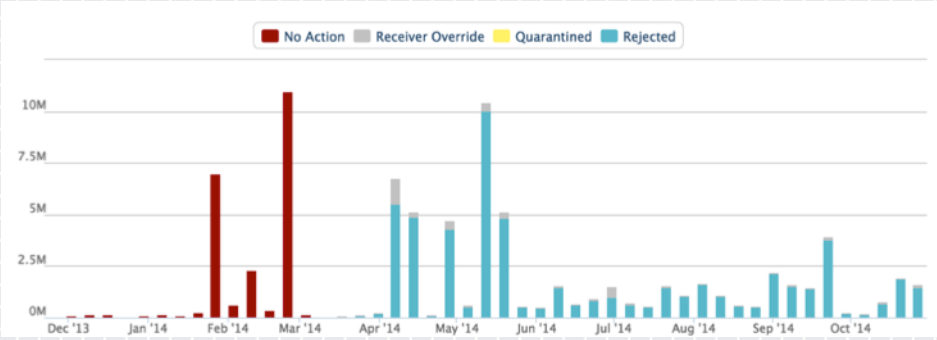
Cloudmark Study

DMARC – Solving the problem



Success criteria – reduce hijacked accounts

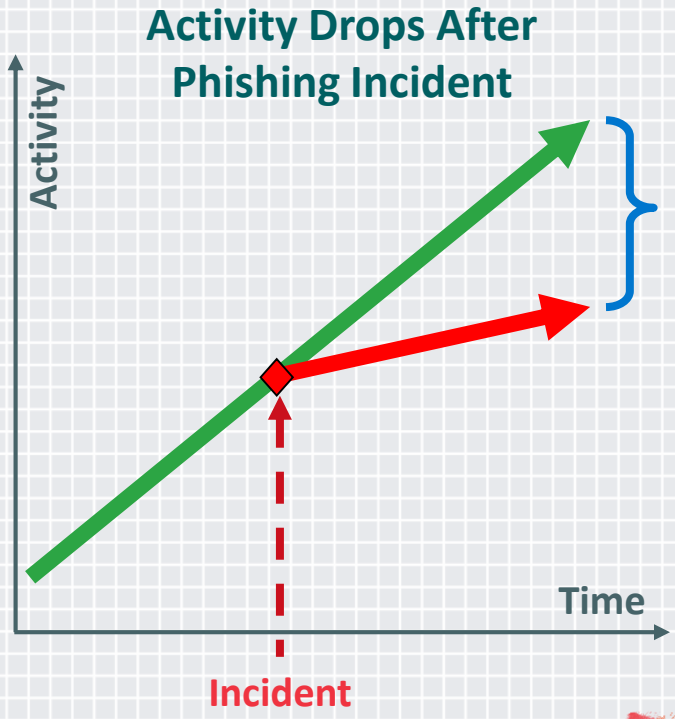
Reject policies on 35 active and 3000+ defensive domains



Rejected 30M emails within days – the majority of them having Cryptolocker

Case Study

- **These truths are self-evident:**
  - Email must be protected as a trusted channel of communication.
  - Email protection extends beyond our direct control.
  - No single solution to protect email.
  - Failing to protect email results in measurable losses.



Proof Points

- PayPal noticed **70% drop in reported phishing** within the US following the publication of the DMARC specification.[1]
- DMARC drove a **14% reduction in detected phishing** in 2014 vs. 2013 as measured against organizations within the Financial Sector.[2]
- DMARC effectively **protects ~80% of PayPal customers** from spoofed domain email.[3]

1. PayPal data for 2012 - 2014
2. Kaspersky Lab Report: http://bit.ly/Kaspersky-Financial_cyberthreats_2014
3. PayPal data as of March, 2015

Where Are We Today?

	2013		2014		2015	
	DMARC	R/Q	DMARC	R/Q	DMARC	R/Q
FDIC 100	13.0%	2.0%	21.0%	2.0%	24.0%	6.0%
IR 500	3.0%	0.1%	6.2%	2.0%	9.4%	2.4%
Federal 50	4.0%	0.0%	6.0%	0.0%	12.0%	2.0%
Social 50	22.0%	14.0%	36.0%	18.0%	46.0%	26.0%

Source: OTA Analysis as of April 9, 2015. IR 500 (Internet Retailer Top 500, Social (gaming, social, dating, storage and other top visited sites excluding content, banking and commerce) sites.
DNS validator tool https://otalliance.org/resources/spf-dmarc-record-validator
R/Q – Reject or quarantine policy
Lists updated as of April 9, 2015 based on current rankings. See https://otalliance.org/HonorRoll for details.

But DMARC Coverage Varies

- DMARC protection requires mailbox provider adoption to be effective.
- Coverage varies by region, driven by the top 5 regional mailbox providers.
  - US coverage is the strongest: **~85%**
  - Global average: **~63%**
  - Germany has the lowest: **~30%**

Apply What You Have Learned Today

- Within 1 week
  - Publish a DMARC “p=none” Policy (aka. “monitor only”)
- Within 30 days
  - Compete a audit of all domains
  - Evaluate Email Flows + Threats
  - Lock Down Defensive & Parked Domains
  - Pressure MTA / enterprise vendors to support email authentication
- Within 90 days
  - Implement SPF & DKIM on all domains and subdomains
  - SPF “-all” Record
  - Move to DMARC “p=reject” if / when necessary

Resources

- **Email Security & Integrity Resources**
  - https://otalliance.org/resources/email-security
  - https://otalliance.org/DMARC
- Agari http://agari.com/
- Online Trust Audit & Honor Roll https://otalliance.org/HonorRoll
- Symantec http://www.symantec.com/email-security-cloud/?fid=symantec-cloud