Are You Protecting Your Email & Your Customers?

Learnings from the 2017 OTA Trust Audit

August 1, 2017

Panel

Kevin Gallant
Manager, Intelligence Products, Yes Lifecycle Marketing

Peter Goldstein
CTO & Co-Founder, ValiMail

Mike Jones
Director, Product Management, Agari

Jeff Wilbur
Director, Online Trust Alliance, Internet Society
Why Care? The Risk.

- Rise in phishing attacks, precision, variety of methods
- Entry point for >90% of breaches

Why Care? The Value.

- Protect customers, partners & employees
- Insight into authentication, attacks
- Deliverability
Who Cares?

2016 – Who’s Doing It?
2017 – Who’s Doing It?

9th Annual Audit Overview

- Over 1,000 web sites
  - Internet Retailer Top 500
  - Bank 100 (previously FDIC 100)
  - Consumer Services 100
  - News/Media 100
  - Federal Gov’t 100
  - ISP/Carriers/Hosters 100
  - OTA Members

- Scoring
  - 100 baseline points for each category
  - Weighted composite analysis
  - Bonus points for emerging practices
  - Penalties for vulnerabilities, data loss incident & fines/settlements
  - Honor Roll = 80% or higher overall, no failure(s)
  - Failure for less than 60 points in each category
Causes of Failures

- Overlooking the basics & fundamentals
- 36% failed in one area, 11% failed in 2-3 areas

Consumer Protection – 2017

- Base points
  - Email authentication
    - SPF and DKIM at top-level and subdomains (↑ TLD weight)
    - DMARC record and policy
    - DMARC reject/quarantine
      - Increased weight for reject
    - Invalid SPF / DMARC & “naked” DMARC records not counted

- Bonus points
  - TLS for email
  - DNSSEC
  - IPv6
  - Multi-factor authentication

- Penalty points
  - Domain locking (not locked)

• Can the app or website be spoofed, fooling a person to open/download an update, open an attachment or simply open an email with a drive-by exploit?
• Does the site or app exercise best practice to help prevent brand-jacking and domain abuse?
Overall Adoption Trends

- General uptrend, especially DKIM and DMARC
- Dip in SPF-related adoption this year due to invalid records, shift in sector lists

Fighting Phishing

- SPF & DKIM allow recipient to verify sender
- Recommend implementation for inbound & outbound email
- All domains – top-level and subdomains
Fighting Phishing

• DMARC ensures “from” matches real sender, allows sender to get reports, tell receiver how to handle messages that fail authentication
• Use of “enforcement” (reject/quarantine policy) growing, but far from adequate

The “Trifecta” – Gaining Momentum

• Shows percent of organizations that support both SPF and DKIM at the TLD and have a DMARC record with a “reject” or “quarantine” policy
• Highlights need for increased focus across organizational “silos” to protect consumers, employees and brands
2017 – Who’s Doing It?

Audit Findings – Common Mistakes

- SPF (10% of records)
  - References to invalid, non-existent records
  - Multiple SPF records
  - Syntax errors
  - Use of ?all or +all
  - *Excessive lookups (8%)*

- DMARC (5% of records)
  - “Naked” records (p=none, no reporting)
  - Syntax errors
  - Send records to places not set up to receive

- Bottom line – check your records regularly!
- Utilize resources of OTA members
Notable Trends

- DMARC initially focused on consumer email, now available in many enterprise offerings, e.g. –
  - Google G Suite, Microsoft O365
  - Cisco/IronPort, Mimecast, Proofpoint
- ARC – new proposed standard to “connect the dots” for DKIM signing (mailing lists, etc.)
- Sender identification – ongoing developments to build on authentication

Justifying Internally

- Security
  - When door’s shut, bad guys go elsewhere
  - Protects users, and employees (when used inbound)
- Insight
  - Email governance (“shadow email”)
  - Attackers
- Deliverability
  - Helps receivers better assess real reputation
  - Improves overall reputation (bad guys stop, spoof messages don’t count)
What Now?

- Self-assessment – inventory, stakeholders, etc.
- Get help – OTA, industry resources
- Build a business case
- Implement and put processes in place

Tools & Resources

OTA
- Email Security  https://otalliance.org/eauth
- DMARC  https://otalliance.org/dmarc
- Resources  https://otalliance.org/eauth/resources
- TLS  https://otalliance.org/tls

OTA Members
- Agari  https://www.agari.com/resources/
- Dmarcian  https://dmarcian.com/
- Global Cyber Alliance  https://dmarc.globalcyberalliance.org/
- ValiMail  http://www.valimail.com/