Are You Protecting Your Email & Your Customers?

Learnings from the 2017 OTA Trust Audit

August 1, 2017

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

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

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Why Care? The Risk.

SC Media UK > News > APTs/cyber-espionage > Russia's 'Grizzly Steppe' kicked off with 'spear-phishing campaign' against DNC

by Teri Robinson

January 02, 2017

Russia's 'Grizzly Steppe' kicked off with 'spear-phishing campaign' against DNC

SC Media UK > News > Phishing > Plot twist: Phony Netflix membership emails turn out to be phishing scam

by Bradley Barth

January 11, 2017

Plot twist: Phony Netflix membership emails turn out to be phishing scam

SC Media US > News > Email security > Massive uptick in tax scam phishing emails, records cost $50 on the Dark Web

by Doug Olenick, Online Editor

April 05, 2017

Massive uptick in tax scam phishing emails, records cost $50 on the Dark Web

For everything there is a season and for tax scammers that time period are the months leading up to income tax filing day, April 18.

IBM's X-Force researchers noted in a report released today called Cybercrime Riding Tax Season Tides a 6,000 percent increase in the number of spam emails containing a specific form of tax form, such as W-2s, fraud between December 2016 and February 2017. At the same time the amount of spam that uses a generic tax

Tax data is one of the hottest sellers on the Dark Web.

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

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Why Care? The Value.

- Protect customers, partners & employees

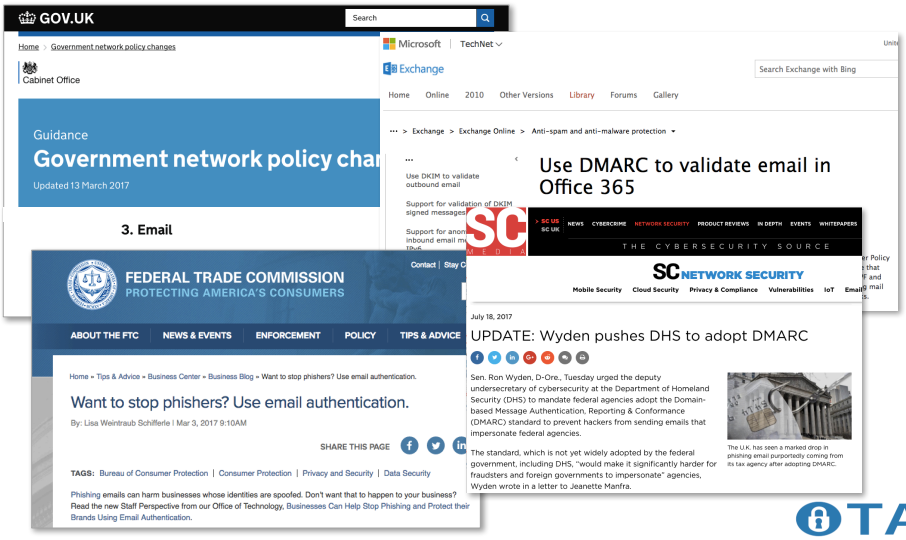
- Insight into authentication, attacks

- Deliverability

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Who Cares?



OTA Online Trust Alliance an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

2016 – Who's Doing It?

LEARN • INNOVATE • COLLABORATE

2017 – Who's Doing It?

1-800-PetMeds, amazon, American Greetings, Blue Apron, CustomInk, Etsy, BuildDirect, fitbit, GAP, Google Play, GROUPON, iHerb, kate spade NEW YORK, LifeWay, newegg, NordicTrack, REALTRUCK, REVOLVE, SIERRA TRADING POST, STAPLES, SwimOutlet.com, The RealReal, Walmart, WARBY PARKER

Bank of America, CHASE, citi, First Citizens Bank, Huntington, First Republic Bank, KeyBank, usbank, WELLS FARGO

CONSUMER INFORMATION: FDIC, HealthCare.gov, National Do Not Call Registry, USPS.COM, USPS.COM Store, USPS.COM Tools

airbnb, Aol., badoo, box, Booking.com, classmates, Dropbox, eHarmony, flickr, Google Play, glassdoor, IDENTITY GUARD, indeed, Instagram, LifeLock, LinkedIn, Pinterest, pch.com PUBLISHERS CLEARING HOUSE, reddit, Spotify, TaxSlayer, UBER, Upwork, YAHOO!, YouTube, WordPress

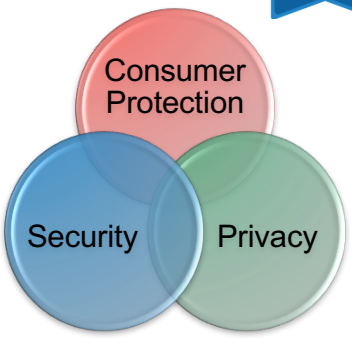
Akamai, Aol Mail., DigitalOcean, Google Sites, Microsoft Azure, ProtonMail, SQUARESPACE, verizon, verizon Wireless, YAHOO! MAIL

Aol. On NEWS, CNN, FT FINANCIAL TIMES, Mashable, TMZ, Mirror, VICE, BuzzFeed, Google News, reddit, YAHOO! NEWS

9th Annual Audit Overview

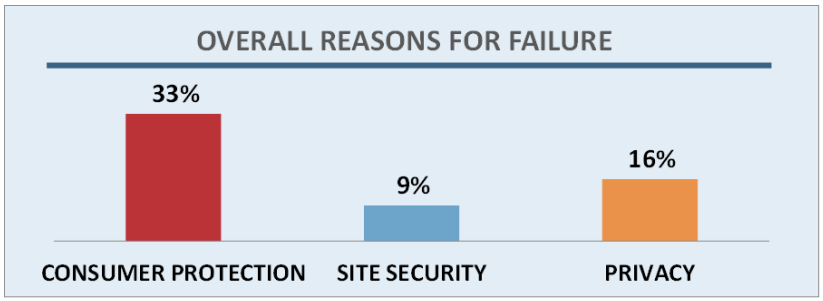
OTA Online Trust Alliance an Internet Society initiative ONLINE TRUST HONOR ROLL 2017

- **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



OTA Online Trust Alliance an Internet Society initiative

Causes of Failures



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

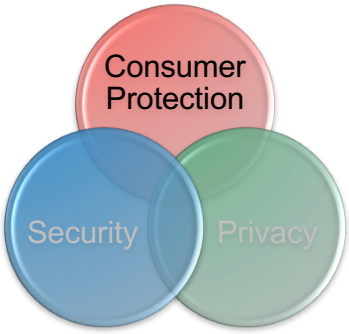
Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Consumer Protection – 2017

Italics = new for 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)

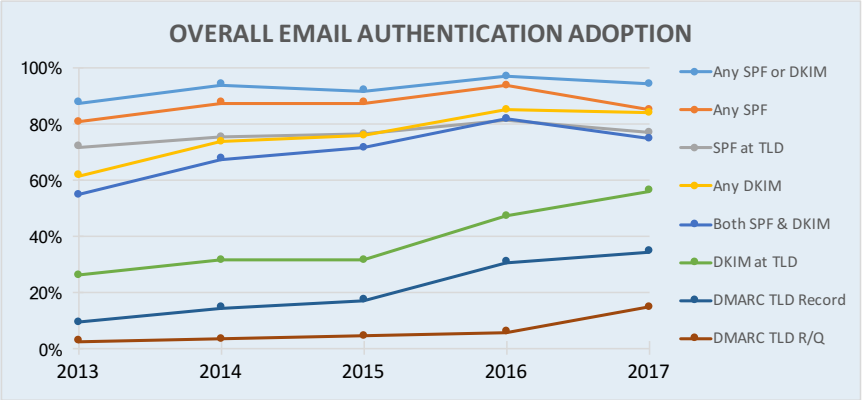


- Can the app or website be spoofed, fooling a person to open/download an update, open an attachment or simply open an email with a drive-by exploit?
- Does the site or app exercise best practice to help prevent brand-jacking and domain abuse?

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Overall Adoption Trends

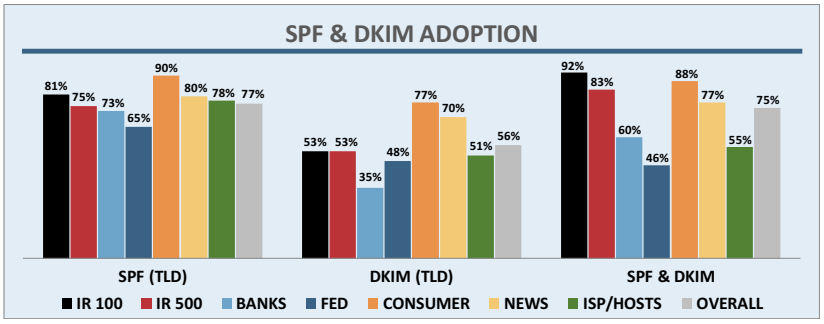


- General uptrend, especially DKIM and DMARC
- Dip in SPF-related adoption this year due to invalid records, shift in sector lists

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Fighting Phishing

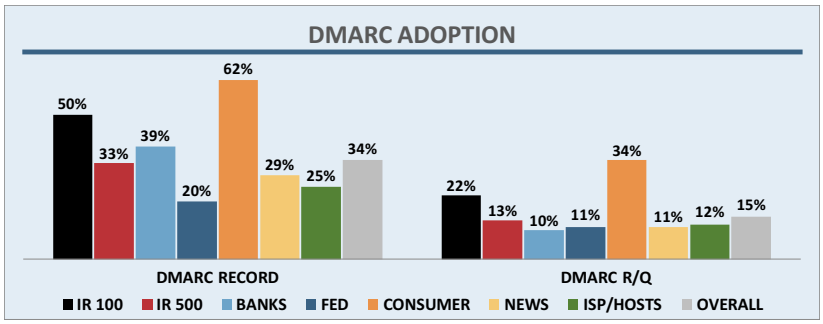


- SPF & DKIM allow recipient to verify sender
- Recommend implementation for inbound & outbound email
- All domains – top-level and subdomains

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

Fighting Phishing

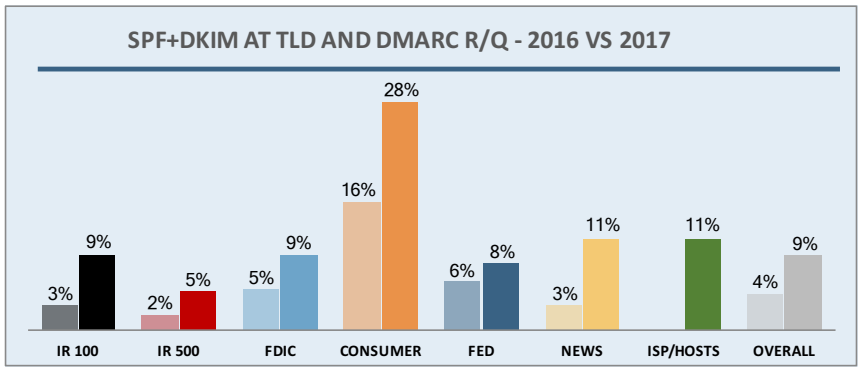


- DMARC ensures "from" matches real sender, allows sender to get reports, tell receiver how to handle messages that fail authentication
- Use of "enforcement" (reject/quarantine policy) growing, but far from adequate

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

The "Trifecta" – Gaining Momentum



- Shows percent of organizations that support <u>both</u> SPF and DKIM at the TLD <u>and</u> have a DMARC record with a "reject" or "quarantine" policy
- Highlights need for increased focus across organizational "silos" to protect consumers, employees and brands

Online Trust Alliance
an Internet Society initiative

LEARN • INNOVATE • COLLABORATE

2017 – Who's Doing It?

LEARN • INNOVATE • COLLABORATE

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

OTA Online Trust Alliance an Internet Society initiative

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/