A Vision for Trusted Email

Online Trust Alliance

Since the introduction of email over 45 years ago, email has become ubiquitous for individuals, businesses and governments worldwide. The total number of worldwide email accounts is expected to exceed 4.9 billion by the end of 2017. Highly scalable and resilient, email offers significant value which the economy and society increasingly rely on. For businesses, email marketing is an affordable and effective way to reach customers, maintain loyalty, inspire purchases and establish positive consumer brand perception. Unfortunately, these same attributes have been exploited by cybercriminals and deceptive businesses as the "tactic of choice."

Email is the tactic of choice for cybercriminals. Its resiliency and ability to deceive users make it a security "blind spot."

While growth of the email channel is encouraging, many consumers are facing email fatigue – finding email not relevant, being overwhelmed by spam and most troubling, facing increasing levels of malicious email. Fraudulent and phishing emails are increasingly difficult to distinguish from legitimate emails, reflecting criminals' increased skills and ability to mimic an organization's brand, tone and infrastructure. Spammers and deceptive businesses have "enjoyed" these same capabilities, using confusing email subject lines in attempt to defraud consumers into buying bogus products and services. Aggressive marketers have embraced the "free" cost of sending email, at times overwhelming inboxes. Combined with lack of discoverable or functional unsubscribe mechanisms, trust of email is at an all-time low and the clear and present threat is growing every day.[1]

Stolen credentials and account takeovers have become a dominant goal of these crime based email campaigns. Malicious email typically starts with spear phishing, which opens the door for crimes ranging from theft of credentials to distribution of ransomware to Business Email Compromise (BEC) attacks. Compromised credentials, when combined with further code exploits, can lead to theft of intellectual property, funds and employee records, and even takeover of critical infrastructure and physical systems. According to the FBI, losses from BEC increased 1300% in 2016 with total losses exceeding $3.1 billion.[2] Ransomware infections targeting businesses averaged 35,000 per month with payments exceeding one billion dollars. [3] [4] Combined more than 82,000 cyber incidents occurred in 2016, compromising over 4.2 billion records.[5] [6]

Leveraging the growth of connected devices (Internet of Things), criminals have recognized another green pasture. As the popularity of IoT devices grows in the home and office, so does the attractiveness to use these devices to drive further exploits. As demonstrated by the recent "Mirai" botnet-based DDoS attack and phishing emails targeting users and their devices, criminals have discovered another avenue for harm.[7]

Though at first glance email may seem unrelated to the development and maintenance of an IoT device's security over its lifespan, we have already seen attempts to use spoofed email as a starting point to infect or control IoT devices. For example, fake security notifications are used to gain access and force unauthorized password resets, and IoT devices have been hijacked to be part of a bot network as a result of users downloading malicious updates. These attacks can lead to compromise of users' privacy, physical infrastructure (e.g., door locks, garage doors) and broad attacks on network-connected infrastructure (e.g., power grids, water supplies). Due to these increasing risks, manufacturers of IoT devices should be more vigilant than ever to protect their email from abuse.

While organizations continue to invest heavily in security defenses, email has become a "blind spot" for many organizations' security portfolio. Using cleverly crafted social engineering and spoofed emails, criminals are increasingly successful in getting recipients to open malicious emails, click on links or attachments and accept downloads. By gleaning data from social networks and company web sites, criminals trick employees into replying to or acting on what appears to be a legitimate personalized email. Unknowingly they provide logon credentials and passwords, authorize bank transfers and transfer data to senders masquerading as business partners or the employee's own executives.

SOLVING THE PROBLEM

Since 2003 the email industry has recognized the problem of deceptive emails and spam which overwhelm ISPs and users' inboxes. Through the standards process and leadership of many organizations including AOL, Cisco, Microsoft and Yahoo, two critical and complementary standards evolved in late 2006, gaining broad support as best practices to give ISPs and receiving networks the ability to distinguish legitimate email being sent by or on behalf of legitimate senders. Known as email authentication, these standards include Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). These standards allow receivers to verify whether a message is truly sent by the purported sender. Today is it estimated that more than 90% of consumer email sent daily utilizes one or both of these protocols, which are supported by all major ISPs and mailbox providers including Comcast, Gmail, Microsoft and Yahoo.

Building on the foundation of email authentication, the industry recognized that additional functionality was required to further improve the processing and handling of email. In 2007 an expanded working group including AOL, Cisco, Google, IronPort, Microsoft PayPal, Yahoo, and others began to address the short-coming of email authentication. This effort set the foundation for the development of "Domain-based Message Authentication, Reporting & Conformance" (DMARC)" and the release of the draft specification in January 2012.[8]

DMARC is helping to stem email abuse and distribution of malware. Organizations who fail to adopt place users in harm's way.

Today, as a draft open standard, DMARC is helping to protect hundreds of millions of users' inboxes from the escalating levels of malicious emails. DMARC is designed to complement an organization's existing email and anti-spam technologies. DMARC builds on the widely deployed SPF and DKIM protocols, providing significant additional benefits. The first benefit is a reporting function that allows senders to see how their email authentication is “seen” by receivers. This telemetry allows domain holders to manage their outbound email and provides notices on unauthenticated or forged email purporting to be coming from their domain. The second major benefit is that DMARC provides domain owners the ability to publish a “policy” in their public DNS specifying how receivers should process and handle unauthenticated messages.

Such polices are typically set to “p=none” during an initial monitoring period of 60-90 days. Once all outbound mail streams are correctly authenticated, an organization’s DMARC policy should be revised to “reject” or “quarantine,” protecting users and their brands from abuse. Leaving a policy set to “none” provides no brand or consumer protection value and should be changed as soon as an organization has fully reviewed data generated through their DMARC reports.

Through this email authentication cocktail (SPF, DKIM and DMARC), organizations have easy access to effective, open standards that can enhance trust and integrity of email. The combined business and technical value is clear and conclusive. Organizations which thoroughly implement SPF and DKIM across all domains and utilize DMARC with a “reject” policy protect both their organization and their customers from abuse.

BEST PRACTICES TO ENHANCE EMAIL SECURITY

1. Assess where you are today. Build an inventory of all your email systems and determine the level of email authentication (SPF, DKIM and DMARC) in use. As businesses increasingly rely on cloud providers for key functions it is critical to assess their support as well.[9]
2. DMARC reports can provide significant telemetry and insights into your outbound mailing activities. It is recommended that you start with DMARC in “monitor” mode (p=none) which allows you to receive reports and refine your authentication practices. There are dozens of free tools offered by leading companies (e.g., Agari, Dmarcian, and ValiMail) as well as organizations and working groups including DMARC.org, Global Cyber Alliance, MAAWG, OTA and others.
3. Engage your security, operations and marketing teams to explain the importance of email authentication in the context of overall security and to encourage them to implement inbound authentication checking to protect the organization from spoofed email.
4. Continually monitor your DMARC reports. They provide great insights and telemetry into your outbound mail streams. Utilize this data to optimize your SPF records and DKIM signing. Consider use of service providers to monitor and manage outbound authentication, update DNS records and rotate keys as required.
5. Reach out to your vendors and business partners; require that they authenticate all email sent to you and request they implement a DMARC reject or quarantine policy as soon as possible to help protect your employees from harm. As practical, consider this as a contractual requirement not unlike notification for breaches or data loss incidents of your company data.[10]

> *“Email is a vibrant and effective mechanism to drive results, but users need to have confidence that their email is from a legitimate sender.”*

6. Implement inbound authentication checks to help protect your employees and infrastructure from receiving malicious email.
7. Secure security bulletins and customer advisories. As outlined in the IoT Trust Framework, email authentication is a required baseline security element for all IoT device manufacturers, including the connected home, office and wearables.[11]

ADDITIONAL STEPS TO ENHANCE TRUSTWORTHY EMAIL

1. Review unsubscribe processes to maximize discoverability and functionality. Confirm that your email: a) contains clear and conspicuous links, b) uses commonly understood terms and c) utilizes a design that maximizes readability in font, color and size.
2. Maximize user expectations and relevancy through the use of consumer controls and email preference centers.
3. Review privacy and newsletter subscription policies, maximize transparency limiting data use and sharing with third parties.

ABOUT OTA

The Online Trust Alliance (OTA) is a charitable non-profit think-tank with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. OTA's goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning the public policy, technology, ecommerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors. https://otalliance.org

[1] 2016 Unsubscribe Audit https://otalliance.org/Unsubscribe

[2] FBI BEC data https://www.ic3.gov/media/2016/160614.aspx

[3] Symantec 2016 Ransomware Report http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

[4] NBC News Ransomware Growth http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[5] 2016 Cyber Incident & Breach Readiness Planning Guide, page 6 https://otalliance.org/Incident

[6] Risk Based Security https://pages.riskbasedsecurity.com/2016-ye-breach-quickview

[7] IoT DDOS Attack https://www.infosecurity-magazine.com/news/iot-ddos-attack-warning-as-mirai/

[8] DMARC Overview & Resources https://otalliance.org/DMARC

[9] Email Authentication https://otalliance.org/Eauth

[10] 2016 Cyber Incident & Breach Response Guide

[11] IoT Trust Framework including a set of security and privacy enhancing principles, https://otalliance.org/IoT