Email Security Conference 2017
JP Tower Hall & Conference, Tokyo, Japan

なぜいまだにスパムやフィッシングに悩まされるのか？
Why Is There Still So Much Spam and Phishing?

Steven M Jones
Senior Systems Engineer, LinkedIn
Executive Director, DMARC.org

Topics

- Introduction
- Evolution of spam and phishing
- Spam, phishing, and email authentication
- Recent developments in email authentication

How spam got started

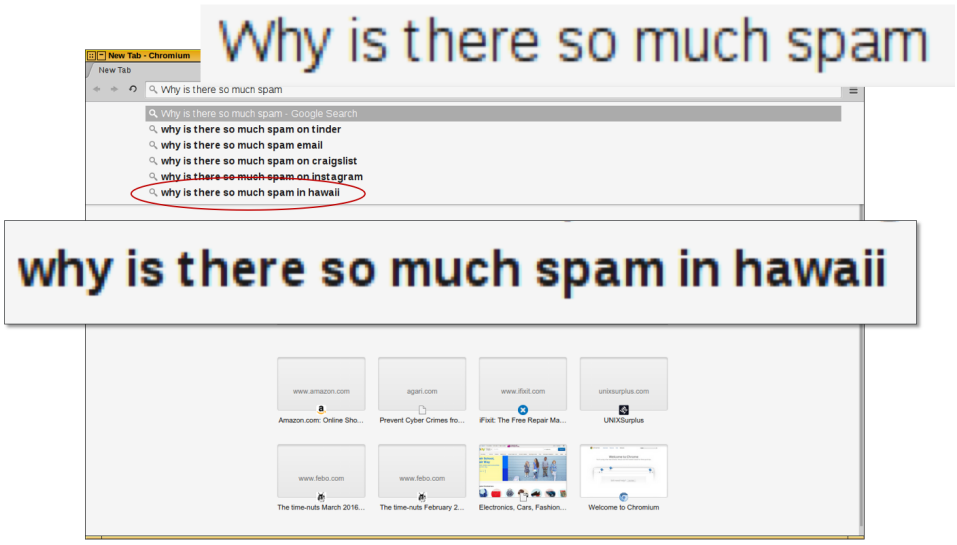
How it went to professional criminals

Why spam won’t stop (it isn’t just spam)

Email auth and messaging

Recent developments

2017: Google Knows Everything



Japanese-Hawai’ian Cuisine

スパムむすび
Spam musubi

First Modern Commercial Spam?

```
Path: panix!udel!news.sprintlink.net!indirect.com!
From: ni...@indirect.com (Laurence Canter)
Newsgroups: sci.op-research
Subject: Green Card Lottery- Final One?
Date: 12 Apr 1994 08:10:35 GMT
Organization: Canter & Siegel

Freen Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal
program giving away a certain annual allotment
of Green Cards to persons born in certain
countries. The lottery program was scheduled
to continue on a permanent basis. However,
recently, Senator Alan J Simpson introduced a
bill into the U. S. Congress which would end
any future lotteries. THE 1994 LOTTERY IS
SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE
THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY
FOR FIRST TIME.
```

Fundamentals of Spam

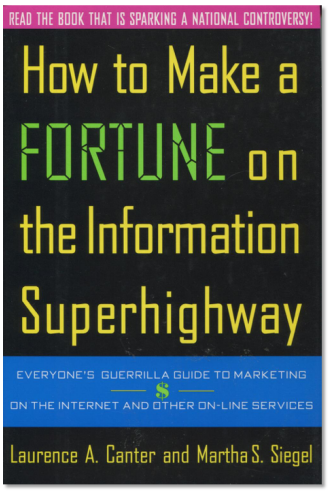
- Low cost to send messages
- Ease of impersonation
- Difficult to block
- Low risk
- Generates reliable revenue

Evolution of Spamming

First Wave of Spam - 1990s

Easy To Get Started

- Spammers are amateurs teaching others
- Limited by Internet connectivity (dialup era)
- Email and USENET servers unprotected
- Many people bought from spam messages
  - Gambling, pharmacy, pornography
  - "Fake news" stock trading schemes
- High returns: 2.4% of users bought from spam



Canter & Siegel

1996: 22%, 50 Bn messages; 1999: 18%, 290 Bn; 2002: 27%, 1.5 Tn
Source: Computerworld, Nov 11, 2002; page 33;
https://books.google.com/books?id=3dKY-OZNNuYC&printsec=frontcover#v=onepage&q=As%20unwanted%20e-mail&f=false

Spam study: https://web.archive.org/web/20000815224755/http://www.chooseyourmail.com:80/INTRO.HTML

Start of the Second Wave

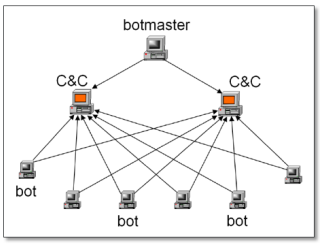
Internet Bubble Bursts - 2000

- More of the world on the Internet
- Internet an excellent carrier for viruses
- Programmers, marketers lose jobs
- Datacenters lose tenants
- Backbone carriers lose customers
- But under 200 people account for most spamming activity into the early 2000s

Graph source: http://theforecaster-interactive.com/wp-content/uploads/2015/06/infographic_english2_nasdaq_composite-1280x720.png

Spam Wars: https://www.technologyreview.com/s/401981/spam-wars/

Second Wave of Spam - 2000s



Growth and Innovation

- "Bulletproof" hosting (McColo, etc)
- Criminals begin moving into spam, e-crime
- Virus writers and spammers unite
- Creation of botnets using infected PCs
- Business users become targets
- 100 Billion spam messages each day
- Growth: 40 – 60 – 80+% of all Internet email

Source, crimeware image: www.javiermarques.es
Source, botnet image: https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html/
Botnets: https://www.informationweek.com/beware-the-bots/d/d-id/1047696
$7,000 per day: https://www.sitepoint.com/spam-roi-profit-on-1-in-125m-response-rate/
$700,000 per year: https://admin.fee.org/files/doclib/westley1103.pdf

Training Users To Be Phished - 2000s

Vendors And Outsourcing

- Marketing, Sales teams hire contractors
- Vendors sending email as the Enterprise - poorly
  - Spoofed sending address
  - Linking to company logo images
  - No knowledge of SPF, DKIM
- 2005: 10,000 New York State employees phished
  - 15% entered personal information
  - 8% did it two months later in second test

NYState study: https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/IEEESecurityPrivacy-SpearPhishing-Jan-Feb2014.pdf

Second Wave of Spam - Fighting Back

McColo Datacenter Shutdown

- Reduced global spam volumes by 70-75%

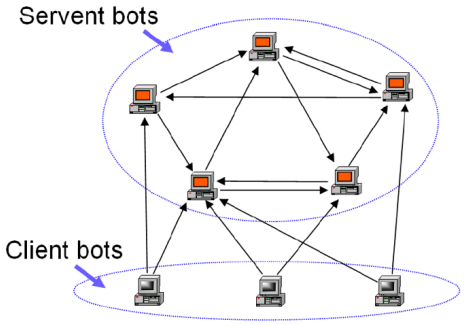
  … for about 4 months
- Criminals suffered financially
- Several botnets disappear, others crippled
- Shows effectiveness of attacking Command & Control (C&C) servers

https://www.cnet.com/news/postini-googles-take-on-e-mail-security/
http://www.slate.com/articles/technology/future_tense/2014/11/spam_nation_meet_the_russian_cybercrooks_behind_the_digital_threats_in_your.html
https://www.networkworld.com/article/2273143/network-security/after-mccolo-takedown--spam-surges-again.html

Third Wave of Spam - 2010s

Resilience

- Shutting down datacenters forced evolution
- Lessons learned from peer-to-peer networking
- Online operations now distributed
- Criminals also located around the world
- All critical functions redundant
- Encryption of control channels and files



Advanced Hybrid
Peer-to-Peer Botnet

Source: https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html/

Third Wave of Spam - 2010s

Diversification

- Many uses for compromised PCs
  - Address book / social network harvesting
  - Credential theft (banking, employer, cloud)
  - Scanning email and documents
  - Cryptocurrency mining
  - Ransomware
  - Distributed Denial of Service (DDoS) attacks
  - Sending more spam/phishing messages

The User Problem Continues

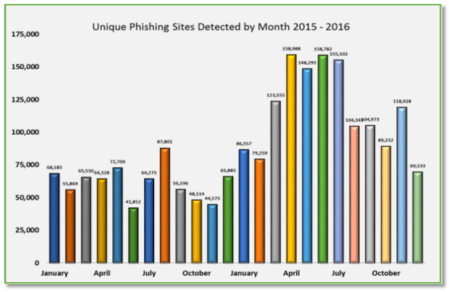
2013 Study: Can Users Detect Phishing?

- 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/

Crime Pays Very Well

Phishing, Data Breach, Ransomware



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

2015: 740 MM records disclosed in data breaches
$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
$5,000 MM damage from ransomware

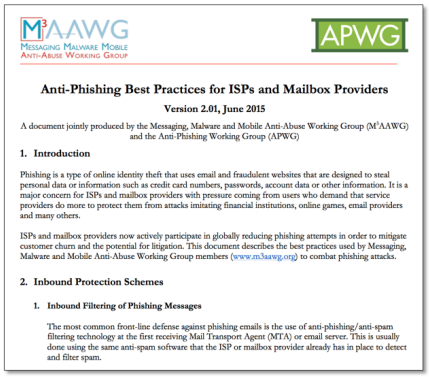
2017: Global cost of phishing $9 Billion (predicted)

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/

Companies Still Acting Like Phishers

How many follow best practices?

- All email using consistent Internet 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.”



M³AAWG
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 (M³AAWG) 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

Spam and Email Authentication

Spam And Email Authentication

Impersonation is a foundational technique of spammers

- First Wave: Avoid bounces and user complaints
- Second Wave: Help avoid filters, fingerprinting
- Third Wave: Leverage trust and reputation

Email authentication designed to combat spammers.

- Make it difficult to impersonate senders
- Easier to detect and block spammers

Email Authentication

Timeline for Key Protocols

More information about email authentication:

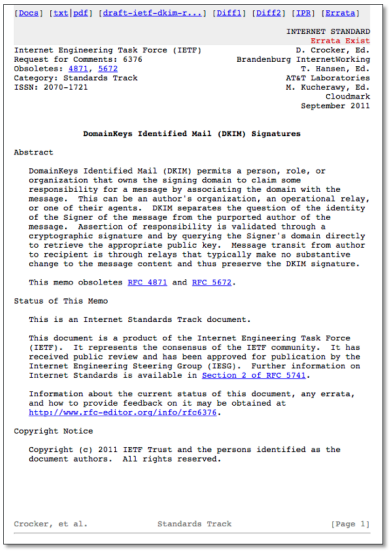
- https://www.iajapan.org
- https://dmarc.org
- https://openspf.org
- http://dkim.org

2002-2004: Sender Policy Framework (SPF)

2004-2007: Domain Keys Identified Message (DKIM)

2009-2012: Domain-based Message Authentication, Reporting and Conformance (DMARC)

Progress and Limitations



[Docs] [txt|pdf] [draft-ietf-dkim-r...] [Diff1] [Diff2] [IPR] [Errata]

INTERNET STANDARD
Errata Exist

Internet Engineering Task Force (IETF) — D. Crocker, Ed.
Request for Comments: 6376 — Brandenburg InternetWorking
Obsoletes: 4871, 5672 — T. Hansen, Ed.
Category: Standards Track — AT&T Laboratories
ISSN: 2070-1721 — M. Kucherawy, Ed.
Cloudmark
September 2011

DomainKeys Identified Mail (DKIM) Signatures

Abstract

DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. This can be an author's organization, an operational relay, or one of their agents. DKIM separates the question of the identity of the Signer of the message from the purported author of the message. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature.

This memo obsoletes RFC 4871 and RFC 5672.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6376.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

Crocker, et al. — Standards Track — [Page 1]

SPF: Combat "backscatter" from spamming

- Left header `From:` unprotected
- Easily misconfigured, rarely enforced

DKIM: Protect header `From:`, message replay

- No accepted policy mechanism
- Third-party signatures problematic

DMARC: Has policy mechanism, enforced at ISP

- Cousin domains and "display name" attacks
- Problems with mailing lists, forwarding

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

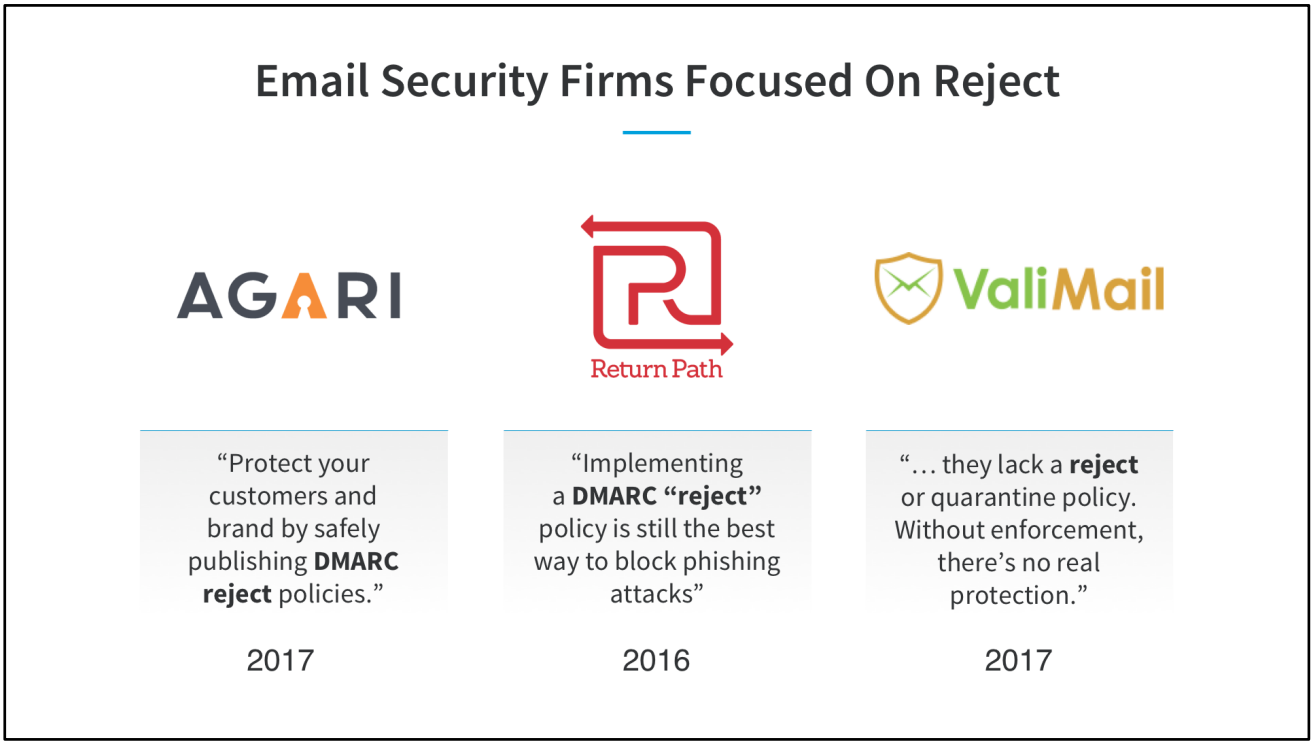
External Challenges

- 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

Recent Developments in Email Authentication

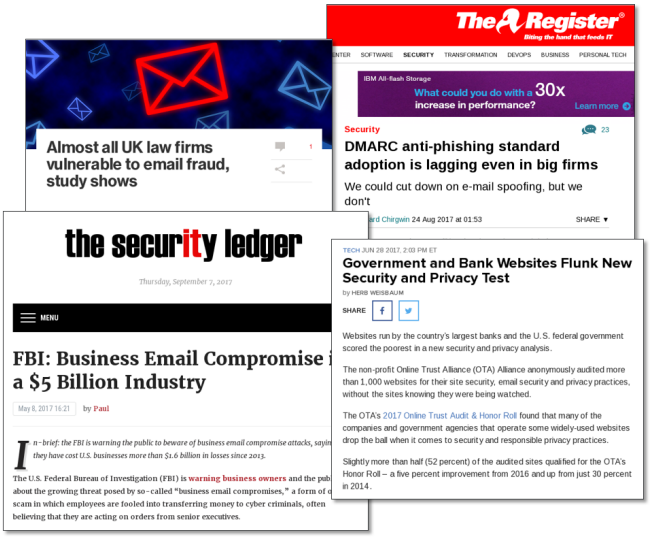
Annual Email Security Reports

- Annual reports have tracked growth of spam & phishing for many years
- Industry analysts (Gartner) added email authentication to their buying guides
- Growth of DMARC 2012 - 2015
- Recent reports focus on slow adoption of DMARC “reject” policies



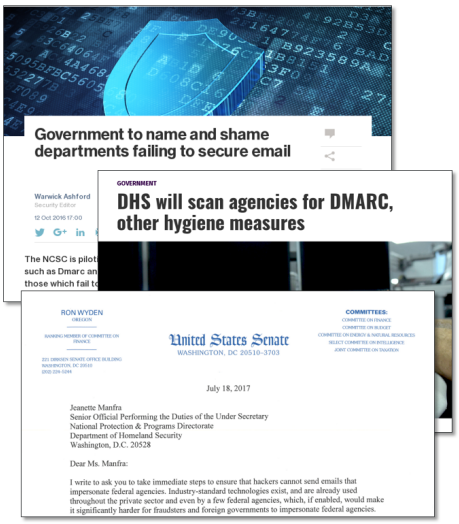
Agari: https://www.agari.com/customer-protect/ on 2017/09/06
ReturnPath: https://blog.returnpath.com/return-path-launches-beta-new-email-threat-intelligence/ as of 2016/07/07
Valimail: https://blog.valimail.com/senator-why-are-fed-agencies-so-vulnerable-to-email-fraud published 2017/07/18

News Articles Published More Frequently



- Crime is accelerating, leading news
- Email is frequently the vector for these attacks
- Industry and press push for solutions, now asking why DMARC isn't being used more widely
- Increase in data breach, and press focus on it, will change focus of all companies

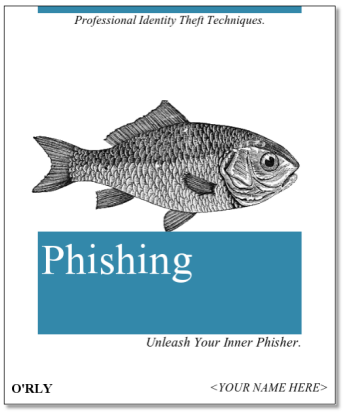
Government Views Evolving



- 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
- US DHS announces DMARC initiative

What Happens Next?

Predictions



More Email Authentication

- Phishing will continue to grow, spam may decline
- More governments will recommend/require DMARC
- ARC protocol will help address limitations of DMARC
  - ARC implementations arrive in 2017 Q4
- Global ISPs resume motion toward “No Auth, No Entry”
- More visual indicators of authentication for end users
- DMARC adoption up 75% through 2017, 100% in 2018

Q & A

ありがとうございました

Thank you

Speaker

http://linkedin.com/in/stevenmjones

- Joined LinkedIn Postmaster Team in 2017
- Executive Director of DMARC.org since 2015
- 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

Don’t repeat slide. Only thing to say: “LinkedIn and BofA were both part of the original DMARC project. And 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”

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

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/