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
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

Why is there so much spam

why is there so much spam in hawaii
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

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:
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:
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/
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

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

Crime Pays Very Well

Phishing, Data Breach, Ransomware

2013 phishing figure: https://www.phishingusertraining.com/the-cost-of-phishing/

2015-2016 data breach:


APWG 2016Q1 report:


Ransomware damage costs:
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.”

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

**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
Email Security Firms Focused On Reject

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
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
ありがとうございます
Thank you
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

eco.de / Certified Senders Alliance: DMARC is compatible with Germany’s federal and state data privacy laws

eco.de / Certified Senders Alliance: Members required to adopt strong authentication (DMARC)
Resources – UK Policies

November 2016: £1.9 billion national cyber security strategy

October 2016: National Cyber Security Centre plans to create dashboard showing government department adoption of DMARC

September 2016: NCSC Chief outlines new, active approach

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/