Observations on Phishing and DMARC

Steven M Jones
Senior Systems Engineer, LinkedIn
Executive Director, DMARC.org
A disturbing observation about company email and phishing
An update on DMARC and email authentication

A few words about DMARC.org, LinkedIn, and Japan
“LinkedIn and Microsoft were both part of the original DMARC project. 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”
Phishing And How Companies “Train” Employees
Companies Hiring Vendors to Phish Employees

Companies developed policies to protect email sent to their customers.

But companies have not done this with communications to their employees.

In the United States employee retirement savings, health insurance, paychecks, and many other services are “outsourced” to other companies.

These companies communicate directly with company employees.

The email communications these companies send do not meet the standards developed for consumer communications – no SPF, no DKIM, no DMARC.

So companies have essentially hired companies to phish their employees, and contradict their anti-phishing training, telling them to trust these messages.
Dr. Markus Jacobsson of Agari has developed this taxonomy to describe all the ways malicious email is constructed. This is a very useful model, but it leaves out the threat of legitimate messages sent from a vendor that confuse employees – and contradict their anti-phishing training – by looking like phishing messages.
In mid-2000s we would routinely discover new outsourced projects when the in-house contact complained that their vendor’s messages were being blocked by anti-spam filters.
Phishing Resistant To Training

Study of New York State Employees

- 2005: 10,000 New York State employees phished
  - 15% entered personal information
  - Received some training
  - Two months later, 8% did it again

2005-2010: Phishing was usually motivated by financial gain, not stealing corporate information

2011 Cisco study: “Spear” phishing 10x more profitable than non-targeted phishing

NYState study:
* Cisco phishing story from 2005
Cisco spear phishing study:
https://www.darkreading.com/mobile/targeted-attacks-10-times-more-profitable-than-mass-campaigns/d/d-id/1135960
Phishing Still Resistant To Training

8 Years of Training – Did It Help?

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.
Why Is Phishing So Successful

- Some aspects are due to human nature
  - We are busy and distracted at work
  - Messages “look right”

- Some problems companies increase through their actions
  - Companies don’t see the confusion these vendors cause
  - No internal communications policy (company → employee)
  - Different departments using different outsourced vendors
  - Addresses and links using multiple, external domains
  - Anti-phishing training is a tedious, once-a-year obstacle to work
Which Is Phishing, Which Is Outsourced?

<table>
<thead>
<tr>
<th>Action Required: New Online Account Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Support Desk</td>
</tr>
<tr>
<td><a href="mailto:employee@examplecorp.com">employee@examplecorp.com</a></td>
</tr>
<tr>
<td>Tuesday, November 22, 2017 at 8:40 AM</td>
</tr>
<tr>
<td>Show Details</td>
</tr>
</tbody>
</table>

**ExampleCorp**

To ensure adequate security, we have made slight changes to some of our security policies. All employees are being asked to review and record acceptance of these new policies.

Please visit [http://outlook.office365.com/owa](http://outlook.office365.com/owa) to review the new policies.

Thank you for your prompt attention,
IT Support

<table>
<thead>
<tr>
<th>Action Required – Please complete your certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA</td>
</tr>
<tr>
<td>Vrimini Automated Notification Mailing</td>
</tr>
<tr>
<td><a href="mailto:employee@examplecorp.com">employee@examplecorp.com</a></td>
</tr>
<tr>
<td>Tuesday, November 14, 2017 at 10:10 AM</td>
</tr>
<tr>
<td>Show Details</td>
</tr>
</tbody>
</table>

**ExampleCorp**

Our records show that you are one of the few remaining employees who hasn’t yet certified that you have read and understood the updated Employee Travel Policy. This certification is now past due and must be completed immediately.

[Click here to begin](#)

We have changed the company names, but these are both examples based on real messages received by company employees.
This Is Phishing

Action Required: Complete Online Account Renewal

IT Support Desk [mailto:jan@prismmg.com]
employee@examplecorp.com

Tuesday, November 22, 2017
Show Details

ExampleCorp

To ensure adequate security, we have made slight changes to some of our security policies. All employees are being asked to review and record acceptance of these new policies.

Please visit http://outlook.office365.com/owa to review the new policies.

Thank you for your cooperation.

IT Support

https://randomsite.com/backend/Microsoft?
&userid=employee@examplecorp.com

- From: address is external
- Urgent Call-To-Action
- Uses expected company logo
- Link goes to external site
- Link displayed doesn’t match target
- Link domain doesn’t match From:
This legitimate campaign frequently reported as phishing!
This practice – and problem – did not develop overnight. But we must start to pay attention to securing these communications, just as we have started securing communications to customers.
Phishing is Growing (So Is DMARC)

- Annual reports have tracked growth of spam & phishing for many years
- Phishing a greater threat than spam
- Industry analysts (Gartner) add email authentication to their buying guides
- Growth of DMARC 2012 - 2015
- Recent focus on DMARC “reject”
- Will they focus on internal communications in 2018?
**Phishing → Compromises → Headlines**

**Phishing, Data Breach, Ransomware**

2015: 740 MM records disclosed in data breaches
US $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
US $5 Billion 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:
APWG 2016Q1 report:
Ransomware damage costs:
News Articles Calling For Solutions

- The Press Has Noticed!
- Crime is accelerating, leading news
- Email is often the vector for attacks
- Industry and press push for solutions, asking why DMARC isn’t used more widely
- Increase in data breaches, 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
- October: US DHS announces DMARC requirement
What Should Companies Do?

Stop Acting Like Phishers

- Consistent use of 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
DMARC Update
Only 62,000 ending same quarter in 2016. We only include domains that are still publishing DMARC records. For the graph above, our figure for 2016-09 reflects domains that first published a DMARC record from 2012-01 through 2016-09, and which are still published as of 2017-10. Therefore the figure shown in the graph for 2016-09 is 48,838 – however, when these same records were checked in 2016-10, the total was roughly 62,000. Between 2016-10 and 2017-10, roughly 13,000 domains that had published DMARC records before 2016-10 withdrew their records, lowering the total observed in 2017-10.
United States ~350% 2017 versus 2016
United Kingdom 380% 2017 versus 2016
Active DMARC Records in Euro ccTLDs

United Kingdom
Netherlands
Italy
France
.EU
Spain
Germany

Data provided by Farsight Security
Graph © 2017 Trusted Domain Project
Predictions

- Phishing will continue to grow, spam steady or declines
- More governments will recommend/require DMARC
- ARC protocol will help address limitations of DMARC
  - OpenARC implementation ships in 2017 Q4
- Global ISPs resume motion toward “No Auth, No Entry”
  - Google, Microsoft
- More visual indicators of authentication for end users
- DMARC adoption up 300% through 3Q2017, but perhaps 200% in 2018 due to increased scale
ありがとうございました
Thank you
References & Resources
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/
Resources – US Policies

https://cyber.dhs.gov/

https://www.wyden.senate.gov/download/letter-to-dhs-regarding-dmarc

March 2017: FTC - ”Use Email Authentication”

April 2016: NIST Special Publication 800-177: Trustworthy Email
https://csrc.nist.gov/presentations/2016/nist-sp-800-177-trustworthy-email
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)
Agari: Email Threat Taxonomy

Sender
- Impostor
  - Spoof
  - Look-alike Domain
  - Display Name Deception
- Authentic
  - Compromised Account
  - Account Owner

Classification
- Fraud
- Social Engineering
- Scattershot
- Targeted
- URL
- Malware
- Con
- Unsolicited Email
- SPAM
- Grey Mail
- Legitimate Email

Recipient
- Internal
  - Employees
  - Contractors
- External
  - Partners
  - Customers

Objective
- Monetary
- Data/Credential Theft
- Denial of Service

© 2016 Agari. All rights reserved.
# 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