Evaluating DMARC Effectiveness for the Financial Services Industry

by Robert Holmes
General Manager, Email Fraud Protection
Return Path

Executive Summary

- Email spoofing steadily increases annually.
- DMARC helps to combat spoofing cybercrime, but DMARC's protective coverage is being debated.
- Return Path executed a study of top 11 financial service brands, spanning 900 million email messages.
- The results show that an average of 30.1% of those emails would have been stopped by DMARC.
- A multi-layered solution, beginning with DMARC and enhanced with Threat Intelligence and Mitigation Services (TIMS), is a better strategy for securing your data, brand and assets.

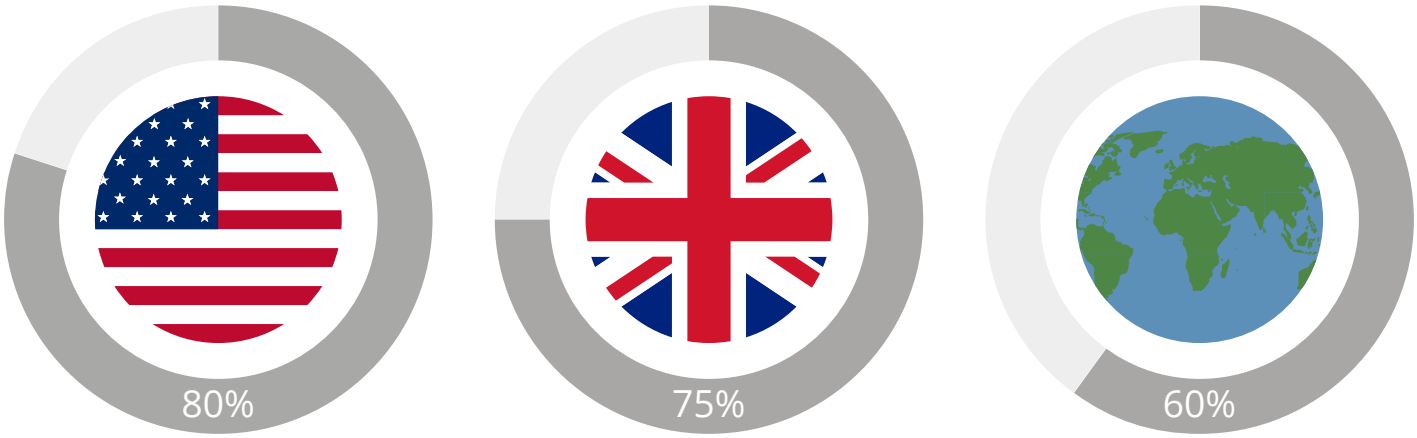
It can be frustrating when hackers discover a hole in your security model, but it happens to the best of us.

One needs to look no further than Home Depot's recent announcement that malware was used to steal data on 56 million credit and debit cards along with 53 million email addresses, with damages estimated at as much as $3 billion.[1] It's bad enough when a cyber criminal beats your security technology, but it's exasperating when you fall into the trap of an email phishing scam by unwittingly letting the bad guys in.

Research shows the total number of phishing scams observed in Q1 2014 was 125,215, a 10.7% increase over Q4 2013. That figure is the second-highest number detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.[2] Email offers vulnerabilities that criminals exploit, fully knowing that the first step in the course of action is for Internet Service Providers (ISPs) to shut the source down, and that criminal prosecution is unlikely.

But that doesn't mean enterprises and individuals have not developed counter-strategies. Billions of email accounts are now protected by DMARC (Domain-based Message Authentication, Reporting & Conformance), and enterprises such as Fidelity, Visa, and LinkedIn are realizing more secure email exchange. Although online payment services are certainly a prime target, more than 25 million email messages spoofing PayPal were rejected during the 2013 holiday buying season, according to DMARC.org. Our records show that there was a 130% increase in client adoption, as well as domains publishing DMARC records, between 2012 and 2013.

Percentage of mailboxes protected:



Hold your applause, however. While DMARC is effective to a certain extent and adoption is growing, we know that there's much more to eliminating email phishing attacks. And we believe that the first and best thing to do is to find out how much more needs to be done.

How Important is DMARC?

One question that the industry as a whole differs on is: What is the actual percentage of email fraud blocked by DMARC? The answer to that question is critical because implementing a DMARC strategy is not a trivial undertaking. It requires either investing in a third-party service or dedicating in-house resources to the project. Most enterprises consider the following when weighing that decision:

“

Ask yourself:

How integral is implementing a DMARC policy to our business success?

We believe a good way to determine the answer to that question is to then ask:

How much do we need our customers to trust us?

”

- While some organizations have IT resources in-house who understand the underlying email technology well enough to execute DMARC, finding actionable information in the data requires authentication specialists, which is rarely what corporations look for in IT skills and therefore have on-staff. Also, the DMARC space is relatively new, as it was just publicly announced in January 2012, and there are very few in-house experts.

- Organizational challenges compound the technical challenges. Even for medium-sized enterprises, multiple stakeholders need to align and it's almost certain that third-party senders will need to be involved. The upshot is that the project and risk management create operational costs and organizational headaches that far outweigh using a provider such as Return Path.

Return on investment is the bottom line when it comes to your email efforts and ROI can be measured both in financial terms as well as impact on your brand, which often is directly equated to your industry. Financial services and ecommerce-dependent organizations surely need to be protected more than a small brick and mortar business, for example. However, according to APWG's 2H 2013 report "the companies (brands) targeted by phishing targets were diverse, with many new targets, indicating that e-criminals are looking for new opportunities in new places."[4] Ask yourself: "How integral is implementing a DMARC policy to our business success?" We believe a good way to determine the answer to that question (in addition to considering operational costs) is to then ask: "How much do we need our customers to trust our email program?"

Return Path is focused on multiple facets of email intelligence. We track proprietary data relating to 7 billion emails per day to identify malicious senders – and that doesn't even include DMARC tracking and reporting. Fraud detection and prevention is a significant part of our core competency, and in order to gauge how effective our data is in addition to the impact DMARC has, we built a formal campaign designed to analyze the phishing attacks we detected.

Types of spoofing include

Domain-based threats
mimic the precise sending domain of the brand (e.g support@mybank.com).

Cousin domain threats
are sent from addresses with domains that closely resemble the sending domain of the brand (e.g support@my-bank.com).

Display name spoofing
mimics the brand in the header from label which most email clients render (entirely unrelated to the header-from email address itself).

Subject line spoofing
mimics the brand in the subject line (independent of domain/ display name) in order to get the recipient to open the malicious message.

Campaign Rationale and Analysis

There are two essential components to our analysis: The data we collected and explored (and masked the identity of) and the type of phishing attacks that we decided to investigate, which we called "campaigns" in our analysis.

Based on the fact that the financial services industry is one of the most highly targeted sectors for attacks, we narrowed the data set to 11 of the largest banks operating in the U.S. and U.K. This allowed us to focus on 20 million emails per day by using only domain-based attacks and by culling false positives and legitimate third-party senders that simply mentioned a target brand; the evaluation time frame was set at 45 days.

We analyzed data points comprised of spam, spam traps and relevant complaint emails tracked back to the 11 brands. Another criterion we established was that the brands we chose to study had not implemented DMARC; the rationale behind this is that if an organization had already implemented DMARC, spoofing campaigns would have been blocked, at least to some degree.

Ultimately, our goal was to use data-grounded analysis to determine the percentage of fraudulent campaigns that appear to come from a legitimate source that could be blocked by DMARC, and thereby show the impact for top brands. Prior to our study, most email fraud protection providers have essentially speculated about the percentage of spoofed mail addressable by DMARC, with some stating extremely high levels of blocking.

With that in mind, we defined five combinations of domain-based campaigns that initial review of the data sets showed to be common spoofing tactics:

- Header from | Subject | Date
- Header from | Subject
- Display name | Header from domain | Subject
- Header from domain | Subject
- Sending IP address | Subject

Campaign definition	Count of campaigns (across 11 brands)	Domain-based campaigns (average % across 11 brands)
Header from | Subject | Date	10,823	26.66%
Header from | Subject	8,347	25.46%
Display name | Header from domain | Subject	6,770	25.45%
Header from domain | Subject	6,316	26.04%
Sending IP address | Subject	12,124	30.18%
Average	8,876	26.76%

We determined that the Sending IP address | Subject strategy was the most frequently used type of domain-based attack and likely to give the most legitimate results.

What follows is our analysis of the volume of the attacks that DMARC would have blocked, had the financial institutions previously implemented a reject policy.

Brand (Sending IP address | Subject)	Domain-based campaigns
Brand 1	1.06%
Brand 2	8.47%
Brand 3	76.53%
Brand 4	3.22%
Brand 5	27.81%
Brand 6	43.80%
Brand 7	18.21%
Brand 8	66.39%
Brand 9	38.46%
Brand 10	1.18%
Brand 11	46.90%
Average	30.18%

> We found that DMARC would have blocked 30.18% of attacks on average across the 11 banks we analyzed, with the range of effectiveness between 1.18% and 76.53%.

Results and Potential Impacts

We found that DMARC would have blocked 30.18% of attacks on average across the 11 banks we analyzed, with the range of effectiveness between 1.18% and 76.53%. Our results show that DMARC will produce a very good ROI for some brands and domains, even though it will not block all phishing schemes.

Other brands will not be as fortunate, as DMARC will not block the attacks on their brand. There are also hard costs associated with these attacks. The enterprise is obligated to reimburse people who have been defrauded. They also will need to engage their fraud team and perhaps a service provider to remediate – take down the offending site, reset passwords of compromised accounts and perhaps reevaluate their entire security strategy. A thorough assessment of damages could involve looking deeper into their infrastructure for worms, viruses, etc. As we frequently read about in the mainstream press, advanced persistent threats (APTs) might go undetected for months or longer, siphoning sensitive and valuable information that leads to multi-million dollar damages and immeasurable negative publicity.

As bad as the financial impact can be, consider the damage to brands when their customers can't trust them. For example, retailer Target's sales "nose-dived once news of the attack broke, a week before Christmas. More important, analysts said, will be rebuilding shoppers' faith."[5]

Recommended Next Steps

A multi-layered security strategy is clearly the best approach. Traditional solutions operate downstream of the attack; they are reactive and focus on shutting fraudulent sites down after the damage has been done. A more ideal solution is proactive and more responsive:

- Block email fraud from reaching mailboxes.
- Mitigate email threats that get through more quickly.
- Provide greater intelligence regarding the nature, size and impact of the threat.

> The first step for any organization evaluating their security strategy is certainly to implement DMARC.

The first step for any organization evaluating their security strategy is certainly to implement DMARC. The ISP reports that come with DMARC implementation (regardless of the chosen policy) will help you decide if adding more fraud protection services is technically practical and financially sound. In those reports, you will receive feedback from mailbox providers on every email that does not pass authentication, thus improving email visibility. We would welcome the opportunity to help you assess DMARC reports; simply contact us and point the records to us for review. Should you decide to engage with Return Path, you will find that our resources enable you to:

- Eliminate the impact: suspicious emails that fail to meet authentication, reputation or other heuristic criteria are blocked by ISPs that support DMARC.
- Mitigate the impact: fraudulent URLs are published to a global network of providers who block access to the malicious site and ultimately remove the offending content.
- Accelerate mitigation: real-time threat intelligence feeds an automated process to reduce the time to detection, thereby reducing the time to mitigation.

Conclusion

Wouldn't it be great if you could use email for what it is intended: efficient and convenient communication, doing business at scale and cutting operational costs? DMARC is a great element in the multi-layer strategy which we believe is necessary to reaching an optimal email security state. Additionally, Return Path's real-time threat intelligence and mitigation services (TIMS) will bolster defenses, helping you build on the blocking capabilities that DMARC provides and mitigating the impact that it doesn't.

You have options and can take decisive steps to gain and maintain control of your communications, operations and your brand. But going it alone is probably not the most effective strategy. Working together, we can help you stay out of the traps cybercriminals set every day.

About Return Path

Return Path is the worldwide leader in email intelligence. We analyze more data about email than anyone else in the world and use that data to power products that ensure that only emails people want and expect reach the inbox. Our industry-leading email intelligence solutions utilize the world's most comprehensive set of data to maximize the performance and accountability of email, build trust across the entire email ecosystem and protect users from spam and other abuse. We help businesses build better relationships with their customers and improve their email ROI; and we help ISPs and other mailbox providers enhance network performance and drive customer retention.

To find out more about Return Path's anti-phishing and brand protection services, visit www.returnpath.com/security

References:

1. http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/
2. http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf
3. http://dmarc.org/overview.html
4. http://www.washingtonpost.com/business/economy/data-breach-hits-targets-profits-but-thats-only-the-tip-of-the-iceberg/2014/02/26/159f6846-9d60-11e3-9ba6-800d1192d08b_story.html
5. http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf

Global Offices

USA (Corporate Headquarters) rpinfo@returnpath.com
Australia rpinfo-australia@returnpath.com
Brazil rpinfo-brazil@returnpath.com
Canada rpinfo-canada@returnpath.com
France rpinfo-france@returnpath.com
Germany rpinfo-germany@returnpath.com
United Kingdom rpinfo-uk@returnpath.com

Return Path

returnpath.com/security