Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication

STAFF PERSPECTIVE | MARCH 2017

Introduction

With subject lines such as "Suspicious Account Activity," "Invitation to Connect," or "Online Confirmation Required," phishing emails can trick people into divulging usernames, passwords and other sensitive information to scam artists and harm the reputations of the businesses whose identities are spoofed. These messages often include the phished businesses' graphics and appear to include links to the businesses' web sites, making it difficult to tell the difference between real messages and spoofed ones. The best way to prevent people from falling for phishing messages may be to keep these scam emails from ever showing up in their inboxes.

Several technical solutions exist that can help reduce the number of phishing emails reaching people. Many businesses already use some of these low cost, readily available solutions to help email providers determine the authenticity of received email. However, few of the major online businesses use the full capability of these solutions, potentially allowing many phishing emails to get through. As explained below, online businesses can play a significant role in decreasing the number of phishing emails by instructing receiving email servers to automatically reject unauthenticated emails.

In this BCP Staff Perspective, we explain that:

- The same design that makes email ubiquitous and simple also makes it easy to spoof email senders' addresses and to generate phishing messages.
- A business can take two major steps to prevent its domains from being used in phishing scams:
    - Use domain level email authentication so that receiving mail servers can verify that a message that claims to be from the business actually came from a domain authorized by the business. There are two forms of domain level authentication that a business can use -- Sender Policy Framework (SPF), which allows a business to designate the IP addresses it uses to send email, and DomainKeys Identified Mail (DKIM), which allows businesses to use digital signatures to verify the authenticity and integrity of their messages.
    - Use a complementary scheme called Domain Message Authentication Reporting & Conformance (DMARC) which, among other things, enables a business to: (1) gather intelligence on how phishers and other scam artists are misusing their domains, and (2) instruct receiving email servers how to treat unauthenticated messages that claim to be from the business's domain. In its DMARC listing, a business can instruct a receiving email server to reject unauthenticated messages

or quarantine such messages (send them to a junk mail folder). Or the business can provide no instruction in its DMARC listing.

- A study by the FTC's Office of Technology Research & Investigation (OTech) of more than 500 business with a significant online presence found that:
  - The majority of the businesses have implemented SPF, one of the two domain authentication tools.
  - Only one-third of the businesses have implemented DMARC in any form. And, of these businesses that have implemented DMARC, fewer than ten percent are using the strongest available setting in DMARC which tells receiving email servers to reject (block delivery of) unauthenticated messages.
  - Businesses in the "Financial Services" category were the most likely to use the strongest available setting.

Background

Email sender addresses are easy to forge

Phishers and other spammers exploit a design decision made early in the history of the Internet. The Simple Mail Transfer Protocol (SMTP), the Internet protocol for email, was designed to make it easy for computers to send and receive messages, even if information was incomplete or corrupt. For a message to be delivered, SMTP only requires that the address in the "To" line be a valid address. All of the other information in the message can be false. Phishers and other spammers take advantage of this by spoofing where the message comes from.[1]

With email, there are actually two types of "from" information that phishers can spoof – the "Envelope From" and the "Header From."[2] The "Envelope From" indicates which server is sending the message. It is like the return address appearing on an envelope sent through the postal system. An email recipient does not usually see the "Envelope From." The "Header From," on the other hand, is the information that a recipient sees in the "From" line of a message. It indicates the original author of the message. With SMTP, the "Envelope From" and the "Header From" do not have to match. Furthermore, they can both be inaccurate. The ease of spoofing both types of "from" information (it requires virtually no technical sophistication) and the free nature of email help contribute to large numbers of phishing messages.

Domain-level authentication reduces sender address spoofing

Since 2004, the FTC has been urging web site operators and email providers to adopt domain-level authentication systems that verify that an email actually comes from the domain identified in the "From" line of the message.[3] (In other words, if a message claims to be from john@example.com, domain-level authentication methods can verify that the message actually comes from some address at example.com). In the intervening years, two major domain-level authentication systems have become fully developed and widely deployed – SPF and DKIM.[4]

SPF enables receiving mail servers to determine whether a message that claims to be from a particular domain comes from an Internet Protocol (IP) address that domain uses for sending

messages. For SPF to work, both sending domains and receiving domains must use the protocol. A sending domain implements SPF by adding to its Domain Name System (DNS) record the IP address(es) it uses to send email originating from the domain.[5] A receiving email server implements SPF by comparing the "Envelope From" of an email to the IP address listed in the "Envelope From" domain's DNS Record. If there is a match, the message is considered authentic.

DKIM also can be used to verify that an email truly comes from the sender it claims to be from. As with SPF, sending domains and receiving domains have important roles in DKIM's implementation. With DKIM, a sending domain creates a public/private cryptographic key pair and publishes the public key in its DNS record. The sending domain creates a cryptographic hash of the body of the message and then creates a second hash using the message's header information and the hash of the message's body. Then the sending domain digitally signs this second hash using its private key, and places this digital signature in the email's header. The receiving email server then uses the public key published in the sending domain's DNS record to verify that the domain listed on the signature did in fact send the message and that the signed content has not been tampered with since the time it was signed.

While SPF can authorize a specific server to send messages on behalf of a domain and DKIM allows assurance to the recipient that an email was sent by a particular domain, they leave important gaps in a full anti-phishing solution. SPF only validates the "Envelope From" domain and DKIM only validates the domain listed in the signature. Neither includes a way for recipients and senders to communicate regarding which messages fail validation or what to do with failed messages. Domain owners remain unaware of the extent of spoofing attempts, and the decision of what to do with failed messages is left up to the receiving server alone.

A complementary protocol called Domain Message Authentication Reporting & Conformance (DMARC) helps fill these gaps and provides a more robust anti-phishing solution.[6] Specifically, DMARC takes email validation a step further by comparing the domain in the "Header From" address to the domains used for SPF and/or DKIM validation. DMARC additionally provides a way for a sending domain to instruct receiving email servers how to treat unauthenticated messages that claim to be from the sending domain. Using DMARC, a sending domain can include in its DNS record one of three instructions to give to receiving domains should validation fail:

(1) block delivery of unauthenticated messages (noted in the DMARC listing as "p=reject"),
(2) place unauthenticated messages in the recipient's junk email folder (noted in the DMARC listing as "p=quarantine"), or
(3) no specific guidance on how to treat unauthenticated messages (noted in the DMARC listing as "p=none") (as explained below, a sending domain could use the "p=none" instruction in conjunction with a request for receiving domains to send it reports about authentication failures, thereby enabling the sending domain to monitor whether its SPF and DKIM DNS entries are working properly).

In other words, by using DMARC, a sending domain can instruct receiving email servers to block delivery of all unauthenticated messages – such as phishing messages – that claim to be from the sending domain.

Equally critical, the sending domain's DMARC listing can ask that receiving domains email back reports whenever they receive an unauthenticated message that purports to be from the sending domain. This enables the sending domain to observe and monitor efforts to spoof its domain and be more proactive in combating spoofing.[7]

Complex email set-ups and the use of third party and cloud service providers may create challenges for the speedy implementation of DMARC with the use of a "p=reject" instruction. These tools also can require ongoing maintenance, as independent actions by third parties can affect a company's email operations.[8] By working to overcome these challenges, businesses will not only protect consumers from phishing schemes, but also protect their own brand reputations from misuse.

When creating a DMARC listing, a business may wish to start by setting a policy of "p=none" and requesting that receiving domains send reports of authentication failures. This is especially true for businesses that do not know all of the legitimate emailing domains and subdomains being used by their various divisions or that use third parties to send email on their behalf or to manage their DNS. After reviewing these reports and making any necessary changes to its DNS records, a business can change its DMARC listing to instruct receiving mail servers to reject ("p=reject") unauthenticated messages or place them in junk folders ("p=quarantine"). A DMARC "p=reject" instruction provides the strongest protection against phishing because it ensures that unauthenticated messages are not inadvertently opened by recipients who are checking messages in their junk folders.

Current State of Email Authentication Adoption

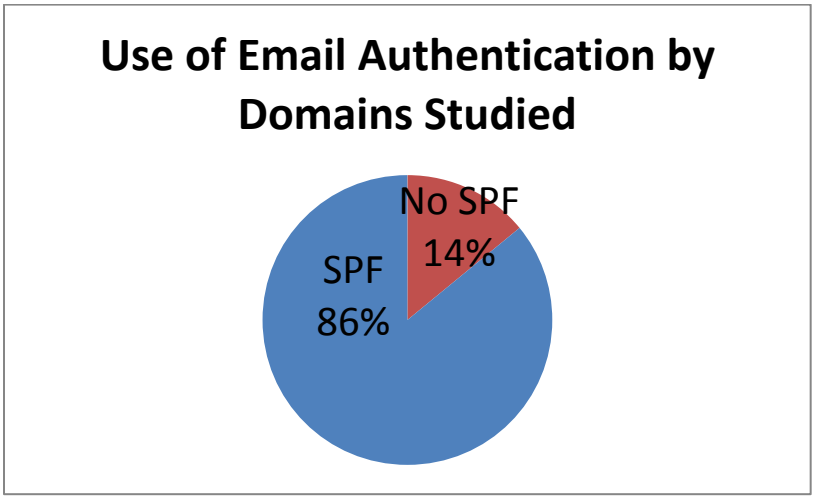
Study of 500+ online businesses shows that many could do a better job preventing the delivery of phishing messages

During July 2016, the FTC's Office of Technology Research & Investigation (OTech) identified 569 businesses with a significant online presence and determined whether the businesses' DNS records contained SPF and DMARC entries. OTech selected these businesses using Alexa.com, a service that ranks websites based upon their traffic volume and popularity.[9] For businesses that had a DMARC entry, OTech determined whether the DMARC entry instructed receiving email domains to reject unauthenticated messages ("p=reject") or quarantine the messages ("p=quarantine"), or whether the DMARC entry provided the receiving server with no instruction ("p=none").

86% of top businesses authenticate the emails they send using SPF

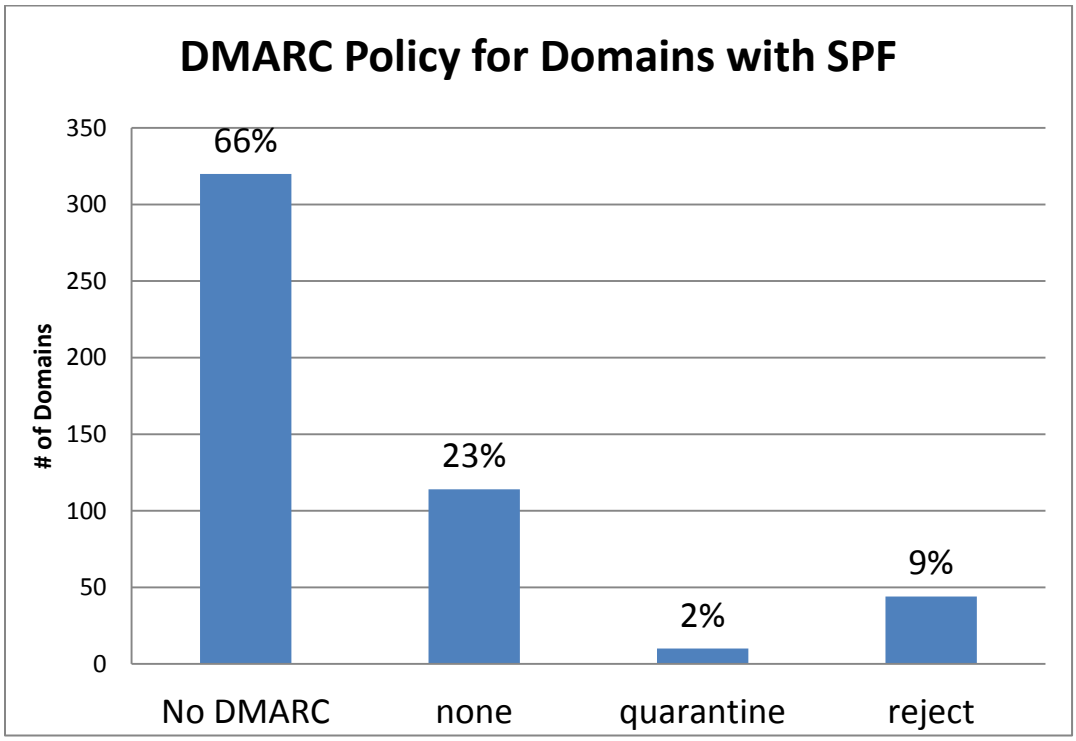
SPF has been widely adopted, with 86% (489 out of 569) of the surveyed domains having SPF information in their DNS records. Though this study was not able to verify if all domains used

DKIM,[10] given that SPF is easier to implement, it is unlikely that a domain has implemented DKIM without SPF.



Businesses Rarely Use DMARC to Instruct Receiving Email Servers to Reject Unauthenticated Messages

Of the 489 domains that had implemented SPF domain authentication, 66% (320 out of 489) had no DMARC entry, meaning that these domains provided no instruction on how receiving mail servers should treat unauthenticated messages and were receiving no reports about unauthenticated messages that were claiming to be from their domains (such as phishing messages). Therefore, many businesses are not taking advantage of an important tool that provides useful intelligence on spoofing and ensures consistent treatment of unauthenticated mail.



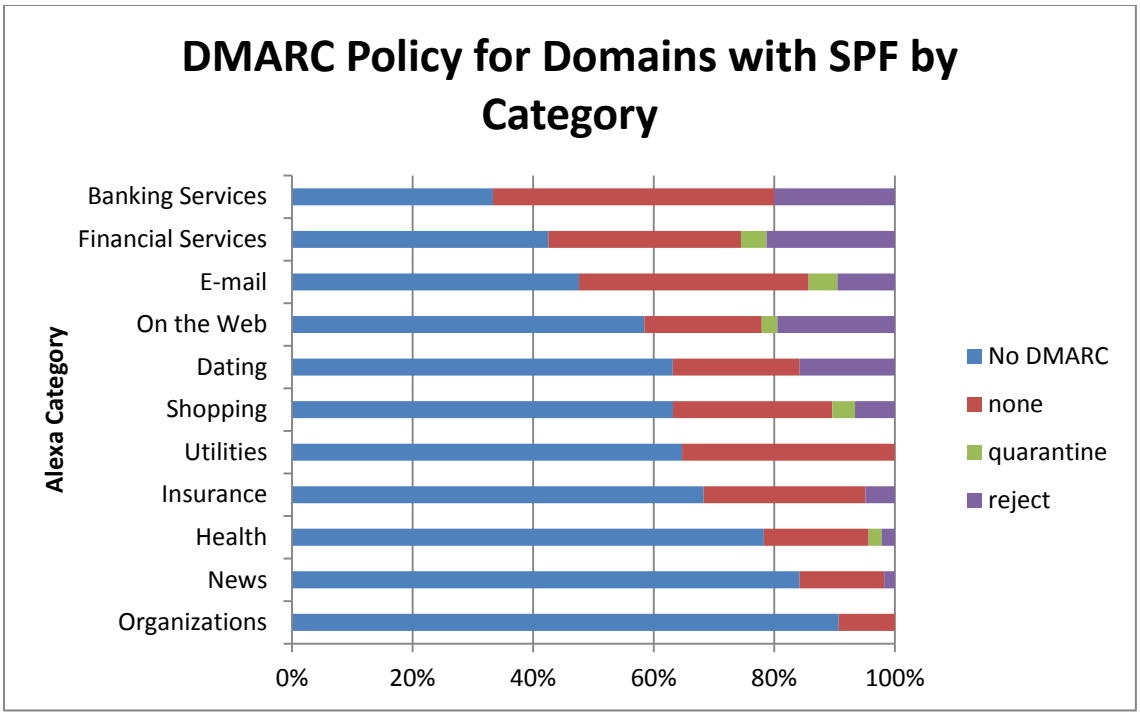
Of the 34% (168 out of 489) of domains that had a DMARC entry in their DNS records, the majority had set their DMARC policy to "none," which does not give specific instructions on what to do with emails that have failed authentication. All of the domains with a DMARC "none" policy did, however, include an email address in their DMARC entry, which allows the sending domains to receive reports about emails that have failed authentication while still allowing for their delivery.

Many businesses that implement DMARC will start with a "none" policy. This enables the businesses to determine whether any of their legitimate messages are being erroneously identified as unauthenticated. For instance, businesses that extensively use third-party mailing services can encounter challenges because the services sometimes "spoof" a business's email domain by sending email on its behalf, breaking the key assumptions of SPF and DKIM.[11] However, with the benefit of the DMARC reports, a sending domain may gain insight into how its domains are being used (or misused) for email and whether a shift to a "reject" policy would result in the rejection of its legitimate messages.

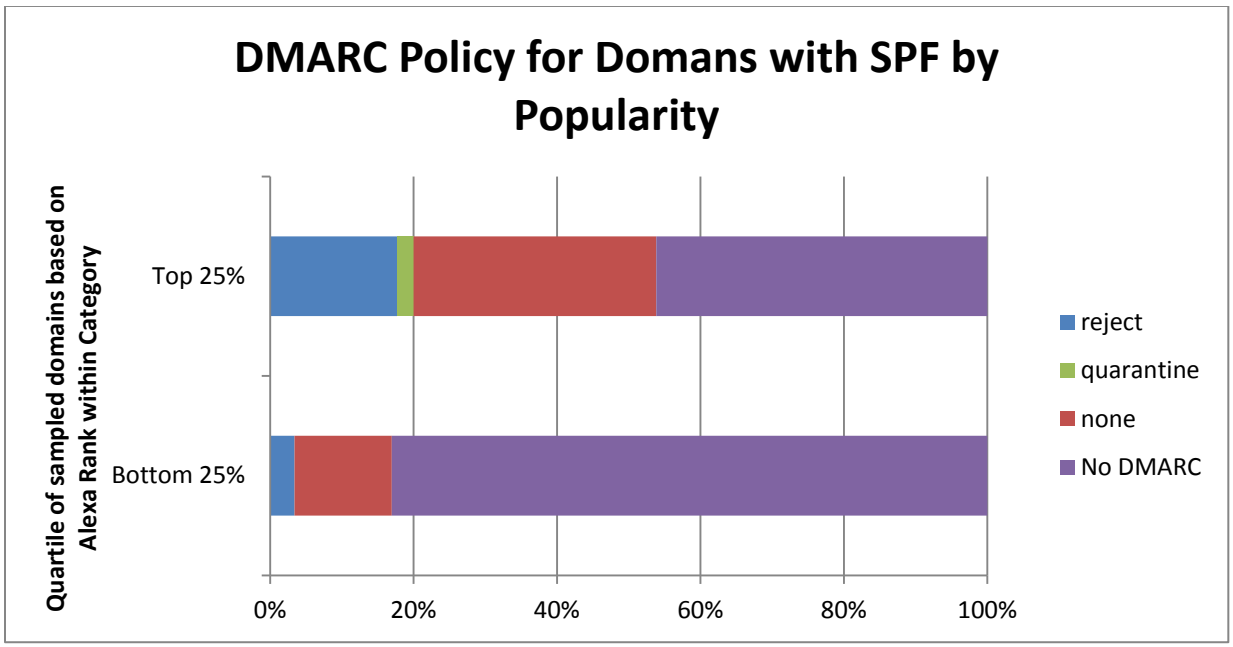
Two percent (10 out of 489) used the "quarantine" policy, which asks the receiver to treat the email with heightened scrutiny (e.g., flag it as spam). And, only 9% (43 out of 489) used the most aggressive of email authentication policies, instructing receiving mail servers to reject and not deliver messages that have failed authentication.

A small number of the surveyed domains (13 out of 569) did not appear to be used for email (the domain did not have a mail exchange (MX) record in its DNS listing). However, even if a business does not use a domain to send email, or a domain is parked (i.e., used as an alias for the main domain), phishers could still send email claiming to be from an address at the domain. For a business's non-mailing domains, the inclusion of a DMARC record with "p=reject," along with an appropriate SPF policy indicating that no addresses are authorized to send email originating from that domain, will help ensure that these domains are not used in phishing campaigns, and spoofing attempts are reported back to the domain owner.

The use of email authentication technologies varies by the type of commerce a domain engages in, and the relative popularity of the domain. While companies in Alexa's "Financial Services" category were the most likely to include DMARC listings with "p=reject," only about 20% of these domains used this strictest of DMARC settings.[12]



Moreover, when looking at the relative popularity of the sites based on their Alexa Rank within a category, the more popular sites were more likely to have implemented DMARC and more likely to use the strictest policy ("p=reject"). For this analysis, we separated each Alexa category into quartiles of domains based on the popularity of the domains and then examined the use of SPF and DMARC by domains in each quartile. We found that 54% of the domains in the top quartile with SPF records had a DMARC record, with 33% of those domains using the "p=reject" policy. However, only 17% of domains in the bottom 25% of SPF protected domains had implemented a DMARC policy of any type.



Conclusion

Businesses can help stop phishing and protect their brands against spoofing by fully implementing current technical solutions

Businesses can help reduce the number of phishing email messages and protect their reputations by fully implementing the low cost, readily available email authentication solutions described in this BCP Staff Perspective.

Our research shows that most top online businesses have adopted email authentication technologies, but only a small fraction have taken the additional step of implementing DMARC. With DMARC, a business can protect its domains from being used by phishers and other scammers by instructing receiving domains to automatically reject unauthenticated messages that claim to be from the business's domains. This powerful tool could be an effective means of combatting phishing scams. Unfortunately, our research demonstrates that few of the top US online businesses are using the DMARC solution to the fullest extent. Wider implementation of DMARC with the "p=reject" instruction could further combat phishing by keeping these scam emails from ever showing up in consumers' inboxes.

Contributors

Division of Litigation Technology & Analysis

OFFICE OF TECHNOLOGY RESEARCH & INVESTIGATION (OTECH)

Phoebe Rouge
Sheryl Roth
Dan Salsburg

[1] When the SMTP protocol was originally designed, the priority was to ensure interoperability and resiliency. Messages should be able to reliably and efficiently reach their destination, even after being transferred and relayed across numerous servers with slow or inconsistent connections. For more details, see the official Internet Engineering Task Force (IETF) document on SMTP, RFC5321 (https://tools.ietf.org/html/rfc5321).
[2] The "Envelope From" and "Header From" are officially referred to as the RFC5321.MailFrom and RFC5322.From, based on the IETF documentation that describes them.

[3] National Do Not Email Registry: A Federal Trade Commission Report to Congress (June 15, 2004) https://www.ftc.gov/reports/can-spam-act-2003-national-do-not-email-registy-federal-trade-commission-report-congress. *See also*, opening remarks of former FTC Chairman Deborah Majoras at the FTC's 2004 Email Authentication Summit (urging industry to combat spam and phishing by making email authentication a reality) (https://www.ftc.gov/sites/default/files/documents/public_events/email-authentication-summit/draft_transcript_day1.pdf).

[4] More details on SPF and DKIM are available in their IETF documentation, RFC7208 (https://tools.ietf.org/html/rfc7208) and RFC6376 (https://tools.ietf.org/html/rfc6376), respectively.

[5] The Domain Name System (DNS) is a system of servers on the Internet that have lookup tables to convert human readable addresses (www.ftc.gov) into numerical addresses computers understand (e.g., 192.168.1.1). It is roughly equivalent to a phone book for all of the devices connected to the Internet. All of this information is necessarily public and automatically accessed as users navigate to various domains. Over time, additional types of information have been added to the DNS as an efficient way of allowing devices to query important information about a particular domain. More information is available in numerous IETF documents (e.g., RFC1034, RFC1035) . For recent updates, see RFC7719 (https://tools.ietf.org/html/rfc7719).

[6] More details regarding DMARC are available from IETF RFC7489 (https://tools.ietf.org/html/rfc7489).

[7] While SPF, DKIM and DMARC are important anti-phishing and anti-spoofing technologies, they are not a panacea for phishing and spam. For instance, even if the domain examplebank.com implements these protocols, a phisher can still use typo domains (e.g., exsamplebank.com) or subdomains (e.g., examplebank.scam.com). Moreover, if the phisher controlled these domains, it could publish SPF, DKIM and DMARC records in the DNS for these domains. Nonetheless, SPF, DKIM and DMARC enable businesses to prevent their actual domains (and any other typo domains they register) from being misused by phishers and other scammers.

[8] *See, e.g.*, Alexander García-Tobar, "The Trouble With DMARC: 4 Serious Stumbling Blocks," http://www.darkreading.com/cloud/the-trouble-with-dmarc-4-serious-stumbling-blocks/a/d-id/1327957.

[9] The appendix to this BCP Staff Perspective explains the criteria used for selecting businesses for inclusion in the study.

[10] See Appendix for further details.

[11] Third-party mailing services, mailing lists, and auto-forwarding services were developed under the lax assumptions of the original SMTP standard, and therefore, can cause challenges to the strict enforcement of newer measures, such as SPF, DKIM, and DMARC alignment. DMARC.org as well as many third-party companies that provide mailing services offer resources on how to preserve functionality while protecting domains from phishing. Additionally, a new protocol for preserving email authentication information across multiple intermediaries, known as Authenticated Received Chain, or ARC, is currently under development by the IETF, and is intended to address some of these legacy issues. More information can be found at http://arc-spec.org/

[12] Additional data for this chart is in the Appendix.

Appendix - Methodology

OTech selected the 569 businesses using publicly available data from Alexa, a web site analytics firm owned by Amazon.com. Using Alexa's own categorization of web sites, OTech selected the top ranked domains appearing in Alexa categories where domains were likely to have significant interaction with consumers and where consumers could have accounts, thereby making the domains particularly vulnerable to phishing campaigns. These Alexa categories were Shopping, On the Web, News, Health, Organizations, Financial Services, Insurance, Email, Banking Services, Dating, and Utilities. We excluded from the analyses any web sites that did not appear to have significant interaction with US consumers (those that used a country code top level domain (ccTLD) or that, according to Alexa, had less than 2% of its traffic with US visitors). We also excluded from analyses educational and government domains that use the .edu and .gov top level domains. In many instances, Alexa places particular domains in multiple categories. When this occurred, we treated such a domain as appearing in the category in which it was ranked the highest and then removed the domain from all other categories.

Using an automated script, OTech queried the DNS records of each of the domains and extracted SPF and DMARC records. We also determined whether each domain was capable of being used to send email by extracting a DNS record called an "MX record." One limitation of this study was the inability to check whether a domain also implemented DKIM. The domain name containing the DKIM signature is not standard, and dependent on an arbitrary string called a "selector," which is only visible to recipients of a DKIM signed message from that domain. Without this additional piece of information, we could not categorically look up the DKIM DNS information necessary. As another potential limitation, when checking SPF and DMARC DNS records, OTech did not determine whether the records were properly configured, only that they were present.

Appendix - Data Supplement

DMARC Policy for Domains with SPF by Alexa Category

Alexa Category	# of Sites	No DMARC	none	quarantine	reject
Society > Organizations	43	91%	9%	0%	0%
News	57	84%	14%	0%	2%
Health	46	78%	17%	2%	2%
Business > Financial Services > Insurance	41	68%	27%	0%	5%
Business > Energy > Utilities	17	65%	35%	0%	0%
Shopping	106	63%	26%	4%	7%
Society > Relationships > Dating	19	63%	21%	0%	16%
Computers > Internet > On the Web	77	58%	19%	3%	19%
Computers > Internet > E-mail	21	48%	38%	5%	10%
Business > Financial Services	47	43%	32%	4%	21%
Business > Financial Services > Banking Services	15	33%	47%	0%	20%
Grand Total	**489**	**66%**	**23%**	**2%**	**9%**