- 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 using 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]

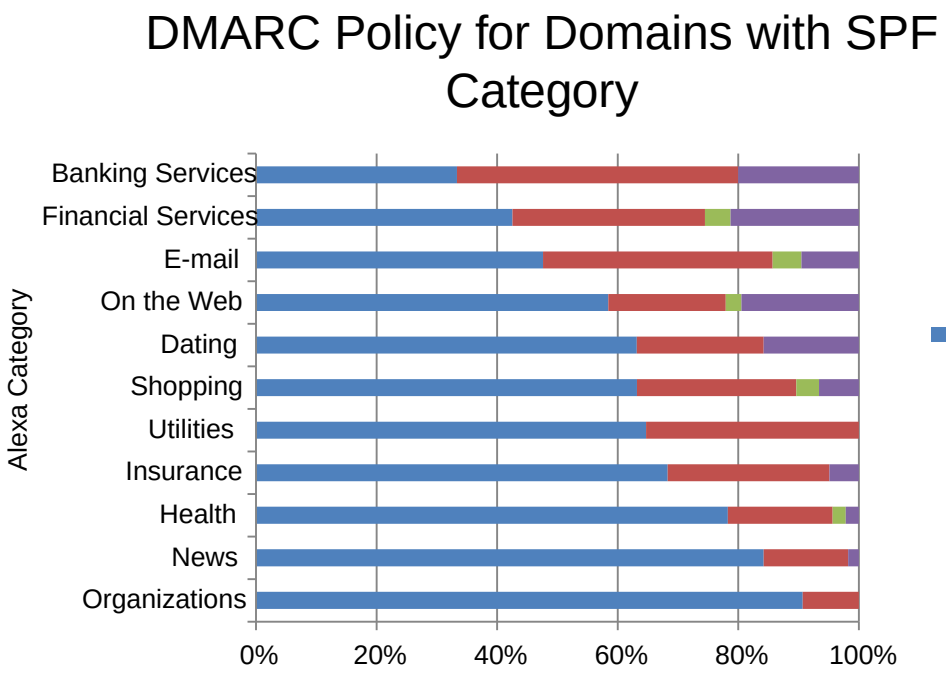
In other words, by using DMARC, a sending domain can instruct receiving email servers to block delivery of all unauthenticated messages – such as phishing messages – that claim to be from the sending domain.

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 setups 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 email servers to reject

DKIM, [10]


DMARC Policy for Domains with SPF by Category
Alexa Category
Banking Services
Financial Services
E-mail
On the Web
Dating
Shopping
Utilities
Insurance
Health
News
Organizations
0%
20%
40%
60%
80%
100%

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

Appendix - Methodology

OTechselected 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%