# Do Web Hosts Protect Their Small Business Customers With Secure Hosting And Anti-Phishing Technologies?

STAFF PERSPECTIVE | FEBRUARY 2018

## Background

During the Summer of 2017, the FTC held its first in a series of "Engage, Connect, Protect" Small Business Security Roundtables.[1] At these events, small business owners explained the challenges they face dealing with cyber threats and data security and asked the FTC for concrete advice. For many small businesses, the initial challenge they confront involves the selection of a web host and email provider. Small businesses that desire a presence on the web frequently do not have the resources or skills needed to host their own sites or to set up email accounts that use their business name as the domain name. This is especially true for businesses that are not technology-centric. A site and email accounts created and maintained by someone lacking the requisite skills may suffer from security vulnerabilities that expose the business, its customers, and others to harm such as the theft of sensitive data.

To overcome this hurdle, some companies turn to web hosting firms that market their services specifically to small businesses. These firms provide inexpensive tools and support for small businesses to establish a web presence, allowing the small business to rely on the firm's security expertise in setting up a website and email.

The FTC's Office of Technology Research & Investigation (OTech) examined the security features of hosting plans offered by web hosting services. OTech specifically reviewed the offerings of 11 web hosts that market their services to small businesses to examine the support they provide the small businesses in setting up SSL/TLS and email authentication technologies. The former helps ensure secure communication between a website and its visitors, and the latter helps prevent misuse of the small business's domain by phishing schemes. Our examination found:

- Web hosts often integrate SSL/TLS setup directly into the web site creation process, helping ensure that small businesses reap the benefits of this technology.

- Support for email authentication technologies is far less extensive: few of the hosts we examined notify users of these technologies, and several do not support some technologies.

Our findings are provided in greater detail below.

---

[1] See https://www.ftc.gov/news-events/blogs/business-blog/2017/07/ftc-small-businesses-gather-round.

## SSL/TLS

SSL/TLS is a protocol[2] that serves three primary purposes. First, it offers some assurance to a website's visitors that they are viewing the legitimate site rather than an imposter. Second, it establishes an encrypted connection between a browser (i.e., a user's computer) and a server (i.e., a website), shielding anything from credit card numbers to passwords from eavesdropping. Finally, SSL/TLS protects against modification of the information exchanged, including changes to the information so small that users are not likely to perceive them. Together, SSL/TLS adds an extra layer of security for consumers, and helps companies protect their brand and build trust with customers.

## Email Authentication

Email authentication technologies protect domains from being used in phishing scams and can be divided into two major categories. First, domain level authentication, such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), verifies the identity of the domain that an email claims to be from. For instance, these systems can be used to verify that a message that claims to be from an address @example.com actually comes from example.com's mail server. Second, using a complementary scheme called Domain Message Authentication Reporting and Conformance (DMARC), an emailing domain can instruct receiving mail servers how to handle unauthenticated messages (e.g., place the message in the "junk" folder or block the message entirely) and can tell receiving mail servers to send the emailing domain alerts whenever phishers and other spammers attempt to send messages that claim to be from an address at the domain.[3] For instance, using DMARC, example.com could instruct receiving domains to reject any messages that claim to be from an address at example.com unless the messages actually come from example.com's mail servers and could ask receiving domains to send an email to an address at example.com (e.g., DMARCreports@example.com) whenever the receiving domain received a message that wrongly claims to be from an address at example.com.

## Smaller Businesses are Less Likely to Use Email Authentication Technologies than Larger Businesses

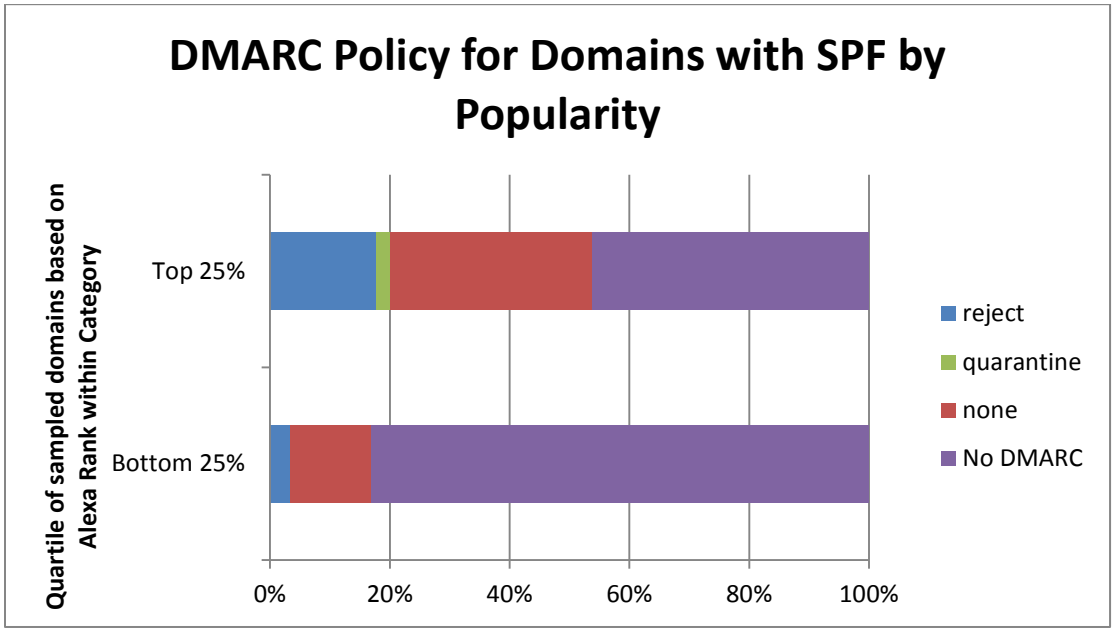
In March 2017, OTech released a Staff Perspective that examined the most popular 500+ domains' use of email authentication technologies. When analyzing the adoption rates for email authentication technologies, OTech found that domains with fewer visitors were less likely to implement anti-phishing email authentication technologies than domains with more visitors. Specifically, OTech divided the 500+ domains into four quartiles ranging from the most popular sites to the least popular sites. The more popular sites were far more likely than the less popular

---

[2] Though we use "SSL/TLS" as an overarching term to describe the protocol that facilitates secure communication properties of HTTPS, we generally mean TLS rather than its predecessor SSL

[3] See FTC Staff Perspective "Business Can Help Stop Phishing and Protect their Brands Using Email Authentication" (March 2017), https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf.

sites to use SPF. Moreover, they were significantly more likely to implement DMARC on the strictest setting (i.e., instructing receiving email servers to block unauthenticated messages). This finding motivated the present study.




Why do operators of relatively less popular domains implement email authentication less often than operators of more popular domains? If less popular domains are likely to be owned by smaller businesses that do not have significant IT budgets, could the answer lie with the types of services being offered to them by hosting providers? Furthermore, do the low implementation rates of email authentication hint at additional disparities between the security of high-traffic websites and small business domains?

# Study of Small Business Web Hosts

## Identifying Web Hosts and Reviewing Their Small Business Offerings

We identified the web hosts for our study by approaching the search for a host in the same manner that a small business might: we Googled the term “best small business web host” and then reviewed the top organic search results. These results included two sites that purported to review and rank the best hosts for small businesses, based on criteria such as the amount of

storage, types of servers, and availability of customer support. From these two sites, we compiled a list of 11 hosting firms.[4]

We then examined the support that each web host provides for SSL/TLS. For example, we determined whether the host automatically provides its customers with this security feature, offers it for an additional fee, or provides clear documentation and direct assistance on how to configure SSL/TLS in the event that it was neither integrated into the setup nor included in a plan.

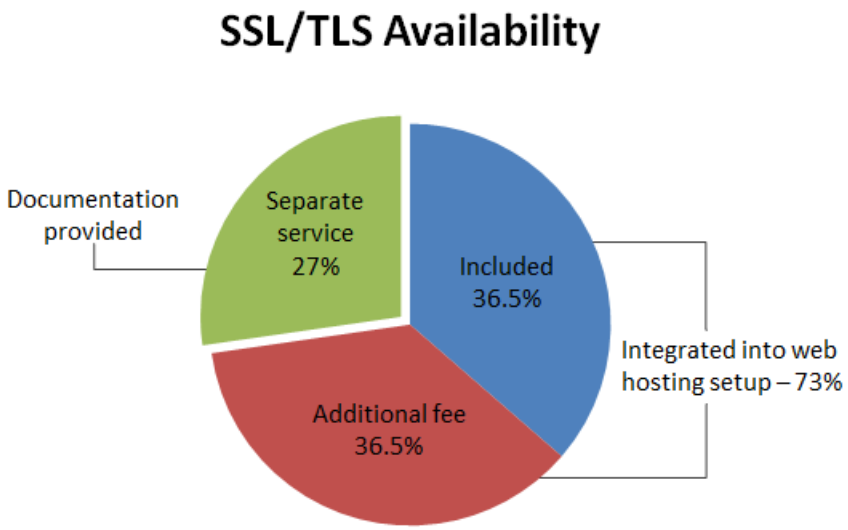
We also examined each web host's support for the SPF, DKIM, and DMARC email authentication technologies. For instance, we determined whether the host provides these by default, as an option that is readily available and simple to implement, or as an option that is available only if the small business owner is aware of the technology and searches the "help" materials on the host's website or contacts the host directly for assistance.

We gathered our data in three ways. First, we searched the help sections of the web hosts' websites. Second, on a few occasions, we obtained information by submitting questions via the "chat" feature of the hosts' sites. Lastly, in some instances we purchased hosting services, observed the hosting account and email creation process, and determined whether and how the host offered SSL/TLS and email authentication.

## The Majority of Small Business Web Hosts Offer Plans that Include SSL/TLS

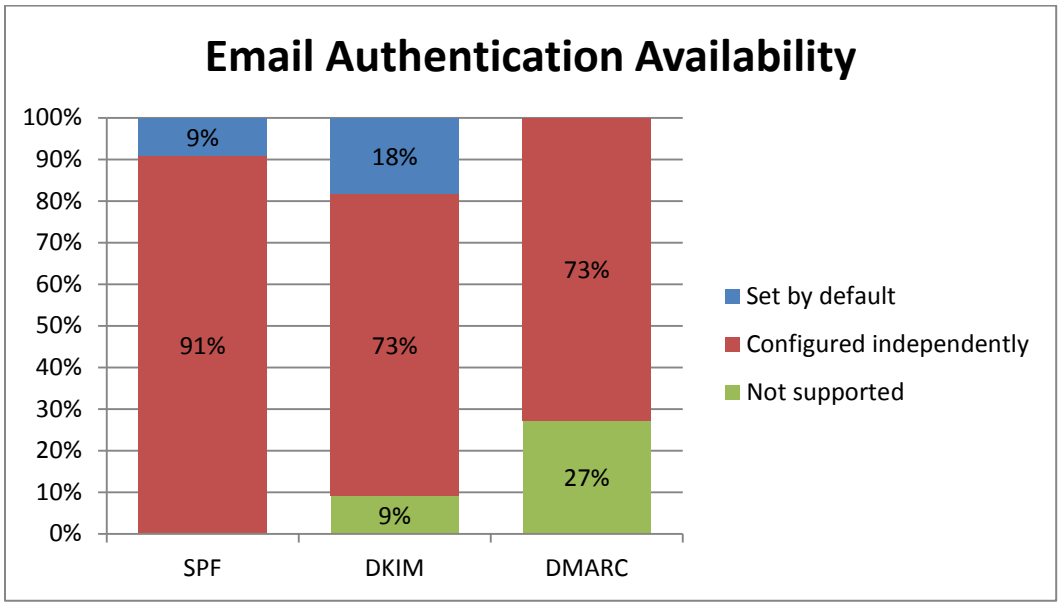
We found that 73% (8 of 11) of web hosts integrated the cost and configuration of SSL/TLS into the setup of a website. This includes 36.5% (4 of 11) of web hosts that included it in all plans, as well as 36.5% (4 of 11) that presented it as an optional add-on (for a fee) during the setup, or included it in at least one plan. The remaining web hosts provided assistance with SSL/TLS implementation as a service separate from creating and hosting a website. Rather than integrating it into the setup process, these web hosts provided documentation for businesses in the help section or on pages dedicated to marketing the feature. Nevertheless, the instructions were clear, and assistance was readily available.

[4] Our original list of top small business web hosts contained 12 hosts. We dropped one host from the study because we were unable to find relevant data on the host's website or obtain information through its customer support system.



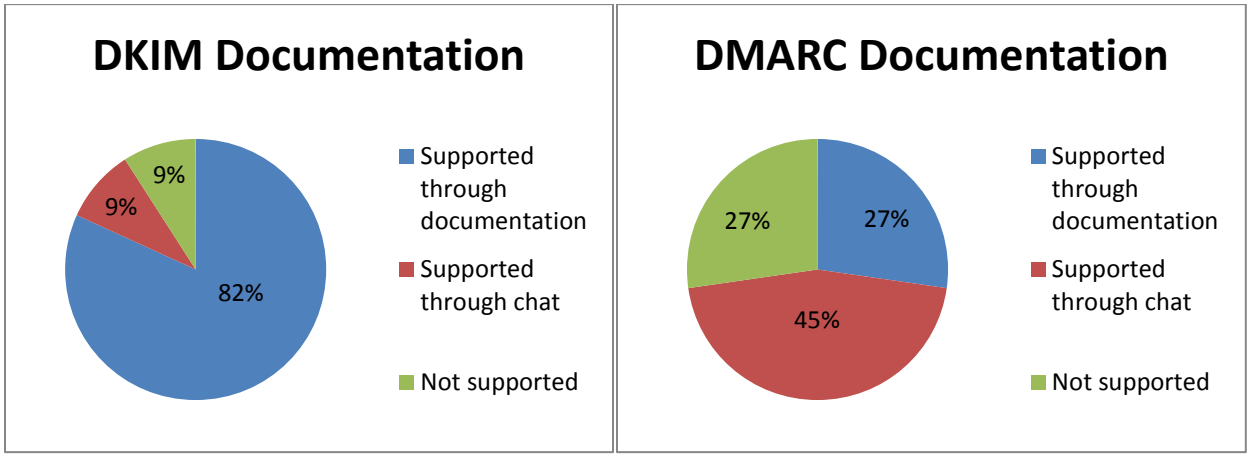

## Small Business Web Hosts Do Not Readily Provide Email Authentication Technologies that Would Protect Small Business Clients from Having their Domains Used in Phishing Attacks

Although web hosts that advertise their services to small businesses generally provide SSL/TLS, few readily provide the small businesses with email authentication and anti-phishing technologies. Of the web hosts studied, only 9% (1 of 11) implement SPF and 18% (2 of 11) implement DKIM by default. Ninety one percent (10 of 11 for SPF) and 73% (8 of 11 for DKIM) neither integrate setup of SPF or DKIM into the email account creation process, nor provide any mention of these technologies during that process. With the exception of one web host (9%) that did not support DKIM, small businesses could implement SPF or DKIM independently in these remaining cases, but the small businesses would need the knowledge to do so.



The web hosts studied provide less support for DMARC, making it unlikely that their small business clients will instruct receiving mail servers to reject unauthenticated messages, the most secure practice. None of the web hosts configure DMARC by default. Nor do any of the web hosts provide a straightforward way to configure DMARC during the email account setup process. Twenty seven percent (3 of 11) do not provide any method for configuring DMARC. For the other 73% (8 of 11) hosts, small business customers would need to have independent knowledge of DMARC and configure it on their own – something that a small business that is relying on the web host's expertise is unlikely to do.

In addition, documentation on how to fully implement email authentication protection is difficult to find on the web hosts' sites. While all web hosts provide documentation and clear instruction on how to obtain SSL/TLS and to configure SPF, some web hosts do not provide instructions on how to implement DKIM or DMARC. Although, 82% (9 of 11) of web hosts provide written instruction on how to implement DKIM, only 27% (3 of 11) explain how to configure DMARC. Instead, we had to submit questions via the hosts' support chat systems to learn about the availability of these technologies and how to implement them. The remaining web hosts did not support their small business customers' use of DKIM or DMARC.




# Conclusion

Small businesses seeking a web host should pay close attention to the security features of the hosting plans being offered. Hosting plans with SSL/TLS and with strong email authentication technologies can protect the small businesses and their customers from a variety of attacks.

Our review of the top web hosts for small businesses found that many of the hosts are helping small businesses implement SSL/TLS, with the majority of hosts integrating the process into their basic hosting plans or offering them as straightforward options for an additional fee. Web hosts should consider the significant benefits of SSL/TLS and determine whether offering web security as part of all plans they offer by default outweighs the costs associated with providing small business customers with SSL/TLS.

Unlike SSL/TLS, small business web hosts have not embraced email authentication, leaving small businesses at risk of having their domains used in phishing attacks, harming their business reputations and potentially causing financial harm to their customers. Web hosts that cater to small businesses can play a significant role in increasing the adoption rates for SPF, DKIM, and DMARC by automatically configuring these technologies for their small business customers. These technologies are all free to use and implementation costs for web hosts are likely to be minimal.

Finally, sites that purport to identify the best web hosts for small businesses can also help improve the level of web site and email security hosts provide. The sites that we used to identify web hosts for our study purported to rank hosts using a variety of factors, such as amount of storage, type of servers, and availability of customer support. The ranking criteria did not, however, include the availability of SSL/TLS or email authentication technologies. By adding security issues to the ranking factors, the rating sites could help encourage small businesses to take security into consideration when selecting a host.

# Contributors

## Division of Litigation Technology & Analysis

### OFFICE OF TECHNOLOGY RESEARCH & INVESTIGATION (OTECH)

Tina Yeung
Dan Salsburg