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: Our findings are provided in greater detail below.

[1]

SSL/TLS

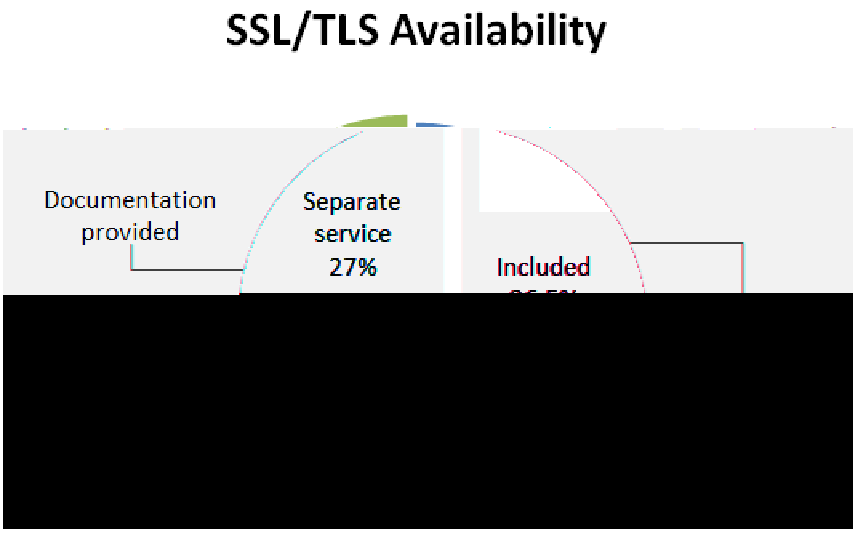
SSL/TLS is a protocol[2] that serves three primary purposes. First, it offers some assurance to a website's visitors that they are viewing the legitimate site rather than an imposter. Second, it establishes an encrypted connection between a browser (i.e., a user's computer) and a server (i.e. a website) 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

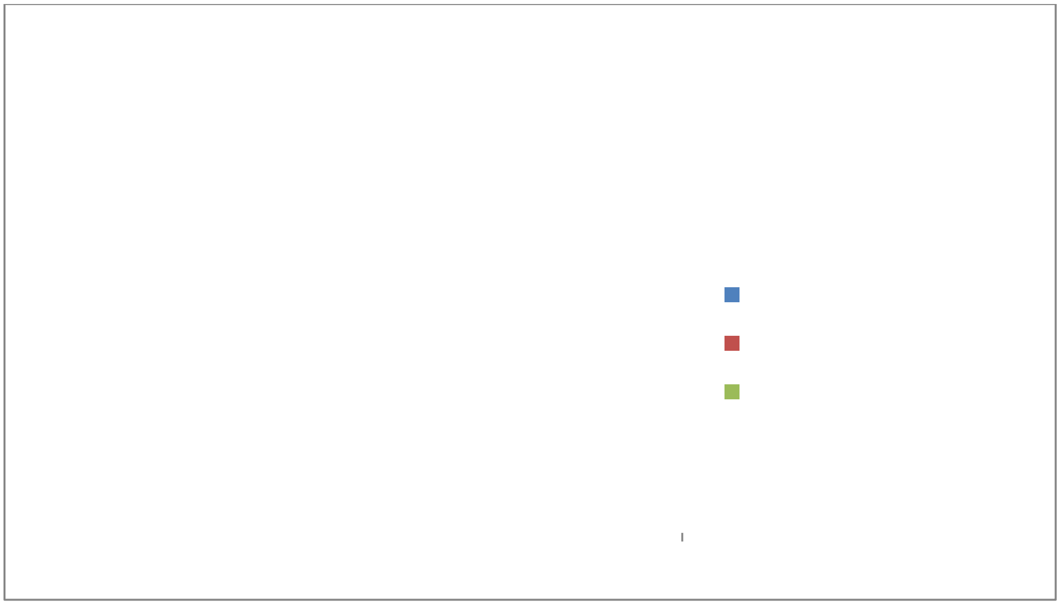
Email authentication technologies protect domains from being used in phishing scams and can be divided into two major categories. First, domain level authentication, such as Sender Policy Framework (SPF) and

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


SSL/TLS Availability
Documentation provided
Separate service 27%
Included

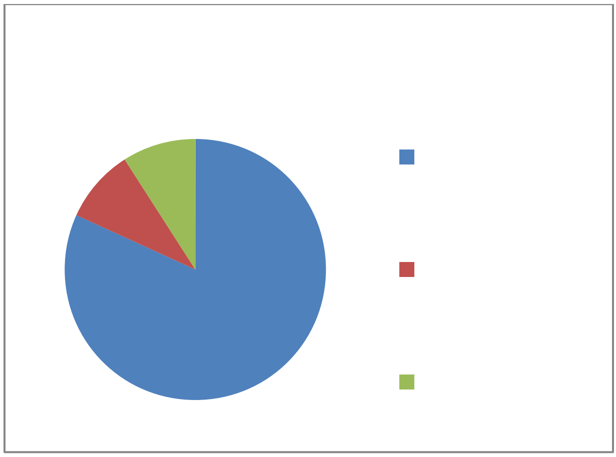
Small

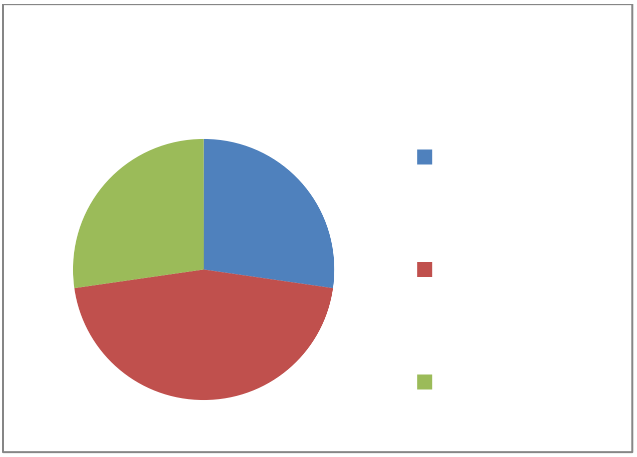

🟦
🟥
🟩

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 protocols 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

cos1(5 0.5.00r co)o Tc m 4 1Tca v Tc a-2(t)r-0.004 04et5 16 0 155.9 4 fb (M9(at.004t.004ack2





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