Website Hosting - Is The Security Adequate

Posted At : March 27, 2019 3:31 PM | Posted By : Admin
Related Categories: Internet

The Computing Center hosts websites and has done so for over 20 years. We're defintely NOT the least expensive, our clients choose us for our security and reliability. We also offer everything that's listed in the article from the FTC.

by Andrew Smith, Director, FTC Bureau of Consumer Protection

Your website is the online face of your business. Some companies have the in-house capability to manage their web presence. Others hire a web host to handle it for them. When launching a new business or upgrading their site, savvy business owners comparison shop for web hosting services. At the top of your shopping list should be the security features built into what you're buying.

In our meetings with small business owners across the country, you asked for more advice on selecting a security-conscious web host. As part of our **cybersecurity initiative for small business**, the FTC has suggestions about what to look for and what to ask when hiring a web host.

What To Look For

Transport Layer Security (TLS). The service you choose should include TLS, which will help protect your customers' privacy. TLS helps make sure people looking for your business online reach your real website when they type your URL into the address bar. When TLS is up and running on your site, your URL will begin with https. TLS also helps make sure the information sent to your site is encrypted – an important feature if you ask customers for sensitive data like passwords or credit card numbers.

Email authentication. Some web host providers let you set up your company's business email using your domain name. Assuming your domain is yourbusiness.com, that means your email might be yourname[at]yourbusiness.com. Without email authentication, scammers can send emails that look like they're from your company. A key defense against fraudsters is a web host that provide three essential email authentication tools:**Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC)**.

Software updates. When it comes to creating a website, you're too busy to start from scratch. That's why many web hosts offer pre-built templates or ready-to-go software packages. But cyber risks are constantly changing. Be sure you know how you or your web host provider will keep your site's software up to date, including the installation of the most recent security patches.

Website management. If it's necessary to make changes to your site, will you have to go through your web host or is there an option of managing it on your own? Make it clear from the start who will manage the site after it's built.

What to Ask

When you're in the market for a web host provider, make it clear that security matters to you. Here are some questions to ask a prospective web host to gauge if you're on the same security page:

- Is TLS included in your hosting plan? Is it free or offered as a paid add-on? Will I set it up myself or will you help me?

- Are the most up-to-date software versions available with your service? Will you keep software updated? If it's my responsibility, how do I do that?
- Can my business email use my business website name? If so, can you help me set up SPF, DKIM, and DMARC email authentication technology? (For in-the-know business owners, those three tools are musts. No SPF, DKIM, and DMARC? No deal.)
- Once the website is up and running, what if changes are needed? Will I have to go through you? Can I log in and make changes on my own? If I can log in, is multi-factor authentication available?

Download the FTC's **web host fact sheet** and keep it handy as you comparison shop.