Five Things Your Web Host Won't Tell You!

A Special Report

Knowing the right questions to ask will make your website more secure in the long run!!

The HelpDesk LLC

You are busy! You need a reliable web hosting service. A service that never crashes, has sufficient storage, easily handles your traffic capacity, and support is fast and efficient. Everyone and their brother is offering web hosting these days--for cheap! What's the difference in all those services?

If you're not a "nerdy-geek" type you won't know. Currently the web hosting market is a buyer beware environment. Everyone sells on price because they're going after volume. So, what you see offered and described is not always what you get.

This report was written for you. It's purpose is to equip you with enough simple information to know the questions to ask when purchasing web hosting services. If you know the right questions, you will know what you are buying and what to expect.

Much of what we describe here for you is either buried in the fine print on the web host's site or simply unspoken and assumed.

5 Things Your Web Host Won't Tell You

1. Unlimited Isn't Really Unlimited

"Unlimited" has become a popular word in web hosting ads. We all got used to unlimited minutes in the cell phone world. Then it quickly became popular in the web hosting world. In short, it's a marketing ploy. The truth is that unlimited traffic, disk space, etc. is not really unlimited. Providers are simply doing the math to see how much space the average user utilizes and then calculating their rates based on that usage. If you dig around in the fine print you discover that there really is a limit and when you reach it the host provider will take steps to either charge you more money or boot you down the road.

If your only need is a single personal web page for two dollars per month, then unlimited will probably be OK for you. But, if you are a real business with merchant activities, a database or real time transactions, then you will want to ask more questions about your space and traffic requirements.

2. Security Is <u>Your</u> Responsibility

You won't see security discussed much in web hosting ads and promotions. The fact is, most web hosting providers offer nothing in the way of protecting your site from hackers and attacks. If you read the fine print you will find that they specifically say they are not responsible for the applications that run on your site. A few providers offer scanning services that check for "ways in" to your site. These are OK, however you should expect to pay for that protection. The bottom line is

that the applications and activities that run on your site must be protected by you.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks Are Prevalent And Increasing

Unfortunately there are people in the world that have nothing to do except figure out ways to attack your website. The way they go about this is rather sophisticated and involves establishing large networks of computers that act as "zombie" or "robot" computers. Once established, this unsuspecting "botnet" army of computers unleashes an attack on a specific website. That site could be yours. If your organization has enemies or folks that would like to see your activities harmed in some way, then you will want to learn about DDoS protection. Most providers do not offer this protection, because it requires expensive and sophisticated traffic monitoring hardware, software and specialized skills.

4. Two DNS Servers Are Not Adequate Any More

Back in the day, service providers offered two DNS servers, typically on one server that also provided web site services. Today many small hosting providers still follow this same model. The problem comes when and attack occurs. Any of these three key business components: e-mail, website or DNS can come under attack. Under the old model, if any of the three are attacked, the other two will also be harmed and probably come down. When that occurs, the chances are your business will be severely harmed. The solution in today's threatening environment is to increase the number of DNS servers.

A current solution is to use AnyCast routing. In an AnyCast system all DNS servers are simultaneously monitored. If a given server in the system fails, it is bypassed in the system to assure reliable service for end-users. You will want to be sure your provider has reliable DNS services.

5. A Firewall Is Not Sufficient Protection From Attacks

The best way to think of a firewall is that it opens and closes doors to allow traffic to flow through. It does not look at the traffic to determine what kind of traffic is flowing through. Today, many applications run entirely over a single port: 80. To avoid damage to your business applications that are running on your website, you will need to use a host provider that can protect your site. The protection requires an investment in specialized hardware and software that most hosting providers either cannot or will not make. Such hardware can monitor traffic on all ports and "look into" the traffic on port 80. Then, when unwanted malicious traffic is attempting to infect your website, the specialized equipment alerts security personnel of the attempt so that it can be stopped.