

The Wireless Web: Are You Sharing Your Client's Data?

Article Rating: NA

Submitted by: articlediner on 2006-11-29 and viewed 26 times.

Total Word Count: 901

Author Rating:

Sample of Content:

Are you wireless? Should you be? Does it matter?With wireless capabilities being built into every newlaptop under the sun, the internet is quickly becoming analways-on, always accessible way of doing business.So what does that mean for you then?Learn how to protect your client's data and make sure wireless technology translates into added value for your business.

Content:

Are you wireless? Should you be? Does it matter?

With wireless capabilities being built into every new laptop under the sun, the internet is quickly becoming an always-on, always accessible way of doing business.

So what does that mean for you then?

Well, I don't need to tell you the value of being able to communicate with your clients from anywhere, at anytime. (Of course, we all have the power to choose just how accessible and available we are to our clients, but I digress...)

The real power of a quick email reply to an urgent client request from your wireless device of choice is this: it makes your client feel VALUED and IMPORTANT. It is a feeling we all live for. Delivering that feeling to your clients will do more for increasing your profits than many other activities.

That's the power of wireless.

Want to go wireless? Here are some basics. Much of this is not stuff you need to remember, but just information to help fill out your understanding:

*Wireless networks have flavors. There aren't many, but most wireless networks are one of three types, which are labeled by the letters a, b, and g. The differences are quite technical. In short, A and B are pretty old and G is the newest and the fastest. End of story.

*Wireless networks have names. These network names have been given the techie acronym SSID, which stands for Service Set Identifier. When you sit down at your laptop and pull up the list of wireless networks in the area, the names in that list are, you guessed it, the SSIDs. Please don't bother to remember this acronym, you most likely won't need it again.

*Wireless networks can have extra security. This extra security comes in the form of encryption. Just like the technology used to protect your data when logging on to your bank accounts online, wireless networks can be (and should be) ENCRYPTED to protect your business data.

*New laptops are wireless ready. Most every new laptop comes with wireless access built in. No additional hardware or software is required. For older laptops, however, you will need a small wireless card that can be purchased for anywhere between \$15.00 and \$100.00 at your local computer store.

While wireless internet access provides many, many benefits to you and your business, there is a dark side...

As internet access becomes more and more interwoven into the business landscape, internet SECURITY, will become more and more of a priority.

Wireless security is not only something for the tech world to worry about. When dealing with private client data (which we ALL do), it is in your best interest to understand what you are dealing with. Don't worry, it's just a matter of understanding a few simple ideas and then applying them to protect yourself.

By default, most wireless networks send everyone's data flying through the air unprotected. If you have the proper tools (which are easily downloadable from the internet), you can pluck that data straight out of the air.

The wireless access at your local coffee shop or library is most often this type: completely unsecured and open to prying eyes. Yes, even Starbucks lets your data fly through the air, available for all.

So enough scare tactics...

The only word you have to remember when it comes to protecting yourself and your data is ENCRYPTION.

A good rule of thumb: If a wireless network is not encrypted, DON'T connect to it.

Some might say this is a bit paranoid. To that I might say, "Should my clients expect anything less?"

It is one thing if you are a college kid sitting at a coffee shop sending messages back and forth between your friends. It is quite another when you are preparing a legal brief or some other piece of confidential information that will be sent to your client.

So how do you tell if a wireless network is encrypted?

Simple...

If you need a password to connect, it is encrypted. If no password is required, you are operating in the open with no protection whatsoever.

There are various encryption strengths, some suited for your basic office environment and some more suited for even more confidential situations, like a doctor's office.

At this point, the important thing is not so much the strength of the encryption as much as whether or not you have it at all. Most would-be internet thieves (no, that is not their technical name), upon seeing an encrypted wireless network, will move on the thousands and thousands of easier targets with no encryption.

The bottom line:

The benefits wireless internet access bring to your business are too numerous to count. If you aren't "wireless" yet, look into it. If used properly, it can add heaps of value to the service you offer your clients.

Once you go wireless, you owe it to yourself, your business and your clients to be knowledgeable enough to protect your data from theft.

Hi. My name is Jason Leister. I have been helping people do productive things with computers and technology for longer than I can remember.

I started Computer Super Guy, LLC because I love business. In particular, I love helping others make their businesses GROW.

Now when I say business, I am talking about passionate businesses, that stand for something and are creative expressions of their owners.

If that sounds a bit mushy, or a bit too touchy-feely, well, I'm not sorry. It's what I believe and it is what I live.

And it is why you will benefit from working with my firm.

Article Source: <http://www.ArticleDiner.com/>

About the Author:

Jason Leister