



WIRELESS CONNECTIVITY - BEST PRACTICES

WIRELESS NETWORKING AND CONNECTIVITY MAKES IT EASY TO ENJOY THE INTERNET OR EMAIL ON THE MOVE. WHILE WIRELESS MEANS GREATER FLEXIBILITY AND MORE PRODUCTIVE MOBILITY, IT CAN ALSO ENTAIL RISKS. WE OFFER SOME TIPS FOR MAKING SURE THAT YOU ENJOY OPTIMAL SECURITY ALONG WITH ALL THE BENEFITS OF WIRELESS CONNECTIVITY.

BEST PRACTICES

1. Exercise the same amount of caution in the wireless world as you would the wired. Do not open or respond to questionable emails and look for secure (https) connections. Frequently change passwords to your computer, network connections, email programs and files.
 2. Public “hotspots” offer a less controlled environment with unknown computers sharing one local network and often, lower security settings to allow everyone easy access to the network. Protect yourself by looking for a sign indicating a legitimate provider such as “Wayport” or “tmobile” and check the list of SSIDs to ensure you are connected to the correct one.
 3. Look for providers that have software clients that encrypt your information before sending it over the Internet. Unless you are using a secure site (https), any information you send across the network such as your login, password or credit card information is often sent from your notebook to the access point in plain text, making it clearly readable to anyone intercepting the information! With the number of rogue access points and phishing scams growing, this is a real concern. To protect yourself from this type of crime, you can download freeware and shareware encryption programs that allow you to password-protect sensitive information such as an important file sent in an email. Programs such as Allume’s Stufft Deluxe can help.
 4. Look for hotspots making use of WPA security which automatically ensures the network uses authentication. Only log in to known hotspots using a secure sockets layer (SSL) (https) connection. To be certain of the secure connection, check for the digital certificate on the login page through Internet Explorer by selecting File, Properties, and Certificates.
 5. The most secure way to use a wireless network is by using a virtual private network (VPN) connection. A VPN creates an impenetrable tunnel, a private network, from your computer directly to the network allowing you to securely send and receive email and access files. VPN cards are often distributed by corporations to allow employees to securely access company files and email programs. But if you don’t have a company VPN you can be just as secure by using programs such as JiWire SpotLock. JiWire SpotLock’s IPSec VPN is supported by almost all public and private wireless routers and includes full Wi-Fi connection management.
-



6. Protect your home wireless network by enabling WPA or WPA2 security provided on all Wi-Fi certified products. This, on its own, is not enough. You must configure the security keys on the access point/router and each client to enable security. **Note:** The security is off by default in most Wi-Fi products so you need to turn it on.
7. Disable your wireless card unless you are using it. Your Toshiba notebook has a wireless switch to quickly accomplish this. If your wireless connection is not engaged, hackers can not access your computer. Check that your wireless card is not set to connect automatically to any available network and turn off the ad-hoc mode that allows others to connect directly to you.
8. A firewall monitors incoming and outgoing traffic on your computer. This protects you from outside intruders trying to access your computer. In a hotspot a firewall is particularly useful as the machines sharing the same network as you are (the same subnet) are more easily able to intercept information from and access your computer than other computers on the Internet. If a Trojan Horse is trying to access your system your firewall will alert you to the unusual communication attempts.
9. There are many free personal firewalls for you to use. Zonelabs ZoneAlarm, Kerio's Personal Firewall and the built-in Windows XP Firewall are all good ones to use. If your notebook is a corporate computer, consult your company IT first and buy a license. Take the time to learn and configure your firewall properly for the most protection, but the least interference with regular traffic. Commercial personal firewalls are available from McAfee and Symantec.
10. Look for Wi-Fi certified products because this means these products have passed rigorous and stringent interoperability testing and are certified for WPA and WPA2 security. These security settings ensure data remains private and access to the network is restricted to authorized users.
11. Install anti-virus software on your notebook for added protection from viruses or malicious code to which your computer is vulnerable in a public network. It is worthwhile taking the time to regularly check vendors' web sites for the latest download as many new threats emerge each month.
12. Turn off the file sharing option on your computer. This option is usually on in a home network to allow you to easily open or copy files from one computer to another computer. In a public network, this option leaves all of your private files and folders open for all to access. You can either disable the Simple File Sharing option (which is on by default in Windows XP) when you are at a hot-spot, or configure your system to share files selectively, with authorized users only, by setting up permissions for shared folders.

**LINKS TO HELPFUL RESOURCES**

- Wi-Fi alliance
<http://www.wi-fi.org>
- Toshiba wireless products
http://eu.computers.toshiba-europe.com/cgi-bin/ToshibaCSG/generic_content.jsp?service=EU&ID=ONLINE_SHOP
- Allume Stufft Deluxe
http://www.digitalriver.com/dr/v2/ec_MAIN.Entry17c?PN=5&SP=10007&SID=1839&PID=704491&CID=160413&CUR=124&DSP=&PGRP=0&ABCODE=&CA CHE_ID=160413
- JiWire SpotLock
<http://www.jiwire.com/spotlock.htm>
- Zonelabs Zonealarm
<http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp?dc=12bms&ctry=US&lang=en>
- Kerio Personal Firewall
http://www.kerio.com/us/kpf_download.html
- Microsoft XP File Sharing
<http://support.microsoft.com/default.aspx?scid=kb;en-us;307874>
<http://support.microsoft.com/default.aspx?scid=kb;en-us;304040>