IT@Intel Technology Tips

Intel Information Technology
December 2010

Intel IT creates and publishes articles for Intel employees to educate them on a variety of information technology subjects. Our goal is to help them improve productivity, take advantage of new IT services and raise awareness on other IT topics of interest. We've modified these articles from their original version for sharing with external audiences.

Nine things you should never do while on a Wi-Fi hotspot

A few preparations can go a long way toward warding off cyber crooks

We all appreciate being able to stay connected when we are away from the office. Whether we are traveling for vacations, off-site meetings and other away-from-work excursions, we can still do so with a smile, serene in the knowledge that thanks to Wi-Fi hotspots, the Internet and e-mail are only a few clicks away.

But not so fast. These often-free Internet access ports can be found everywhere from airports and coffee shops to public libraries, gas stations, and hotels and they offer many benefits in terms of flexibility and improved productivity for Intel employees. But they are not all safe to use. There are serious security risks to company and personal data. If you're not careful, you can leave your PC wide open to hackers and other cyber villains.

Here are some precautions to take whenever you access public Wi-Fi that can keep your computer and its information safe from unwanted eyes.

Check before you connect

Due to the number of locales offering Wi-Fi now (approximately 75,000 Wi-Fi hotspots in the U.S. and 300,000 worldwide by the start of 2011), a routine connection attempt from your local hotspot may bring up a half dozen (or more) possible networks. Be extremely cautious here – hackers often set up networks with names such as "Free Wi-Fi Hotspot" to nab unsuspecting users. In addition, a legit public Wi-Fi site will ask you to log on to a Web page before you can complete the connection. If the network or Web page doesn't match your locale – such as a generic "Free Wi-Fi Here" page from your favorite coffee shop site – confirm the site name with someone at your location, preferably an employee. Better yet, have that person connect you.

Consider using VPN when connecting corporate laptops

Some corporations require their employees to use Virtual Private Network (VPN) to ensure maximum data encryption when connecting company laptops to external Wi-Fi hotspots. Check with your IT department for their requirements.

Pick the most secure network

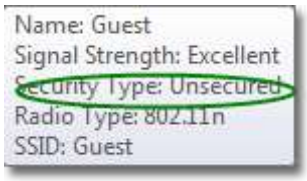

Figure 1: Avoid using unsecure networks unless you have no choice.

Many hotspots are unsecured, but some from more well-known providers do offer encrypted networks. If you have a choice, choose the latter. You can tell which networks are secured in Windows 7* by left-clicking on the wireless network connections icon in your system tray. Hovering the mouse over each SSID will display the security type. Avoid networks with the security type "Unsecured," if possible (see Figure 1). In Windows XP*, secured network SSIDs are displayed with a lock when you click open wireless network connections. In either case, you will need a password key for access, or you'll need to agree to a Terms of Use statement on the provider's Web site. In order of preference, choose networks secured with WPA2 encryption (see Figure 2), then WPA. WEP is a better-than-nothing last resort.

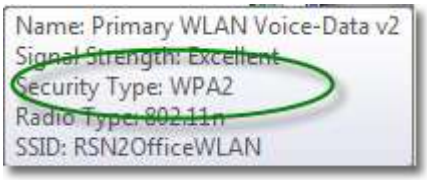

Figure 2: Networks with WPA2 encryption have the highest level of security against hackers.

Remember to update security

Keep anti-virus and anti-spyware programs up to date. These protect you against most cyber attacks.

Don't mess with your firewall

Most company-provided laptops have a preset, activated firewall in your laptop to prevent easy outside intrusion by hackers. Do not shut this off. In other cases, Microsoft Windows operating systems have a built-in personal firewall installed and switched on. This should be used unless you install a more-powerful firewall via third-party software vendor. To check and adjust your firewall status, go to Control Panel > System and Security/Security Center > Windows Firewall (see Figure 3).

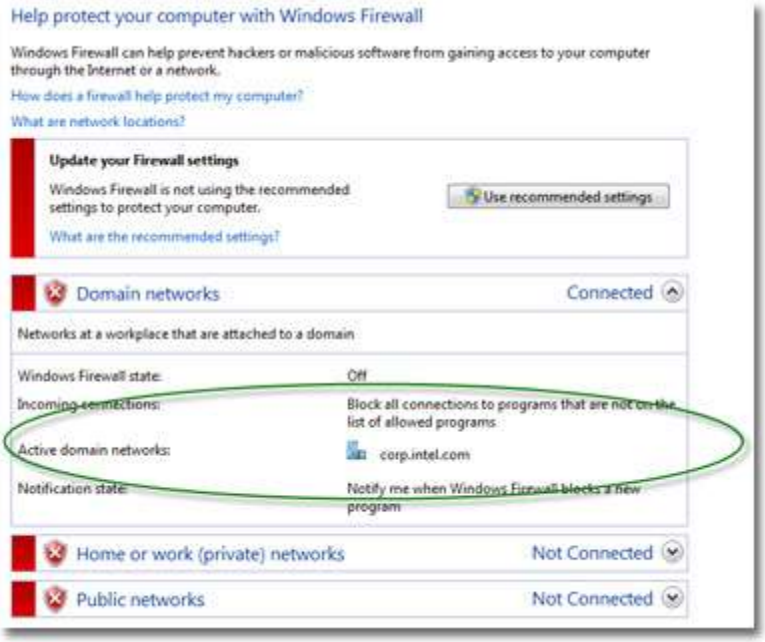

Figure 3: Windows computers have a built-in firewall that should only be turned off if you have a better third-party version installed – or if you're using an Intel computer with its own firewall setup.

Avoid transmitting personal information

Because of the low level of encryption, if any, at Wi-Fi hotspots, beware of the types of information you might transmit through a laptop or cell phone. Assume that what you will transmit will be read by a third party. Save logging into e-mail, bank and credit card accounts, and the making of online purchases, for times when you're fully protected. If you must do it, use only Web sites with addresses that start with "https" (or that send you there during your visit). While not perfect, these sites are far more secure than the basic "http" variety. During commercial transactions, look for a small padlock at the bottom (Windows XP) or next to the address line (Windows 7) indicating a commercial transaction is secure.

Don't save passwords

Web sites and browsers are forever asking if you want to save and store passwords. A general rule of thumb: you're probably better off not storing your username and password anywhere, especially when it comes to banking sites and the like. That goes double for road warriors or travelers who frequently connect via public Wi-Fi.

Secure your public folders

Computers have public folders—such as shared music, pictures, and video locations—that are easily available to anyone on the same network. Don't keep anything personal in those folders. Better yet, don't have any folders that are designated as sharable.

- In Windows XP, right-click on a folder, select **Properties > Sharing and Security** and make sure **Do not share this folder** is selected.
- In Windows 7, right-click on a folder, highlight **Share with** and make sure **Nobody** is selected.

Hide sensitive folders

Firewalls and various anti-intrusion software work well, but you can also hide your folders. This is not the strongest of security defenses, but it does make it that much harder for intruders to readily see sensitive data:

- Right-click on a folder and select **Properties**.
- Under the **General** tab, set the folder's attributes to **Hidden**.

Decide whether you want the Hidden status to apply to only the folder, or to all folders and files inside the folder as well (this will appear the first time you attempt to hide a folder). Click **OK**.

The folder should completely disappear, effectively invisible. If it turns transparent, you have another series of steps to perform:

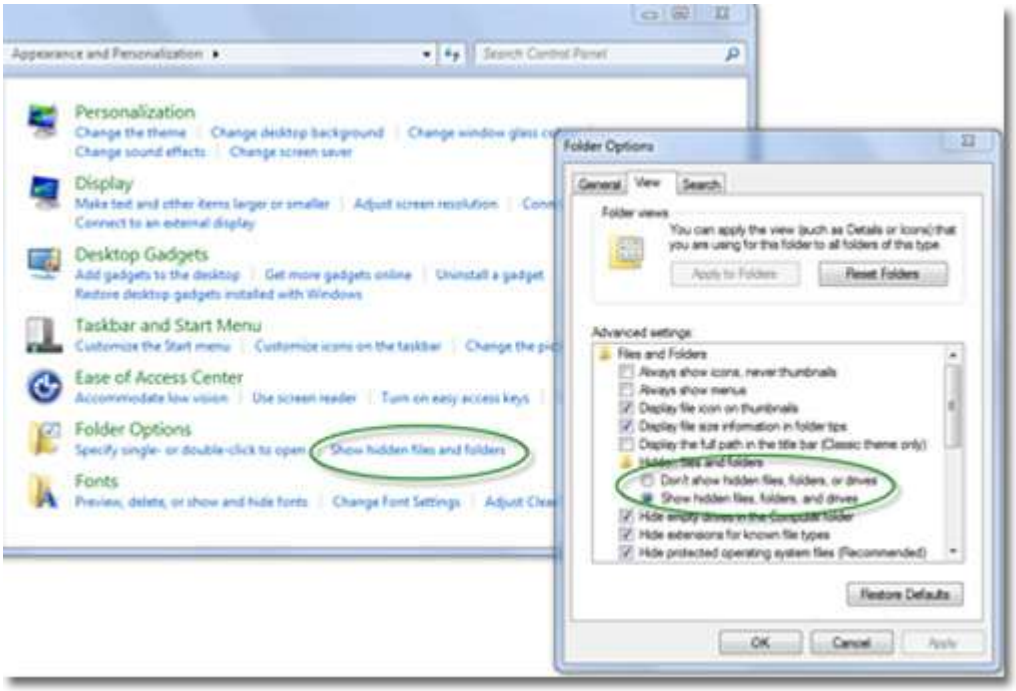

Figure 4: Hiding sensitive folders can make it harder for hackers to see files on your machine.

- Go into Windows Explorer's **Control Panel > Appearance > Folder Options > Show hidden files and folders.**
- From here, under **Advanced Settings > Hidden files and folders, choose Don't show hidden files, folders or drives** and click OK (see Figure 4).
- Transparent folders, and all future hidden folders, will turn invisible.

To restore the viewing of hidden files and folders, repeat the second series of steps, but choose Show hidden files, folders and drives. Any hidden folders will appear transparent, as noted above.

To restore a transparent folder, right-click again on the folder, select Properties and uncheck the Hidden status.

Remember that with just a few precautions, you can make connecting away from the office a safer experience.

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.

Printed in USA Please Recycle 1210/JLG/PDF