TAKE A BITE OUT OF CYBER CRIME®

www.bytecrime.org

CYBER SAFETY CHECKLIST

Wireless Networking & Public Computing Tips

Home Networking Equipment: Broadband Routers, Wireless Access Points

□ **Change the default name of your network –** All home networks come with a default SSIDs (Service Set Identifiers). They're available to everyone on the Internet, so change your SSID to a name you'll know but others won't. Set your system not to broadcast the SSID.

□ **Use a hardware-based firewall –** Buy a broadband router that includes a built-in firewall, even if your broadband provider doesn't include one with the service package. This simple control protects you from the constant torrent of malicious traffic on the Internet.

□ **Secure your wireless network with WPA or WEP –** All major brands have either WPA (Wi-Fi Protected Access), which is best, or WEP (Wired Equivalent Privacy) for security. Enable one of these security features.

□ **Apply latest firmware updates –** Updating network equipment always seems to be missed when it comes to security of the home network. Keep your firmware current and you can better protect computers and devices connected to your home network.

□ **Change default administrative passwords –** Just like default SSIDs, default passwords are available on the Internet. Change yours to keep unwanted people out of your home network. And remember, a good password is one that can not be easily guessed.

□ **Turn your gear off when not in use for extended periods of time –** If you only use your home network for a few hours a day, keep your gear powered down. Aside from being energy efficient, this reduces your exposure to Internet-based threats and people who might want to borrow your broadband connection.

□ **Review who's using your network –** Many newer devices keep track of what systems are connecting to your gear and what they're doing. If you see something unusual, consult with someone you trust who can help you understand the activity.

Public Places

□ **Don't leave valuable hardware unattended –** Coffee shops, wireless hotspots and public places are prime targets for thieves. Unless someone you know and trust has agreed to watch your system, take it with you. The hassle of packing it up is a far less than the loss of the system and the data contained on it.

□ **Security in the car –** A car seat is never a good place to leave a laptop or mobile device. If you must leave a device in the car, put it in the trunk or the glove compartment, or hide it under the seat. If possible, secure your device out of sight before you arrive at a public parking lot.

□ **Watch out for "shoulder surfing" –** Some people will spy on your screen from behind you. Be conscious of your surroundings and consider using a privacy screen, a thin plastic cover for your laptop screen that hides it from others.

□ **Use care when entering passwords on your laptop –** Be aware of your surroundings and make sure nobody is watching what you type.

□ **Be VERY careful using public networks –** Remember that hackers can tap into wireless signals much more easily than they spy on wired networks. So when using public networks, use virtual private network (VPN) software to secure your communications. If you can't use a VPN, then avoid entering any personal information, including credit card data.

□ **Securing email on WiFi networks –** If you're going to be using email on a public WiFi network, be sure that your email login and email transfer program uses Secure Socket Layer (SSL) encryption. Your email program provider can help you with set up.

NATIONAL CRIME PREVENTION COUNCIL · CMO COUNCIL · FAME · comcast · intel · McAfee · VeriSign · Walmart.com