Wireless Network Security

Wireless Internet access can offer convenience and mobility. There are steps that can be taken to protect a wireless network and the computers on it. The steps discussed below are recommended by the Federal Trade Commission (FTC). The tips are designed to help businesses be on guard against Internet fraud, secure their computers, and protect customer and employee personal information.

Use Encryption

Encryption scrambles the information a worker sends over the Internet into a code that it is not accessible to others. Using encryption is the most effective way to secure a company network from intruders.

- Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). The company computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only WEP encryption, which may not protect your company from some current common hacking programs. Consider buying a new router with WPA2 capability.
- Wireless routers often come with the encryption feature turned off. This must be turned on. The directions that come with the router should explain how. If they do not, check the manufacturer's website.

Secure Computer and Router

- Most wireless routers have a mechanism, called identifier broadcasting. Turn it off so your computer will not send a signal to any device in the vicinity announcing its presence.
- Change the identifier on your router from the default so that a hacker cannot use the manufacturer's default identifier to try to access your network.
- If the firewall was shipped in the "off" mode, turn it on.
- Change the pre-set password of the router for administration to something more secure and only known to those who have a need to know. The longer the password, the tougher it is to crack.
- Allow only specific computers on your wireless network. Set the router to allow only devices with particular Media Access Control (MAC) addresses to access the network.
- Use anti-virus and anti-spyware software and keep them updated.

Limit Access To Network

- Allow only specific computers to access your wireless network. Every computer that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access the network. Some hackers have mimicked MAC addresses, so do not rely on this step alone.

- Turn off your wireless network when you know you will not use it. Hackers cannot access a wireless router when it is shut down. If you turn the router off when you are not using it, you limit the amount of time that it is susceptible to an intrusion.

Use Precautions When Accessing Public WiFi Networks

- Be cautious about the information you access or send from a public wireless network. Many cafés, hotels, airports, and other public places offer wireless networks for their customers to use. These "hot spots" are convenient, but they may not be secure.
- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you are logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Do not stay permanently signed in to accounts. When you have finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to one of your accounts access to many of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up to date.
- Consider changing the settings on your mobile device so that it does not automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.
- If Wi-Fi hotspots are regularly accessed, use a virtual private network (VPN) on the company's computers/servers. VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. VPN options are available for mobile devices, and they can encrypt information you send through mobile apps.
- Installing browser add-ons or plug-ins can help. For example, there are add-ons that force a browser to use encryption on popular websites that usually are not encrypted. They do not protect you on all websites — look for https in the URL to know a site is more secure.

The information, suggestions and recommendations contained herein are for general informational purposes only. This information has been compiled from sources believed to be reliable. Risk Consulting Services do not address every possible loss potential, law, rule, regulation, practice or procedure. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any such service. Reliance upon, or compliance with, any recommendation in no way guarantees any result, including without limitation the fulfillment of your obligations under your insurance policy or as may otherwise be required by any laws, rules or regulations. No responsibility is assumed for the discovery and/or elimination of any hazards that could cause accidents, injury or damage. The information contained herein should not be construed as financial, accounting, tax or legal advice and does not create an attorney-client relationship.

This document is not intended to replace any recommendations from your equipment manufacturers. If you are unsure about any particular testing or maintenance procedure, please contact the manufacturer or your equipment service representative.

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange. Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this document.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.