Beyond the expected.®
PEKIN® INSURANCE

AGENCY OFFICE SECURITY GUIDELINES

Version 1.5 – May 2013

Introduction

As a courtesy to independent Pekin Insurance agents, the Pekin Insurance Enterprise Security Team has developed a set of guidelines to help minimize the risk to independent Pekin Insurance agency networks. This document provides recommended best practices that can be used to help protect the confidentiality, integrity, availability, and privacy of Pekin Insurance information. This includes, but is not limited to Personally Identifiable Information (PII), and Electronic Protected Health Information (ePHI), along with the systems and applications that process and store this information.

Scope
These guidelines apply to independent Pekin Insurance Agents. These guidelines are a compilation of recommended best practices to help secure small and medium business networks.

Roles and Expectations
When technically possible, Independent Agents should follow the recommended guidelines specified in this document.

Pekin Insurance will not be responsible for any failure of non-Pekin Insurance/employee-owned hardware and software during the configuration or operation of non-Pekin Insurance computer equipment, personal devices, wireless access points or routers.

The information contained in this document is confidential and non-public. Its use is restricted to the conduct of Pekin Insurance business. It may not be disclosed to unauthorized persons and may not under any circumstances be sold, conveyed or otherwise used for any personal purpose.

Updates and Revisions
This document will be updated as necessary to accommodate an ever-changing business environment. When sections are added, deleted, or rewritten, a revision notice will be posted.

A. Wireless Access Point/Router Configuration

Wireless users connecting to their home or business wireless network should be required to log into their wireless router/access point to modify, update, amend or delete current default configuration settings. Please consult the documentation/user manual for the wireless access point/router to determine how the settings in these can be implemented.

A-1 Default Configuration Settings

A-1.1
Change the Service Set Identifier (SSID) to something unique, if possible. The SSID does not need to be overly complex, but should not remain at the default setting by the manufacturer. The SSID should not contain personal information, such as names and addresses that could help identify the owner of the access point.

A-1.2
Best practice is to disable broadcast of SSID, as doing so gives an attacker one less vital piece of information by which they can gain access to your network. However, some wireless devices will not maintain a connection to the Access Point if the SSID is not broadcast; therefore this set up should be tested by end users before it is made the default setting.

A-1.3
Change the default administrator username and password used for accessing and administering the wireless access point/router. Most wireless access points/routers come with empty or well known administrator usernames and passwords, and changing these will make it difficult for someone else to modify your network and gain unauthorized access. ***TIP: Be sure to remember your Administrator password! It is required in order to gain access to the Wireless router. If you need to write your Administrator password down, be sure to store it in a secure location.***

A-2 Enable and Utilize Security Settings

A-2.1
Home and business users should use WiFi Protected Access Pre-shared Key 2 (WPA2-Personal) along with Advanced Encryption Standard (AES) encryption. Or WiFi Protected Access Pre-shared Key (WPA-PSK) with Advanced Encryption Standard (AES) encryption. Where AES is not available, Temporal Key Integrity Protocol (TKIP) is recommended.

A.2.1.1
It is recommended utilizing the pre-shared key (WPA-PSK) version of WPA, and utilizing a passphrase/pre-shared key that is overly complex (i.e. very long and using random characters). The longer and more random the passphrase is, the exponentially more difficult for an attacker to penetrate your network. ***TIP: Be sure to remember your passphrase! It is required in order to gain access to the Wireless router. If you need to write your passphrase down, be sure to store it in a secure location.***

A-2.2
WEP is not recommended since it is extremely easy to break by malicious users. However, if WPA2 or WPA is not available, Wired Equivalent Privacy (WEP) will provide some protection to secure the wireless transmissions.

A.2.2.1
If using WEP, change WEP keys on a regular basis, a minimum of several times a year is recommended.

A.2.2.2
If using WEP, configure the encryption key/string to utilize the longest/highest possible key/string length. For example, 128-bit encryption should be used rather than 64-bit encryption. Please consult the product documentation for configuration details.

B. PC Configuration/Usage

B-1 PC software updates and Anti-Virus

It is highly recommended utilizing the following system guidelines while connected to the Internet.

B-1.1

- Anti-Virus software should be installed and running at all times. Anti-Virus signatures should not be more than one week old. It is best practice to update Anti-Virus signatures on a continuous basis.
- Automated scheduled Anti-Virus scans should be conducted daily when possible. If daily scans are not possible, users should scan their systems at least twice a week.
- PC's should have application based firewalls enabled when technically possible. Most of the time the default firewall settings provide adequate protection with no modifications needed.
- Automatic software updates should be enabled on all systems running Microsoft Windows. And should at a minimum have Service Pack 3 installed with IE8 or the latest version of your preferred web browser.
- 3rd party applications such as, Adobe Reader/Acrobat/Flash, Firefox, Java, Apple iTunes, and QuickTime should be fully patched to the latest version when technically possible.
- Peer –to-Peer file sharing software should be disabled prior to connecting to the Pekin Insurance network.

C. Motives and Common Hacker Attack Vectors

C-1 Motives

Before we get into the attack vectors hackers use, it is important to understand why hackers target small and mid-sized businesses. Often times small and mid-sized business lack the robust security controls that help keep the bad guys out. And since "hacking" is a for-profit trade, the bad guys will always go after the easiest targets.

In 2010 40% of mid-sized businesses were victims of a data breach. And, recent studies show the number of cyber attacks against mid-sized organizations has more than quadrupled since 2008.

C-1.2 Attack Vectors

Common attack vectors include, but are not limited to the following:

- Social Engineering
  - This is the act of tricking people into divulging confidential information.
- E-mail spam attacks
  - Unsolicited bulk messages sent to a random audience.
- Email phishing attacks
  - Attempts to gain access to confidential information. Similar in nature to social engineering, but typically delivered via e-mail, Instant Messaging, and Social Networking sites like Facebook. An example would be a fake email asking you to provide your banking username and password.
- Malicious Software
  - Trojans
  - Viruses
  - Worms

D. Recommended Security Sites

D-1 Recommended Sites

The following sites can be very helpful for education, troubleshooting, and updating your software:

- http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us
- http://www.bitdefender.com/scanner/online/free.html
- http://www.adobe.com/downloads/

- http://www.grc.com/x/ne.dll?rh1dkyd2
- http://en.wikipedia.org/wiki/Phishing
- http://en.wikipedia.org/wiki/Trojan_horse_(computing)
- http://en.wikipedia.org/wiki/Trojan_horse_(computing)
- http://en.wikipedia.org/wiki/Computer_virus

E. Glossary

Authentication
A process designed to determine the identity of a user that is attempting to access a system.

Authorization
Is the process of granting someone permission to do or have something. In computer systems it is the act of granting users access to a system.

Router
A router can be a device or, in some cases, software in a computer, that determines the next network point to which data/information should be forwarded.

SSID (Service Set Identifier)
A Service Set Identifier (SSID) is a sequence of characters that uniquely names a WLAN. The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same.

WEP (Wi-Fi Equivalent Privacy)
WEP (Wi-Fi Equivalent Privacy) is a security protocol for wireless local area networks.

Wi-Fi (Wireless Fidelity)
Wi-Fi refers to wireless networks that use specifications in the 802.11 family. Products approved as Wi-Fi are interoperable with each other.

Wireless Access Point
A Wireless Access Point (WLAN-AP) is a device which allows individuals to use wireless networking cards in their computers and other electronic devices. A Wireless Access Point typically consists of an Ethernet port, some sort of radio communications and sometimes also a modem.

WLAN (Wireless Local Area Network)
A Wireless Local Area Network allows mobile users to connect to a Local Area Network

WPA (Wi-Fi Protected Access)
WPA (Wi-Fi Protected Access) is a standard that has been developed to improve security features of WEP when using Wi-Fi products.