FELTON, BERLIN & ERDMANN
INSURANCE SERVICES, INC.

February 2017

Welcome

Happy 2017!

I am pleased to send along our quarterly newsletter.

Please feel free to give me your feedback about the material presented as well as topics/ ideas for future newsletters.

Rob Erdmann

Contact Us

Robert H. Erdmann, ARM
President/ CEO
Felton, Berlin & Erdmann Insurance Services, Inc.
100 Corporate Place
Peabody, MA 01960
978-548-3740

rerdmann@fbeins.com
www.fbeins.com

What's New This Month

How To Avoid Public Wi- Fi Security Risks

How To Stay Safe While Shopping Online With A Mobile Device

Do You Know Your Flood Risk?

How To Avoid Public Wi- Fi Security Risks

People who use public connections may be compromised by hackers, but there are several safeguards available to keep from becoming a victim. The recent availability of free Wi- Fi has been a great benefit for businesses and consumers alike, and there are free connections in almost any hotel, restaurant or coffee shop. Since no authentication is required to establish a connection, hackers have an easier time stealing data. Hackers position themselves between a person with an unsecured device and the connection point, which means that the phone's information is sent to the hacker instead of the hotspot. Emails, search requests and credit card information may be sent. With this information, a hacker may be able to access some of the person's information easily.

Many hackers also use unsecured connections to send out malware. For those who allow file sharing, it is easy to be infected. Some hackers can target the connection point, which creates a popup window while the computer is connecting. It offers a free upgrade for a certain type of program that most people use, and clicking on the fake offer automatically installs the malware. As public Wi- Fi becomes more common, expect to see hackers step up their game too. Security issues increase but this does not mean that people should not use any free connections. It is simply a reminder of the available safeguards and the importance of using them.

Always use a VPN. A virtual private network serves as a buffer between the Wi- Fi connection and the mobile device or computer. Any transmitted data is then encrypted and becomes too much work for the hacker to attempt to figure out. Use a trusted and reputable VPN provider. While some providers charge a fee of around $10 or more for monthly service, some are free.

Use SSL connections. Although most people are not as prone to use a VPN, they can easily add encryption to communications by enabling the "always use HTTPS" feature on a computer or mobile device. This ensures a secure connection to sites, and it is vital for any site where financial credentials are entered.

Turn off automatic Wi- Fi when it is not in use. When a phone is not connected to Wi- Fi, an automatic search will still transmit some data while looking for available networks. To stay safe, disable Wi- Fi after finishing.

Turn off sharing capabilities. Access the control panel on a device to do this. Allowing sharing will give people who have the ability to use it access to information and data on the device.

Issues may still arise even with the best safeguards in place. Taking the above mentioned precautions will help reduce the likelihood or frequency of security breaches. Be vigilant. Learn more about staying safe online in public places.

How To Stay Safe While Shopping Online With A Mobile Device

Internet- reliant devices such as smart phones, tablets and now watches should be properly protected. This is especially true during the holidays and other periods of heavy data usage when people shop online. Criminals are always looking for online shoppers to target, and their methods are becoming more sophisticated every year. Be suspicious of emails regarding problems with credit cards. Companies usually call to alert cardholders of suspicious activity. Never click on emails with attachments and urgent offers.

Criminals know that people are always looking to save money or are worried about their credit cards being compromised. Also, they use ads to entice people to visit unsecured sites, and some of these sites may look similar to the homepages of popular retail stores. Always look at the URL bar to ensure that it starts with "https" and is the legitimate site of the retailer. These are some important tips to remember when shopping online:

1. When visiting a new site to make a purchase, read independent reviews to see what other consumers have to say about the company's products and business practices.
2. When completing a transaction online, pay attention to the type of information requested to ensure that no unnecessary personal details are shared.
3. Only fill out the required fields of information when completing a transaction.
4. Avoid clicking links in text messages and emails.
5. When a questionable email about a major retailer's sale is received, look up the site on Google and visit it from the search engine instead of the email link to verify the sale.
6. Always use safe payment options such as credit cards when buying something online.
7. Read and understand a retailer's return policy, privacy policy and other information to know what to expect.

When shopping in a mall or store, always disable a phone's Wi- Fi. Some stores have their connections set to detect and track phones with Wi- Fi. However, criminals can also do the same thing. Always be wary of what business is conducted using a public Wi- Fi signal. Avoid making transactions, sending sensitive information or sending personal emails. Here are some additional security tips:

- Download good security software for all tablets, smart phones and laptops.
- Use authentication methods for logins.
- Choose strong passwords for online accounts.
- Log out of any account after using it instead of leaving it open.
- Use a different password for every account instead of using a universal password.
- Change all passwords frequently.
- Clear and delete downloads and unnecessary files.
- Be sure that an app is trustworthy before downloading it.

To learn more about protecting online shopping safety and avoiding hackers, speak with an agent about your options.

Do You Know Your Flood Risk?

Almost everyone has a risk of being flooded, regardless of where they live. According to the U.S. Federal Emergency Management Agency, more than 20 percent of all flood insurance claims come from areas outside of high- risk flood zones. That still means the vast majority

come from high- risk areas. How can a property owner find out what his flood risk is?

FEMA considers a property to be at high risk of flood if there is at least a one- in- four chance of flooding during the life of a 30- year mortgage. Geographic areas with this risk are known as *special flood hazard areas* (SFHA). Federal regulations require federally regulated or insured mortgage lenders to confirm that mortgaged properties in these areas carry flood insurance.

The traditional way to determine a property's flood risk is to locate it on a flood insurance rate map (FIRM). FEMA publishes these maps based on geographic survey data. They are the official depictions of flood hazards in a locality. FIRMs are freely available for review on Flood Map Service Center on FEMA's web site. A property owner can view his flood risk by entering the address in the search field.

Flood maps assign each area in a community to labeled flood zones. Areas with low- to- moderate risks of flooding are assigned to zones with labels beginning with the letters B, C, X or a shaded X. SFHAs are designated with the letters A or V. These areas are shaded on the maps for easy identification.

Property owners can also search for their flood risks at FEMA's flood insurance consumer web site, www.floodsmart.gov. By entering the address in the fields on the home page, they can quickly learn whether they face a low- to- moderate or high risk. The site offers other valuable tools, such as an estimator that can calculate how much damage a given amount of water (two inches, four inches, etc.) would cause in homes of various sizes. For example, six inches of water in a 2,000 square foot home would cause $39,150 in damage.

FEMA also offers a suite of flood risk products that go beyond the information provided in a FIRM. They include Flood Risk Maps, which show the overall picture of flood risk for a given area; Flood Risk Reports, which show community- specific flood risk information; and the Flood Risk Database, which stores all flood risk data for an area. These products are helpful for community planners, but individual property owners can also use them to get a clear idea of their flood risks.

Elevation certificates may also be on file with local governments for certain properties. This document shows the elevation of the lowest floor of a building (including the basement) compared to the base flood elevation for the area. It demonstrates community compliance with floodplain management laws and is used to set appropriate flood insurance premiums.

A flood can be every bit as catastrophic as a fire. It is worthwhile for property owners to learn their flood risk and take steps to reduce it.