IN THIS ISSUE:
~ GPS Privacy Issues

COMING NEXT MONTH:
~ Windows 7 – First Look

READY NET GO … NEWS

April 2009 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Identity Theft

Although identity theft is on the rise, there are many ways you can protect your personal information. A good place to start is the Federal Trade Commission website, www.ftc.gov

Phishing

Fraudsters send SPAM or pop-up messages to your computer in hopes you will click their link and send them your personal or financial information.

- To avoid phishing scams, don't click links in emails. Visit the website directly through a Bookmark or by typing the address directly into the browser.
- Use anti-virus and anti-spyware software and update them regularly.
- Review financial statements monthly and your credit report at least once per year.

Phone Fraud

If you receive an unexpected phone call from a company you do business with or a number you don't recognize, verify the phone number with your paper statements. You can also "Google" it to see if it's legitimate. The phone number may turn up as there are many blog sites that list fraudulent phone numbers.

From the FTC website...

"Legitimate companies won't call or email you asking for your account number or password. If you are concerned about your account, call the number on your financial statements or on the back of your credit card. And don't assume that you can trust Caller ID to let you know where a caller is located. Because scammers use Internet calling technology, the area code you see may not reflect where they really are."

GPS Privacy Concerns

In last months' newsletter, we reviewed GPS technology and the many uses in which GPS is currently being marketed. The technology has proven to be valuable for both consumers and businesses in added convenience and security as well as increased efficiency and productivity. While GPS technology excels in many cases, there are equal causes for concern.

When GPS was first implemented, it was an expensive technology that few people could justify using. Now that the demand for GPS products has risen, prices have come down significantly enough that nearly everyone can afford the technology. Manufacturers have jumped on board and are now including GPS technology in many products ranging from cell phones and cameras to dog collars and athletic gear.

But at what cost?

While GPS products are convenient and efficient at times, there are also concerns surrounding how the technology can be used. We already have video cameras monitoring city sidewalks, building entryways and at busy intersections to catch red light offenders. Google software even allows you to pinpoint anyone's location and get a close-up view of most homes across the US. Many privacy rights groups are cautious about the "always-on video surveillance" that is already commonplace in our lives. GPS technology adds significantly to this surveillance and has many people wondering where we're headed.

Websites Worth Watching

1. www.privacyrights.org - Privacy Rights Clearinghouse

   As a Nonprofit Consumer Information and Advocacy Organization, PRC provides information on Identity Theft as well as Financial Privacy, Medical Records, Direct Marketing and much more. This site provides one stop for all issues pertaining to privacy.

2. www.eff.org – Electronic Frontier Foundation

   Another excellent site for privacy related information.

GPS Tracking

One of the most daunting uses is in the tracking feature. Since GPS components are extremely small (some newer models can be attached and woven to cloth fiber), the ability for someone to unknowingly track another is quite real. Many Smartphones, in particular, have GPS tracking software installed that allows individuals to track the phone remotely. [In most instances, GPS settings must be enabled and a separate data plan must be purchased in order to use the feature.] Once configured, you can track a person's location and get email alerts when the individual travels outside a pre-designated area.

In some instances, the tracking feature may be overt; an employer may use the technology to track company-owned vehicles to monitor mileage and time. In other ways, the feature could be covert; a parent could enable the tracking software on a cell phone for a teenager and track their child's whereabouts without their knowledge (as long as the phone is turned on). Many individuals and groups believe this could have severe implications for privacy rights.

Mobile Marketing

Cell phone companies can already track you when you're cell phone is turned on. Retailers want to know too and so mobile marketing campaigns are being devised that send messages and coupons to your cell phone when you're near their store (via GPS software in your phone). Some people appreciate the savings especially if they were going to the store anyway. Others, though, don't want retailers to know where they go and what they purchase. If you want the GPS capabilities but don't want to be tracked by retailers, read Privacy Agreements closely and ensure that you have an ability to opt-out of these targeted campaigns at anytime.

Insurance / Rental Car Companies

Insurance companies have begun installing tracking devices in insured cars to monitor driving habits. The companies market the optional devices as ways to save on insurance premiums at the expense of allowing the company to know where you travel, what roads you're on, how fast you drive and what time of day you drive. But the actual idea was devised so that an insurance company has a way to assign premiums. If you exceed the speed limit and drive long distances, your premiums will go up; if you drive the speed limit and only travel short distances, your premiums will be lowered.

Rental car companies have also been using GPS devices although not legally. There have been several instances where rental car companies were fined for installing GPS devices in their rental cars and assessing extra fees based on mileage and driving out-of-state. Both of these instances point to the need to read agreements closely before signing.

Law Enforcement

Another area in which privacy concerns has surfaced is in law enforcement. Recently, a criminal was captured after the police attached a GPS tracking device to a suspect's vehicle. When the suspect was conducting an illegal act, the police were able to respond immediately without the need for constant surveillance. On one hand, a criminal has been taken off the streets but privacy experts have questions. Who will use the technology legitimately and on whom will the technology be used? Will we have a say in the matter?

Currently Washington and Oregon are the only states that require officers to get a warrant before placing a GPS device on a vehicle (there is no Federal law regarding the inclusion of GPS data as evidence in court proceedings). As the technology becomes ubiquitous, however, other states and the Supreme Court may decide to enact legislation for how and when GPS devices can be used.