IN THIS ISSUE:
~ PGP Encryption

COMING NEXT MONTH:
~ DTV Transition

READY NET GO … NEWS

October 2008 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Deleting Data from Hard Drives

Do you have a computer sitting around idle? Have you wondered what you should do with it? You could pass it on to a family member or friend or donate it to a local non-profit. You may even want to try selling it if it is fairly new.

Before you do this though, you'll want to delete **ALL** of the personal information off of the hard drive. Just pressing delete isn't good enough however. **You must thoroughly remove the data which requires special software.**

Data is stored on a hard drive much like how books are stored and accessed in the library. Books are on shelves and the information relating to those books is stored in a catalog. Without the catalog it would be difficult finding a particular book, but it's not impossible. Anyone with the right tool and determination can locate the book without the card in the catalog.

The same thing happens with data stored on hard drives. You may delete the file using Windows Explorer but the file still resides in bits and pieces on the hard drive – on the surface, the file is just removed from the index just like the card from the catalog. With the right tools and know-how, a professional can piece that file back together in a very short time.

In summary, donating used computers is a great idea – just be safe about your data and delete it properly before passing the computer on to someone new. Need a recommendation for disk cleaning software? Give us a call.

Encryption Software

Do you frequently send "sensitive data" via email because of the convenience? Do you know that most email transmissions can be intercepted and read by outside parties? **PGP** (**Pretty Good Privacy**) is an encryption scheme that gets high marks from security experts everywhere. If you're concerned about protecting the transfer of data (email) over the Internet as well as safe file storage, PGP is an important concept to understand and implement.

What is PGP?

PGP encryption software can be used by individuals and corporations to secure the transmission and storage of data over networks. It consists of two parts: a **Public Key** and a **Private Key**. The keys are paired, randomly generated and consist of a block or string of alphanumeric digits such as 1, 2, A, c, %, ? etc. The length of the key can be anywhere between 512 - 2,048 bits which makes it extremely difficult to crack especially when used in conjunction with a strong password.

Public Keys vs. Private Keys

The Public Key encrypts the data and the Private Key decodes the data. Only the Public Key is shared. When someone wants to send you sensitive data, you provide them with your public key. They, in turn, will send the information and only you, with the corresponding Private Key (which you created) can open the data.

The same concept works in reverse if you want to send sensitive data to someone. They send you their Public Key, you package the data with their Public Key and only they will be able to access the information with their Private Key.

WWW (Websites Worth Watching)

1. www.bankrate.com – Excellent site for financial information, calculators, current loan rates, & articles.
2. www.eol.org - Encyclopedia of Life - an ambitious, online database and global learning tool that seeks to catalog every living organism known to mankind.

Important Points in Implementing Encryption Software

PGP Encryption was developed in 1991 and is the most reliable and widely used encryption scheme being used today. Both licensed and Open Source (i.e. free) versions are available. One open source version is called GPG, short for GNU Privacy Guard. Both versions are available on nearly all platforms (Operating Systems) and can be downloaded for individual or corporate use.

#1: The advantage of using PGP for secure email transactions is that even if the email is intercepted in transit, without both keys (the Public AND Private Keys), the information will not be viewable.

#2: In order for PGP encryption to work, **all parties** who send and receive encrypted information must have the PGP software installed on their computer, they must set up an account, and they must create Public and Private Keys. Without an account, encrypted messages will not be able to be read.

#3: The PGP software integrates with your email program to send encrypted messages. After you create your message, you can access the PGP system by clicking a button in the email program or in your system tray and the PGP software will encrypt your message prior to sending.

#4: In most cases, encrypted messages are not automatically saved in a Sent Items box. You must tell the software that you want to save the message (which creates a key for you to use to view the message in the future). Once you encrypt a message, it can only be viewed by the individual who has the private key (the person you are sending it to).

#5: As mentioned above, PGP is a two step process: **Signing** (a.k.a., encrypt&sign) and **Verification** (a.k.a., decrypt&verify). As an added layer of protection, the Public and Private Keys are encrypted with a one time key for each encrypt / sign operation. This way, you can send the same information to multiple people, assign different Public Keys to the message and allow those individuals to use their unique Private Key to view the message.

#6: In addition to encrypting emails, you can also **sign emails** with your PGP encrypted signature which other PGP users can use **to verify your authenticity**. If you frequently contribute to list serves or grant others' access to your computer, as long as you maintain a secret password, no one will be able to impersonate you.

#7: An additional feature of PGP allows you to **encrypt files on your computer** for your own security. When you encrypt a file, a duplicate encrypted file is created. Delete the original file (see this months' Tip on the front) and then use your Private Key to open the file in the future.

#8: Downsides to PGP? You need to be mindful with whom you choose to use PGP - You must know and trust your recipients implicitly. Personal contact is important – never share your public key with someone you have not met. Using PGP adds time to the process and requires organization which can be an inconvenience to some. **Questions to consider**: Will you encrypt all emails? How will you determine which ones you do if you don't encrypt all? Will you be able to keep track of your Public and Private Keys created when you send email to different individuals?

Situations where using PGP would be beneficial:

- HIPAA confidentiality (medical records)
- Confidential client communications such as lawyers, physicians, psychologists
- Personally Identifiable Information such as credit card numbers, social security numbers, employee id's, etc.
- International relief aid workers, foreign correspondence
- Communication regarding projects or products prior to public release (i.e. intellectual property)
- Encrypting voice over IP and setting up an encrypted peer-to-peer network using PGPNet.