Protecting Your Internet Activities and Electronic Data

With more of our financial activities occurring over the Internet, it is important to be aware of risks these activities entail and steps you can take to reduce the risk that someone will illegally gain access to your private information or financial accounts.

Common Internet Scams

- Auction fraud – This may take many forms including emails saying you have a second chance to buy an auction item, non-delivery of an item purchased in an auction, defective merchandise or receiving cheaper merchandise.
- Advance payment frauds – Emails asking for help in getting money out of a country or advising you that you won a lottery lead to requests for money to cover legal fees, taxes, bribes, processing costs and taxes.
- Phishing – Emails notifying you that an institution or store need confirmation of account information lead to a fake (or spoofed) website that looks legitimate but is just a place to disclose personal information to fraudsters.
- Hot stock promotions – Emails, online newsletters and bulletin boards may be nothing more than a scam artist's attempt to have you drive up the price of a stock so they can sell their shares. This is often used with cheap and thinly traded stocks.

Protecting Your Online Activities

Be careful using public computers. Using a computer at a cyber café or a free computer at a trade show can be dangerous. The computer may be programmed to capture user names and passwords. If you use this type of computer make sure no one is looking over your shoulder to memorize your personal data and be sure to sign off when you are done.

If you are using the Internet for financial transactions, be sure the sites you visit are secure. Most secure sites have URLs that start with "https://" instead of the normal "http://." Some websites may display a logo indicating it is secure, but make sure you know the site is one you trust.

Wireless Internet networks have become common and convenient. Some are secure and some are not. Be careful using wireless networks that are free and not secure. Wireless home networks deserve attention as well. It may be time consuming or more expensive to have a secure network at home, but that is better than having a fraudster sitting in a car on your street monitoring your activities and gaining access to your files and information.

It is important to install anti-virus software on your computer and keep it up to date. The safe holds true for firewalls and security patches for your operating system.

Passwords

Many websites you visit require a user name and password. Having a strong password will make your online activities safer. Unfortunately, many passwords are chosen to be easily remembered rather than to protect the user. Some common passwords that hackers could easily guess are password, user name, your real name, your address, 123456, abcdef, or just a number. With just a four digit number, there are only 9,999 combinations and a sophisticated hacker could probably figure that out in seconds.

Strong passwords are at least six characters long and preferably eight. They should contain a mixture of upper and lower case letters, numbers and special characters (#, $, ^, &,!,?, {, >, etc). They should not be based on personal information and not be based on words found in a dictionary.

The difficulty of long and mixed passwords is that they can be hard to remember. One suggestion is to create a password from a sentence that you are likely to remember. For example, start with the sentence "My children John and Mary are 12 and 16 years old." Then use the first letters of the words, characters and the numbers to create the "McJ&Ma12&16yo" password.

Changing passwords often and using different at different websites also increases protection. Keep any written record of your passwords in a safe location.

Disposing of CDs and Diskettes

The best way is to physically destroy the CD. Shred it if you have a shredder that can handle it without difficulties. Otherwise, you can break the CD into pieces. Be careful and wrap the CD in a paper towel to avoid shattered plastic.

Diskettes can be formatted to remove the data if you plan to reuse them. Otherwise, it is a good idea to break them into pieces or shred them.

Disposing of a PC Hard Drive

With the ways you use your PC and financial software you may use, think of the highly sensitive information that is stored on your hard drive. It may have tax returns, investment records, financial account information, and other personal data. It may also have records of your user names and passwords used at dozens or hundreds of websites. This is information that must be removed before disposing of an old PC.

Unfortunately, it is extremely difficult to completely erase that data from your hard drive. Deleting files and even formatting your hard drive does not completely remove the data. With the right tools, a skilled technician could reconstruct your data.

There are some software products that claim to overwrite an entire hard drive and make it impossible to recover the data. A better, easier and cheaper solution is to remove the hard drive and physically destroy it.

If you are considering disposing of, donating or recycling a PC, protect yourself and your data by removing destroying the hard drive.

Article written by Financial Wisdom, advice is solely attributed to that entity.