

Security of online payments

Contributed by knwom

Why is security so important?

There are two reasons for making your online payments as safe as possible. The first one is trivial - you do not want to loose any money. It can happen because of loosing the passwords or spending to merchant that will not send you bought goods. The second one can be more important, while it can be much more painful for you. It is loosing your personal data, which can effect in some real trouble as loosing money from credit cards, someone making debts on your account etc.

Secure your computer.

First thing you need to do is secure your computer. Start with your web browser. There are many browsers available for free, the most popular are Internet Explorer, Mozilla FireFox and Opera. Internet Explorer has always been known as being unsecure, mostly because of multiple bugs and holes. It was improved in IE 7.0, however, it is still far from being perfect. It is mostly caused by its popularity, the more people use a browser, the easier is to find someone who does not instal updates frequently or risks some severre losses. FireFox is currently getting more and more popular. One of the reasons is its safety; in fact its harder to find any bugs or holes in this program, because it is not as popular as Internet Explorer is. Nevertheless, FireFox is more secure, beause patches are made available soon after finding a hole. It has built-in phishing filter that is quite effective in blocking fake webpages. I personally use FireFox 2.0.0.1 at the moment. The webbrowsers I would not recommend to use is Opera 7.0+. It has been frequently criticized for its vulnerability.

The second thing is adware/spyware and virus protection. Adware is any software added, built-in or bundled with any other software. It usually plays ads and makes the software cheaper or even free of charge. However, it often happens that adware becomes spyware, tracking your online behaviour and/or your passwords. There are plenty of free and paid programs that can remove any adware/spyware and/or block installing new. I personally use Lavasoft Adaware SE Personal, this is a free and very effective application that is a part of Google Pack, as well as Mozilla FireFox. I also use avast! 4 Home Edition for antivirus protection. If you access the Internet directly, you should install firewall also. Those who do not have direct access to the Net are usually behind firewalls provided by thier ISPs.

What is Spyware?

Most computer users today are familiar with the term spyware because they or someone they know has experienced the aggravation of this software firsthand. Sluggish computer performance, altered home pages, and endless pop-up ads are all signs your PC could be infected. Everyone who uses a computer is susceptible.

Spyware is a program installed on your computer, with or without your permission that can change system configurations, monitor your Internet activity and broadcast the information back to an outside party, often advertisers. The milder forms of spyware are simply annoying, with increased spam and unwanted pop-ups; these are known as adware. Malware refers to more malicious programs that can rob your PC of its ability to run efficiently. The newer, more advanced forms can actually steal personal information like bank passwords or credit card numbers.

Spyware has often been referred to as a virus, but this is not accurate. The software does not duplicate itself like a virus, which is why it is never detected when an anti-virus program is run. The best protection for your computer is a 3-tiered approach: anti-spyware software, anti-virus software, and a firewall.

How it Works

Spyware can worm its way into your computer even if you are careful while surfing the Internet. Nowadays, it may even invade your system if you simply visit certain web sites. Applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from media-supported sites. These sites are infamous for carrying spyware infections. It is usually disclosed, but buried, at the end of a License Agreement or Privacy Statement. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Occasionally, spyware authors will pay shareware creators to wrap-in spyware with their software.

Spyware is becoming more sophisticated and many applications are designed to spread themselves out on your PC, making it more difficult to wipe them out completely.

Installing proper software, however, is not enough. Even the greater influence on your safety have your actions. Visiting some sort of sites (usually with cracks or porn) can result in downloading or installing trojans and keyloggers (software that tracks our key pressed on keyboard, used for logging passwords). Remember not to download or install any software from this sort of sites. Beware of any popups, these are annoying, but can be dangerous as well. People usually focus on closing the pop up and mechanically click 'ok' in dialog boxes that appear on such sites, what causes malicious software to install. Remember not to allow any ActiveX scripts to activate at any site that might be risky.

The last point in this section is about securing physical your computer. If you are to be the only user of the computer, make sure you are. If your operating system allows securing your computer with password, use it. It is even better when you have your own laptop with finger print reader, you will be sure you are the only one that uses it.

Secure your account.

When computer is finally safe, we can focus on keeping your account secure. Remember, that your account will never be too safe. Different online payment systems have various methods of securing your accounts. The one that is in every

payment processor is password. You should use a different password from those used to your e-mail, webserver online communicators etc. Moreover, you should make the password as strong as possible. Strong passes contains of different random letters and numbers.

Most, but not all, online payment processors use turing numbers while accessing the account. It can prevent account from being breached with brute force (submitting multiple passwords).

There are some more protections, depending on payment processor. E-gold sends PIN codes if you try to access your account from different IP than you did previously. Moneybookers require your birth data to confirm any transaction etc. Secure your transaction.

When your computer is safe, as well as your account, the only way you can loose your money is your mistake. Always doublecheck if the account you are trying to spend to is really the account you want to pay. The second thing you must remember about is checking sellers personal data. AlertPay and PayPal offer merchant authentication, use it to insure that you deal with hones sellers.

What is phishing?

In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. That is why you should never ever use login links provided by e-mail. None of the payment processors will ask you to login to your account with the link provided, they will never ask you for your login information in other place than login page.