



Protecting yourself from Online Banking Fraud

The online banking industry has seen an increase in fraudulent activity over the last several months. With key loggers, virus attacks and phishing scams becoming more prevalent, are you doing all you can to protect yourself from becoming a victim of fraud?

For the past several years, there has been a lot of focus on identity theft. While very serious and very damaging, there are many other ways that the “bad guys” can wreck havoc on your life and your finances. Services like the ones available from the three major credit reporting agencies and companies such as LifeLock® offer protection against other people establishing credit or identities using your Social Security Number. These services are very valuable and worthwhile, but true identity theft is not the only threat out there in these digital times.

Many cyber criminals, also referred to as fraudsters, don't want to steal your identity in the traditional sense. They don't want to get a credit card or a mortgage or a checking account in your name and live their life off of your good credit history. They simply want to take your money and move on to the next victim. While most companies that do business on the Internet including Financial Institutions, are very diligent in providing online protection for their customers, the first line of defense is knowledge about what you, the end-user, can do to protect yourself – an electronic way of “Looking out for Number One”. The two most prevalent types of fraud, “Keylogging” and “Phishing”, occur from viruses on your computer. In both cases, the end result is the fraudster capturing your login credentials.

Keystroke Logging or Keylogging

Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Keyloggers are “Trojan” software programs that target your computer's operating system (Windows, Mac OS, etc.) and are “installed” via a virus. These can be particularly dangerous because the fraudster has captured your user ID and password, account number, Social Security Number - basically anything you have type as you type it. If you are like most other users and have the same ID and PIN/Password for many different online accounts, you've essentially granted the fraudster access to any company with whom you conduct business. After all, they've got your login credentials so they appear to be a valid user.

Here are some ways you can prevent yourself from being a victim of keystroke logging:

- Use Anti-Virus Software. This is the single most important thing you can do to protect your computer from viruses. There are many on the market today – some cost money while others are free. If you opt to use a free version, make sure it is being offered by a reputable company and do research on the company and its product before installing.
- Keep your Operating System up-to-date with the latest security patches.

Phishing

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. If you click on the link to go to the phony website and enter all of your information, you've just been the victim of a phishing attack. The fraudsters have just captured all the necessary information to access your accounts online. **No reputable business will ever email you requesting that you update your personal information, including account numbers, system passwords or Social Security Numbers via a link to their site.**

Follow these guidelines to protect yourself from phishing scams:

- Never click on a link from a business requesting that you provide them with personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you hover the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be.
- If your Financial Institution uses watermarks or personal images, do not log in unless you see the correct image on the screen.
- Report any phishing attempts to your Financial Institution.

If you are unsure that the request is valid, open a new Internet session and manually key in the business' web address. If the business genuinely needs information from you, they will have you log in to your online account to see the request. In most cases, you'll just be greeted with a message indicating that the business will never email you requesting personal information.

Following are some real-life examples of how fraud occurs and the damage it can cause. In each case, the fraudster had all the necessary credentials to gain access to the users' accounts. There is no security system available that will stop fraud if the perpetrator has all of this information, so it is imperative to take the necessary steps to prevent them from getting the information in the first place.

Fraud Case 1

A Florida business man sued his Financial Institution after hackers submitted a \$90,000 fraudulent wire transfer out of his account to an account in Latvia. His claim was that the bank should reimburse the funds since they processed the wire transfer. Upon investigation, it was determined that his computer was infected with a malicious software program (malware) that enabled fraudsters to retrieve his online ID and Password via keylogging. He then claimed that the bank was negligent because they had not specifically informed him that this particular malware was a risk. The courts disagreed and ruled in favor of the Financial Institution, stating that the customer had neglected to take the necessary basic precautions to protect his information. At the time of the fraud, nearly all antivirus software programs had made modifications to look for, and alert users of, the very malware that allowed his information to be compromised. At the time of his claim, those antivirus updates had been available for nearly two years.

Key Factor for preventing fraud:

- Install and update Antivirus Software

Fraud Case 2

A business owner accessed the Internet via an unsecured wireless network and as a result left his device open for a keylogging program to be placed on his computer. Fraudsters captured the user's ID and Password and created a new administrative user for the business account. During the next several days, fraudsters logged in as the new user and sent ACH batches in excess of \$400,000.

Key Factors for preventing fraud:

- Install and update Antivirus Software.
- Beware of accessing account information when using an unsecured wireless network.

Fraud Case 3

A virus on the users' computer compromised the login page to the users' business account. The altered/false login page displayed additional fields asking the user for credentials necessary to gain further access to the accounts, not just the usual ID and Password. Fraudsters were able to initiate two separate ACH transactions totaling more than \$100,000.

Key factors for preventing fraud:

- Install and update Antivirus Software.
- Beware of changes to login pages and areas where you enter credentials. Financial Institutions will let you know in advance if they will be making changes to the information they collect from you. If you are unsure, do not log in. Contact your Financial Institution to verify that the changes are legitimate.

What should I do to protect myself from fraud?

Besides following the tips mentioned in the previous examples, there are other things you should do to safeguard your personal and financial information.

- Change your passwords often. Even if your financial institution doesn't require it, it is a good practice to change your passwords at least every six months. An easy way to remember: change them when you change your clocks to adjust for Daylight Savings Time.
- Don't use the same ID and PIN/Password for every online account you have.
- Never disclose your login credentials to other people or companies.
- Do not store your ID and Password information where others could gain access to it. It is best not to write the information down at all.
- Do business with a financial institution that offers two-factor authentication for accessing your information online.
- If offered by your financial institution, take advantage of hard- or soft-tokens, which provide a unique one-time-use password each time you access your account. This is especially important for business accounts with multiple users.
- If accessing information via a wireless network, ensure that the network is secure. Accessing sensitive information (or any website) over a non-secure network simply leaves the door open for criminals. Even if you aren't visiting a site where you enter an ID and password, you are still leaving your computer exposed to possible threats.

While nothing is foolproof, and new viruses and scams are being developed every day, following these guidelines as well as having a general awareness of the threats that are out there enables you to bank online with more peace of mind and less risk of being a victim of fraud.