CITY NATIONAL BANK
The way up.®

Top Five Ways to Protect Your Business from Online Fraud

Internet fraud is ever-increasing. Hackers and thieves continue to find new ways to gain access to computers in their attempts to steal your personal information. If they succeed it can result in losses to you and your business. City National is doing its part to protect you from fraud. You must do your part as well. Here are some suggestions to safeguard your computer and yourself.

A Required Checklist for Businesses Using the Internet

1. **Install anti-virus software and anti-spyware/ adware software.**
2. **Install a firewall and only allow the necessary incoming/outgoing connections.**
3. **Maintain operating system (i.e., *Windows*) and browser updates.**
4. **Do not open attachments or click on links contained in e-mail from unfamiliar sources.**
5. **Do not download freeware or shareware from unfamiliar sources.**

This document also includes other safety tips and who to contact if you think you've become a victim of Internet fraud.

IMPORTANT Follow this step-by-step and do your best to complete each step in order to reduce your risk of becoming a victim while doing business online.

Regularly review your control systems to ensure they are kept up to date and working properly.

STEP 1:
Install anti-virus software and anti-spyware/adware software.

Anti-Virus software

What is anti-virus software?

Anti-virus software is a program designed to detect the presence or occurrence of a computer virus. The software will alert you if it finds a virus on your computer and, in many commercial products, can then be used to delete the virus.

Why do I need anti-virus software?

If you do not have anti-virus software running on your computer, when downloading files or opening e-mail attachments, you could receive a virus from the sender whether it was intentional or not. Computer viruses can delete files and programs and even send personal information that resides on your computer to a malicious third party.

Recommendations on installing anti-virus software

Install anti-virus software on your computer and set it to automatically scan files.

Free-trial versions are not sufficient as they may not

have all the needed features available. Companies such as *McAfee* (www.mcafee.com) and *Symantec* (www.symantec.com) sell software products that address viruses.

Recommendations on updating anti-virus software

Set your anti-virus software to automatically update itself when updates are available. New viruses come out all the time, and keeping your anti-virus software updated helps your computer recognize new viruses if they attempt to invade your computer.

Spyware/adware software

What is spyware/adware software?

Spyware or adware covertly gathers user information (including passwords, tax ID numbers and other personal information) through the user's Internet connection without his or her knowledge or consent. These applications are typically bundled as a hidden component when a user downloads freeware or shareware (free games, screensavers, etc.) from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Why do I need anti-spyware/adware software?

Most firewall software programs you purchase automatically come with anti-spyware/adware blocking capability. Without this blocking capability, you could click on an advertising banner and download malicious files that infect your computer with a virus – possibly stealing personal information or destroying files.

Recommendations on installing spyware/adware software

Install anti-spyware software on your computer and set it to automatically scan your files.

Here are some examples of spyware/adware protection software: *Spybot* (www.spybot.com), *Ad-Aware* by *Lavasoft* (www.lavasoft.com) and *Microsoft Security Essentials*.

Recommendations on updating spyware/adware software

New spyware/adware come out all the time, and keeping your spyware/adware protection software updated helps your computer recognize these malicious programs as they attempt to invade your computer. Refer to the user guides provided with your software to determine the best method to keep your protection current.

STEP 2:

Install a firewall and only allow the necessary incoming/outgoing connections.

Firewall software

What is a computer firewall?

Firewall software is a must for any computer that connects to the Internet. Firewall software is an application that resides on your computer and monitors all the Internet connections made to and from the computer.

Why do I need firewall software?

It is possible for someone to try to access computers that do not belong to them online. If your firewall software isn't installed and set to block these access requests, then the requestor could get access to information on your computer. Firewall software protects your computer from hackers and other malicious code that is sent around the Internet looking for vulnerable computers.

Recommendations on installing firewall software

When firewall software is installed and kept up to date on your computer, it can help protect you from these attacks. A best practice is not to allow anyone to access your computer without your permission. Therefore, you should set your firewall software to disallow incoming requests except for those requests from your firewall software, anti-virus software or operating system checking for updates.

Examples of common firewall software are *Zone Lab's Zone Alarm* (www.zonealarm.com), *McAfee's Internet Security Suite* (www.mcafee.com), *Norton Internet Security* (www.symantec.com) or *Microsoft Security Essentials*.

Recommendations for updating firewall software

Make sure that your firewall software is set to automatically search for software upgrades when they become available. Software companies will provide upgrades to their software as new malicious programs are developed and spread throughout the Internet.

STEP 3:
Maintain operating system (i.e., *Windows*) and browser updates.

Operating system and browser updates

What is an operating system?

An operating system is the software that runs your computer. The most common names of operating systems are *Windows* or *Mac OS X* and *Linux*.

Why do I need to update my operating system?

Sometimes the company that develops the operating system creates new updates for the operating system in order to make it work better, reduce security threats or the like. Many times hackers exploit weaknesses in a computer's operating system.

In order to ensure the operating system is secure, it is important to make sure it's always up to date.

Recommendations on updating operating systems

Many times you can set up your operating system to update automatically. Setting your operating system to update automatically is a best practice. Users of the popular *Microsoft Windows* operating system can set the "Windows Update" function to automatically update itself. The operating system will always look to the company's Web site for the latest updates while it's connected to the Internet.

Web browsers (*Internet Explorer*, *Google Chrome*, *Mozilla Firefox*, *Safari* etc.) are frequently updated by their vendors as well. Be diligent in making sure you are using the most current (non-beta) version.

IMPORTANT: If you are a *Windows XP* user, make sure you are at least on *Windows XP SP2* and *Internet Explorer SP2*.

STEP 4:
Do not open attachments or click on links contained in e-mail from unfamiliar sources

One of the most common ways to download malicious viruses to a PC is through e-mail attachments and links. If you receive an e-mail from someone unfamiliar to you, do not open it. Delete it immediately. If you are provided with a link to an unfamiliar site, do not link to it. You may get more than you expected.

Though most e-mail software today might have built-in virus scanning, it's not safe to assume that such software will catch everything. Remember, hackers are working on new ways to bypass these tools each day

Phishing

Fraudulent e-mail can often appear to come from a reputable source – this is called "spoofing" or "phishing" because the sender's true identity is concealed.

You may receive fraudulent e-mail aimed at retrieving your personal information – usually username and password and/or credit card numbers. Online fraud is a widespread issue on the Internet, and the best line of defense is education – learn how to recognize scams and e-mail fraud to protect yourself online.

Closely inspect any e-mail that provides a link or requests personal information. Never click on a link in a suspicious e-mail message.

And remember – City National Bank will NEVER ask for personal information through e-mail. Your best protection against fraud is caution. Do not respond to any message asking for the following:

- Password
- Personal Identification Number (PIN)
- Credit card validation code
- Bank account numbers
- ATM or credit card numbers
- Personal information, such as Social Security number

IMPORTANT: If you receive a suspicious e-mail that appears to be from City National Bank, report it to our security team immediately by calling 213-673-8101 or send an e-mail to emailfraud@cnb.com.

STEP 5:
Do not download freeware or shareware from an unfamiliar source.

What is freeware or shareware?

Freeware or shareware is software developed by a software developer or by enthusiasts and is distributed at no charge by users' groups via Web, e-mail, and message boards/blogs. The definition of freeware is not

free software, though it may be free of charges. Freeware is also called shareware.

Though free software does come from reputable companies like Microsoft or Apple, it is a good practice not to download freeware from companies or individuals you are not familiar with.

Why should I not download freeware or shareware?

Freeware or shareware usually does not come with the guarantees most reputable software companies include when their products or services are used. If software from a freeware developer has a security hole in it, it's less likely to be found or corrected by the freeware developer.

Other Safety Tips When Using the Internet

Use a Web site detection tool bar

One of the most popular scams on the Internet today is to send an e-mail from what looks like a legitimate source, but that ends up being from a thief. The e-mail asks you to click on a link and then provide logon or credit card PIN credentials. Most of the time these Web sites look so authentic that the user thinks it's the real Web site – they may even display the real Web site address when it's really not that site!

You can download a simple browser toolbar application that will tell you which Web address you're accessing. Examples of these applications are *Netcraft for Internet Explorer* (www.toolbar.netcraft.com) or *Spoofstick* for *Mozilla's Firefox* and *Internet Explorer* (www.corestreet.com/spoofstick).

Protect your password

A strong password is as long as possible. Always use at least six characters in your password; many online applications allow up to 15 characters. The longer the password, the more difficult it is for a hacker to break.

Strong passwords:

- Have both upper and lower case letters.
- Have digits and/or punctuation characters as well as letters.
- Are easy to remember, so they do not have to be written down.
- Are at least six characters long.
- Can be typed quickly, so someone else cannot look over your shoulder and learn it.

A strong password is <u>not</u>:

- Personal information such as your name, phone number, Social Security number, birth date or address. Names of acquaintances, pets, your kids and the like should not be used.
- Any word in the dictionary, or based closely on such a word (such as a word spelled backwards).
- A word with letters simply replaced by digits. For example, bl0wf1sh is not a strong password.
- Easy to spot while you're typing them in. Passwords like 12345 or ttttttttt should be avoided.

Who do I contact at City National Bank if I think I've become a victim?

If you believe you have received a phishing or fraudulent e-mail from City National Bank, please contact:

City National Corporate Security

(213) 673-8101
Business Hours: M-F, 8a.m. - 5p.m., Pacific time

If you believe your Online Cash Management or Treasury Net℠ username, company name and passwords have been compromised, please contact one of the teams below:

Cash Management Customer Service

Southern California: (213) 673-9393, Option 2
Northern California: (415) 576-2761, Option 2
New York: (917) 322-7434, Option 2
Business Hours: M-F, 8a.m. - 5p.m., Pacific time

Legal Disclaimers

No security system is perfect, and City National Bank does not represent to you that the guidance we strongly suggest above is complete. You may wish to consult your own Internet security advisor to address your particular situation.

CITY NATIONAL BANK
The way up.®