

# Top 10 Ways to Protect Yourself

*Fraud and identity theft are becoming increasingly common in today's world. City National remains committed to safeguarding your personal information and maintaining the confidentiality of your financial activity. However, there are many steps you can take to protect yourself online and help prevent fraud.*

## The Checklist

### ✓ 1. Install a firewall.

Firewall software is an application that resides on your computer and monitors all the Internet connections made to and from your computer. It also protects your computer from hackers and other malicious code that is sent around the Internet looking for vulnerable computers. If your firewall software isn't installed, it's possible that someone may access information on your computer.

#### **Recommend:**

- Keep firewall software up-to-date on your computer.
- Check out Zone Alarm®, McAfee's Internet Security Suite or Norton Internet Security 2006®.

### ✓ 2. Install anti-virus software.

Anti-virus software is a program designed to automatically detect the presence of a computer virus. If a computer virus is detected, the software will alert you and automatically delete it from your computer. By installing anti-virus software on your computer, you can help prevent computer viruses from deleting files and programs – and even sending personal information to a malicious third party.

#### **Recommend:**

- Check out McAfee or Symantec.
- Keep anti-virus software updated regularly.

### ✓ 3. Install anti-spyware/adware software.

Spyware or adware secretly steals personal information (passwords, tax ID numbers, etc.) from a user's computer without his or her knowledge. This usually occurs when a user downloads freeware or shareware (free games, screensavers, etc.) from the Internet. Most firewall software programs automatically come with anti-spyware capability.

#### **Recommend:**

- Check out Spybot® ([www.spybot.com](http://www.spybot.com)) and Ad-Aware® by Lavasoft ([www.lavasoft.com](http://www.lavasoft.com)) for adware/spyware protection software.
- Check out MacScan® (<http://macscan.securemac.com>) for Mac users.

### ✓ 4. Maintain operating system and browser updates.

An operating system is the software that runs your computer. The most common operating systems are Windows® and Apple Macintosh®. Operating system updates are developed to improve performance and reduce security threats.

#### **Recommend:**

- Set up your operating system to update automatically.
- If you are a Windows® XP user, make sure you are at least on Windows® XP SP2 and Internet Explorer SP2.

### ✓ 5. Never open an attachment or click on links 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. Most e-mail software today has built-in virus scanning, but it's not safe to assume that such software will catch everything.

### ✓ 6. Never download freeware or shareware from an unfamiliar source.

Freeware – also called shareware – is software that is distributed at no charge via Web, e-mail and message boards/blogs. Freeware or shareware usually does not come with product guarantees. If software from a freeware developer has a security hole, it's less likely to be found or corrected by the freeware developer.

### ✓ 7. Protect your username and password.

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

#### **Recommend:**

- Do not share your username and password with anyone.
- Change your password regularly.

### ✓ 8. Be wary of phishing e-mails.

Fraudulent e-mails can often appear to come from a reputable source -- this is called "spoofing" or "phishing" because the sender's true identity is concealed. City National will NEVER ask for personal information through e-mail. Never respond to any e-mail message asking for personal information such as social security number, password, bank account numbers, etc.

#### **Recommend:**

- Do not share your username and password with anyone.
- Change your password regularly.

### ✓ 9. Monitor your bank and credit card accounts online regularly.

More than 50 percent of fraud or identity theft cases are self-detected by victims. The quicker fraud is discovered the better. Therefore, we recommend that you regularly monitor your accounts through Online Banking to detect any fraudulent activity.

#### **Recommend:**

- Enroll in Online Banking to track account activity.
- Monitor your deposit, credit card or loan accounts online.

### ✓ 10. Know how to identify a secure vs. non-secure Web site.

It's important to know when a Web site is secure. Your browser should display a locked padlock if you are on a secure site. Microsoft® Internet Explorer displays the icon in the lower right corner of the browser. Netscape® Navigator displays the icon in the lower left corner of the browser, and Netscape® Communicator displays the icon in the navigation toolbar.

*City National Bank does not represent to you that the guidance given above is complete or, if followed, will protect you in all cases. You should consult your own internet security advisor.*

*"The way up" and blue ladder logo are registered trademarks of City National Corporation. All other trademarks are registered to their particular companies. Member FDIC. (8/2006)*