Member Best Practices: Online Security

Use a current web browser.

Be wary of suspicious emails. Carefully review any email requesting your account information and password, particularly if the email states that the information is needed to “award a prize” or “verify a statement.”

Avoid opening any questionable emails. If you have opened an email, do not open any attachments or links it may contain, and delete it.

Check up on the latest email fraud activity. The CUNA website, www.cuna.org, contains a special fraud alert link.

Protect your passwords. Memorize your passwords. Do not write them down or share them with anyone. Change them regularly and use combinations of letters, numbers, and "special characters" such as the "pound" (#) and "at" (@) signs. Do not use your Social Security number as a username or password.

Keep your computer operating system up to date. If your computer is more than five years old, its operating system (e.g. Windows 98, OS 7, etc.) may not offer the same level of protection as newer systems. System manufacturers provide frequent updates to help make your system more secure, possibly automatically through email or via your Internet connection. You may also check their websites, including:
Microsoft® – http://www.microsoft.com/security/
Apple Computer® – http://info.apple.com/

Install, run, and keep anti-virus software updated. Commercially available virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. Two of the most popular programs are:
McAfee® – http://us.mcafee.com
Symantec – http://www.norton.com

Use secure websites for transactions and shopping. Make sure the web page you are viewing offers encryption of your data. Often you will see a lock symbol in the lower right-hand corner of your browser window, or the web address of the page you are viewing will begin with “https://”. The “s” indicates “secured” and means the web page uses encryption.

Avoid downloading programs from unknown sources. Downloads from unfamiliar sources may contain hidden viruses that can compromise your computer’s security.

Disconnect from the Internet when not in use. Dedicated services such as DSL or high-speed cable provide a constant connection between your computer and the Internet. Even if you have a firewall installed, as an additional step to help protect yourself, disconnect from the Internet when not in use to avoid unwanted access to your computer's data.