Tips for Responsible Use of Online Banking Services

We proudly offer our Online Banking, Mobile Banking and telephone teller (MARS) services, and hope you take advantage of them so you have more access to your accounts and greater control over your finances. While use of these services may be indispensible in today's world, lack of responsible use may allow criminals to use these systems to steal funds and information from users who do not take some simple steps to protect themselves. Here are some simple steps you can take to protect yourself when conducting your banking online.

Usernames and Passwords

- Keep your username, password and security questions secure. Never write down your usernames or passwords, and make your password and the answers to your security questions easy for you to remember but hard for anyone to guess. And remember – never share your username, password or the answer to your security questions with anyone who you don't want to access your accounts online.
- Change your passwords. Whether or not you are forced to do so, make it a practice to periodically change your password so that it cannot be used indefinitely if it is compromised. Also, try to use different passwords on different websites. That way, the damage can be limited if one password is compromised.

Shopping Online

- Make sure you know who you are banking or shopping with online. Any website address where you provide account or card information should begin with "https://" (the "s" is important – it means that the website is secure!). Also, look for other indicators (which vary by browser) of the security features of the website, such as padlock icons, color changes, etc.

Emails and Phishing Attacks

- Never click links or attachments in unexpected emails. Scammers will always try to convince you that their schemes are legitimate by telling you a story such as you've won a lottery or inherited a sum of money. When you click that link or attachment, chances are good that you may infect your computer with malware and/or fall victim to a fraud rather than make some easy money! Remember-- if it looks too good to be true, it probably is!
- Accessing your account. The safest way to access your accounts online is to type our website address (www.heartlandcu.org) directly into your browser. Scammers can make links in emails look legitimate, but when you click that link you may end up at fake or malicious websites which may install malware on your computer.
- Never give out your account or card number to callers or emails supposedly from your financial institution. Legitimate financial institutions will never call or email you to ask you for account or card numbers – remember, they issued the number to you in the first place and already have that information!

Protecing Your Computer and Accounts

- Make sure you have all your computer's defenses installed and keep them up to date. Make sure you have anti-virus software and a personal firewall installed on your computer and/or network, and make sure they are kept up to date and running!
- If you have a wireless network, make sure it is password protected. Don't use public networks for online banking or shopping because these systems are usually not secure!
- Log off each time you access your accounts. If you just close your browser, you may not immediately log you off an online banking system. Computers infected with malware may continue to expose your account information after you close the browser unless you fully log off first. Also, close your browser when you are not online.
- Watch your accounts. Make sure you are routinely (at least monthly) reviewing your account history either online or with your paper statement. If you don't recognize a transaction, contact us IMMEDIATELY. This puts you in the best position to potentially recover funds taken from you through fraud.

Contacting the Credit Union

- Finally, contact us IMMEDIATELY at 800.362.3944 if you think your information has been compromised. Whether someone has obtained your username or password, you clicked a link in an email, or you gave out your account or card number, if you notify us right away we can help you protect yourself and your account from potential losses.