

Protecting Yourself Online

Online use is commonplace for most Americans. As your financial institution, we believe it's important to protect yourself and your personal identity online and offline. Here is some good advice when conducting business online.

Protecting Usernames and Passwords

- Keep your username, password and security questions secure. 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. Use a variety of passwords, so the damage can be limited if one password is compromised.

Evaluating Emails and Potential Phishing Attacks

- Never click links or attachments in unexpected emails. If you do, you may infect your computer with malware or a virus.
- The best way to access your accounts online is to type our website address www.appletree.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.
- Please remember: AppleTree Credit Union will never call, e-mail or text asking for personal account information such as your account number, social security number, PINs etc. It is standard banking practice that financial institutions never request this information in this manner, so never reply to any request from any financial institution.

Protecting Your Computer and Accounts

- 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.
- 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. Also, close your browser, or better yet turn your computer off, when you are not online.
- Review your account history either online or with your paper statement at least monthly. 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 AppleTree Credit Union

- If you think your information has been compromised, contact AppleTree Credit Union immediately at 414.546.7800. 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.



www.appletree.org
414.546.7800 | 262.896.8000