UNIVERSITY CREDIT UNION
Prepare • Progress • Achieve®

ONLINE SAFETY GUIDE

www.ucu.maine.edu • 800-696-8628

University Credit Union is committed to the security and confidentiality of your personal and financial information. With the increased speed and convenience of today's technology comes increased risk for fraud. You are your own best defense and the best way to begin safeguarding your financial information is to become informed about safe online practices. Here are some important tips to keep in mind while conducting business online:

• **Set strong passwords.** A strong password is at least 8 to 10 characters in length and is a combination of upper and lower case letters, numbers, and special characters. Do not use names, birth dates, telephone numbers, Social Security numbers, or anything that could be easily guessed. Avoid passwords that spell a word, name, or recognizable sequence. Change your password frequently. Never write it down or share it with anyone.

• **Never reveal personal information via electronic methods.** Do not use e-mail or text message to send information such as account numbers or your Social Security number. Beware of e-mails asking for personal Information. Legitimate companies will never e-mail to ask for your Social Security number, PIN, or password.

• **Remember e-mails and links are not always what they seem.** Do not open e-mails from an unknown source and avoid clicking on links embedded in e-mails, especially if you are prompted to login. These links could direct you to a fraudulent website. Instead, type in the web address in your browser before logging in. Beware of e-mail attachments from sources you are unsure of as these files can allow viruses or malware access to your computer.

• **Make sure the website is legitimate and secure.** If you navigate to an URL (web address) that you did not type in, take the time to verify that the URL you are viewing matches what you would expect. Fraudulent websites deliberately use URLs that are similar to the website they are imitating. Make sure a website is secure before submitting personal information online. A secure URL begins with https://.

• **Monitor your account activity.** Review your account history often and thoroughly review your monthly statements. Investigate any suspicious items and notify us immediately of unauthorized activity.

• **Keep your protection software up-to-date.** Install anti-virus, anti-spyware, and anti-malware programs on your computer. Keep these programs on and update them frequently. It is also helpful to confirm that your operating system (i.e. Windows) and browser (i.e. Internet Explorer, Firefox, etc.) have the latest security updates.

• **Avoid using public computers for financial activity.** Do not use public access computers to view your online banking account. Computers accessible to the public may be infected with malicious software or viruses.

• **Remember to log off.** When you are finished with a site, log off instead of just closing the page or your browser. Do not leave your computer unattended while you are logged in to a site.

Did you know that UCU...

- Offers eAlerts on Personal Finance Manager that can notify you via text or e-mail regarding pre-set transactions or events that take place on your account?
- Uses multi-factor authentication on Personal Finance Manager? You can deter fraud with your challenge questions, username, and password. Your security image and phrase confirms you're on the real UCU website.
- Has a fraud monitoring system in place to detect unusual transactional behavior? We'll contact you to confirm a transaction if it is suspected to be fraudulent. Be sure to notify us if you are travelling so your card isn't restricted due to unusual activity.
- Will never call, e-mail or otherwise contact you to ask for login credentials? We may, however, ask questions during a phone call to verify your identity.
- Keeps our members informed on our Fraud Alerts section of our website? Visit https://www.ucu.maine.edu/fraud-alerts for more information.

Contact UCU at (800)696-8628 with any questions or concerns about safe online financial practices. Notify UCU immediately if your account information has been compromised or if your debit card is missing or stolen.