CASE CREDIT UNION

Our service. Your success.

CASE Credit Union is committed to ensuring the safety of our members' information and our online banking environment is no exception. We are strongly committed to the safety and confidentiality of your records. However, everyday dishonest individuals are working hard to find new ways to scam the unsuspecting public. One of the best defenses against fraud is to remain educated. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

Tips on how to keep yourself safe in the internet environment:

1. **Set strong passwords.** A strong password is at least 8 characters long with a mixture of upper and lower case letters, numbers and special characters. Change your password regularly, do not give anyone your password or allow anyone else to use your password.
2. **Don't reveal personal information via e-mail.** E-mails and text messages can be masked to look like they are coming from a trusted sender. Do not send your account number, social security number, passwords or other personal information via e-mail or text messaging to anyone.
3. **Exercise website caution.** Be aware that if you navigate to a website from a link you don't type in, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify that the webpage you are visiting matches exactly with the URL that you'd expect. Contact CASE immediately if you suspect there is a problem.
4. **File downloads can be dangerous.** Opening files attached to e-mails can be dangerous, especially when they are from someone you don't know as they can potentially allow harmful malware or viruses to be downloaded on your computer. Make sure you have a good antivirus program on your computer that is up to date.
5. **Always log off.** When you are ready to leave a site you have logged in to, log off rather than just closing the page or browser.
6. **Monitor account activity.** Monitor your account activity regularly either online or by reviewing your monthly statements. Early detection is a key component in stopping fraud quickly. If there are any concerns, contact CASE right away.
7. **Assess your risks.** CASE encourages every member to do their own online banking risk assessment and put into place increased security controls where any weaknesses are found. Some items to consider when assessing your risk are:
    - **a.** Who has access to your online accounts?
    - **b.** How and where are your user names and passwords stored?
    - **c.** How strong are your passwords and how often are they changed?
    - **d.** Do you have a strong antivirus protection program that is up to date?

What to expect from CASE

CASE will never call, e-mail or send you a text message asking for any of your online banking credentials. CASE may inquire about your online banking credentials ONLY if you initiate contact and express online banking problems. CASE will never contact you and ask for your credit or debit card number, PIN or 3 digit CVC (security) code.

To verify card information CASE Staff may ask:

1. Last four digits of your social security number
2. Your date of birth
3. Your CASE account password (when applicable)

If you are uncomfortable with the call, please hang up and call the credit union at the toll-free number on the back of your card.

Rights and Responsibilities.
With respect to online banking and electronic fund transfers, the government has put in place rights and responsibilities for both you and CASE. These rights and responsibilities are described in the membership account agreement you received when you opened your account with CASE. You can also find them online under the disclosures link at www.casecu.org under the "**Electronic Funds Transfer Agreement**". If you notice suspicious account activity or experience security-related events, please contact CASE immediately at 1-517-393-7710.