Online Security Awareness

Align will never ask you to share your personal information by email or text messaging. Please do not respond to any communication that asks for information such as your account numbers, passwords, or any other personal identification information. Align ensures that we work hard to safeguard your information and have multi factor authentication to protect you when doing transactions online. Please report any suspicious activity or emails to info@aligncu.com or call us at 800-942-9575.

Protect yourself on online banking

- Never share your passwords or login information with anyone who is not on your account.
- Align requires complex passwords using letters, numbers, symbols, and upper and lower case. Try not to make it too simple.
- Do not use passwords that include your name, children's names, mother's name or their dates of birth or SSNs
- Never give out your member number, passwords, SSN, or date of birth
- Don't use public computers to access online banking
- Note that all online banking text alerts will come from membercare@aligncu.com. If you receive a text from any other email address, do not respond to the text and contact us immediately.
- Be sure to run full virus scans regularly. The quick scans don't always catch all viruses.
- Look for https in the URL when paying online or giving any personal information
- When selecting questions, make sure they are not something you post publicly on sites such as Facebook.
- If you use mobile banking, don't forget to password protect your phone and keep virus protection on there as well.
- Don't give out your information to websites that are not encrypted or secure
- Check account activity frequently and notify the credit union of any unauthorized transactions
- Review your account statements promptly
- Receive your statements electronically

What you can do

- Install the latest antivirus software on your computer
- Use firewall protection on your computer
- Download the latest Windows updates
- Be aware of the latest fraud tactics such as phishing and vishing
- Use Secure mailboxes to send and receive email
- Download signed applications only from a trusted source
- For mobile banking platforms using the Android operating system, do not enable Android's "install from known sources" feature
- Password protect your mobile phone
- Keep your mobile phone with you or secure the device when not in use
- Notify the phone carrier immediately if the mobile phone is lost or stolen so that it can be deactivated
- Do not modify the mobile phone as it may disable important security features
- Adopt safeguards such as not opening attachments or clicking on links contained in email from unfamiliar sources

Useful websites:
Federal trade Commission www.ftc.gov
On Guard Online www.onguardonline.gov
ID Theft Center www.idtheftcenter.org