1. I received an email that says it is from SECU, letting me know my account has been flagged. I was asked to click a link to authenticate my account. Is this safe?

No, it is not safe. If your account has been flagged for any reason, SECU will never ask you to authenticate your account via email. See example of fraudulent email to the right:

2. I Googled “SECU Login page” and wound up at a website, asking me to login. Why isn’t this safe?

Although a website appears to look safe, it may not actually be safe—a quick glance at the address bar will show that the website is NOT a SECU website. Always make sure that you see ‘secumd.org’ between ‘https://’, and the next ‘/’ in the URL address bar. See examples to your right:
3. I received an email from SECU about a new loan offering. There is a button in the email that asks me to click to learn more. How do I know the link is safe?

Don’t click links that you are suspicious of – hover your mouse over the button to see the full website link, and then determine if the link is safe. What looks like a legitimate hyperlink can be a disguised link to a criminal website. When in doubt, hover your mouse over the text of the hyperlink to see the full URL, which will verify it leads to a legitimate website. Better yet, open a browser window and manually type in the hyperlink yourself to prevent it being re-directed to an unsafe website.

4. I received an email from SECU about their new fundraiser. Is this email suspicious?

Yes – the spelling and grammar are poor, which is a red flag. The majority of social engineering pre-texts disguise themselves as a well-known company to make them appear trustworthy. These emails often have misspellings, improper grammar, or awkward wording that can be a sign that it is a scam. Large well-known organizations would not distribute an email with these types of errors. See example to your right:

5. I received the email to your right. Is this web link safe to click?

No – this email and web link are suspicious. A common tactic fraudsters use in phishing emails is to use urgent language and unreasonable consequences to inspire a victim to click on a malicious web link or attachment. Cyber criminals often include links to spoofed websites designed to
look like the legitimate website. If the victim enters their username and password into these sites, their credentials are recorded so that they can be used for account takeover. They may even ask you to select challenge questions and provide answers in an attempt to bypass two-factor authentication. It is best to use a one-time passcode, instead of challenge questions to further secure your online and mobile banking.

6. I received the email to your right. Is this a legitimate message from SECU?

Yes – this is a legitimate activity alert from SECU. There are no suspicious web links or attachments. There are no spelling errors, awkward formatting or obvious grammatical errors. The message does not include an urgent or threatening tone.

7. I received an automated phone call from SECU. The person let me know that there has been some unusual activity on my account they need to verify. They asked me to confirm my address, last four digits of my Social Security Number, and my member number. How can I tell if this phone call is safe?

Hang up – SECU will never call you to ask for sensitive details such as these. Scammers may call pretending to be from SECU. Never provide personal information like your date of birth, social security number, financial data, or other personal information in response to a robocall.