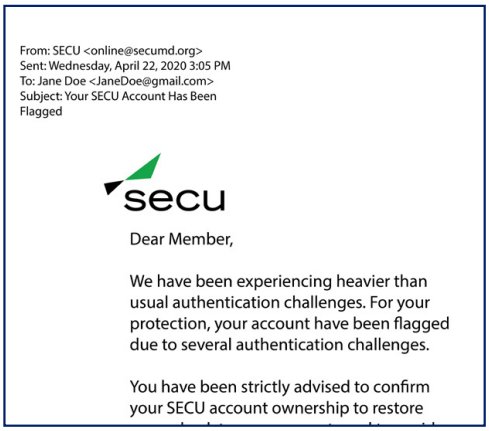
FRAUD FAQS

We're your partner in protecting your accounts and information against fraud. There are things you can do to help protect yourself against common fraudulent activities, now more than ever.

Please note: In order to enlarge images, download and open this document in a PDF viewer.

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:


From: SECU <online@secumd.org>
Sent: Wednesday, April 22, 2020 3:05 PM
To: Jane Doe <JaneDoe@gmail.com>
Subject: Your SECU Account Has Been Flagged

secu

Dear Member,

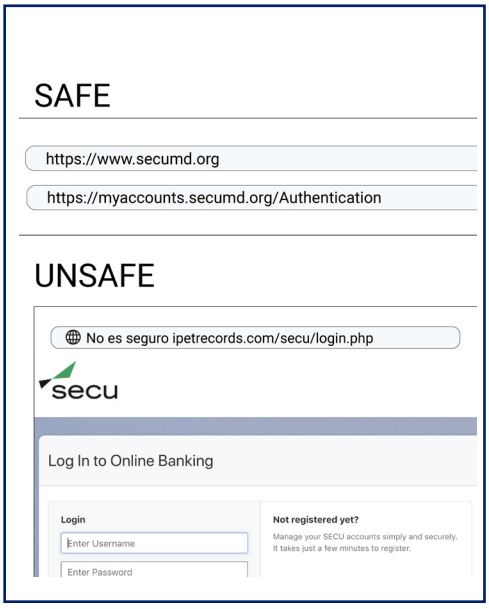
We have been experiencing heavier than usual authentication challenges. For your protection, your account have been flagged due to several authentication challenges.

You have been strictly advised to confirm your SECU account ownership to restore

Click the Image to Enlarge

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:



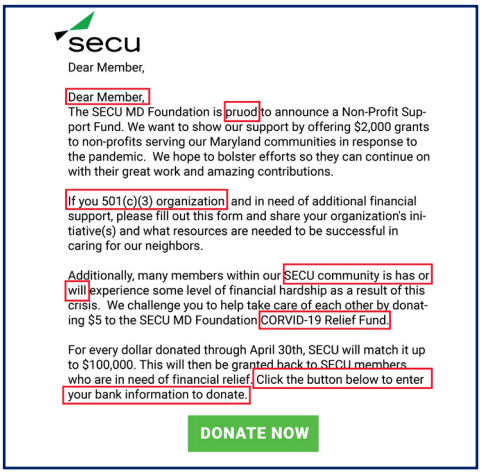
Click the Image to Enlarge

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:



secu

Dear Member,

Dear Member,
The SECU MD Foundation is pruod to announce a Non-Profit Support Fund. We want to show our support by offering $2,000 grants to non-profits serving our Maryland communities in response to the pandemic. We hope to bolster efforts so they can continue on with their great work and amazing contributions.

If you 501(c)(3) organization and in need of additional financial support, please fill out this form and share your organization's initiative(s) and what resources are needed to be successful in caring for our neighbors.

Additionally, many members within our SECU community is has or will experience some level of financial hardship as a result of this crisis. We challenge you to help take care of each other by donating $5 to the SECU MD Foundation CORVID-19 Relief Fund.

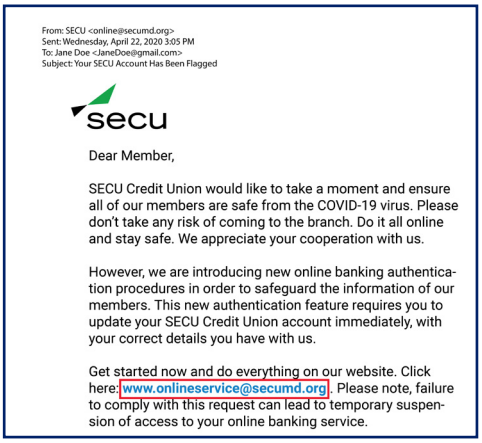
For every dollar donated through April 30th, SECU will match it up to $100,000. This will then be granted back to SECU members who are in need of financial relief. Click the button below to enter your bank information to donate.

DONATE NOW

Click the Image to Enlarge

5. I received the 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



From: SECU <online@secumd.org>
Sent: Wednesday, April 22, 2020 3:05 PM
To: Jane Doe <JaneDoe@gmail.com>
Subject: Your SECU Account Has Been Flagged

secu

Dear Member,

SECU Credit Union would like to take a moment and ensure all of our members are safe from the COVID-19 virus. Please don't take any risk of coming to the branch. Do it all online and stay safe. We appreciate your cooperation with us.

However, we are introducing new online banking authentication procedures in order to safeguard the information of our members. This new authentication feature requires you to update your SECU Credit Union account immediately, with your correct details you have with us.

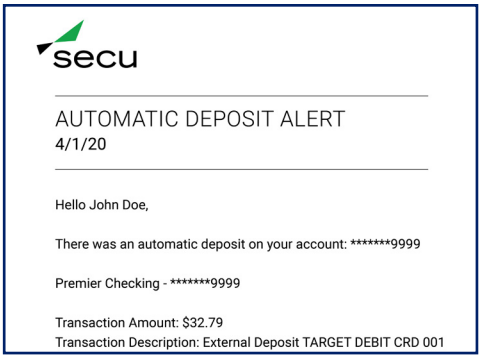
Get started now and do everything on our website. Click here: www.onlineservice@secumd.org. Please note, failure to comply with this request can lead to temporary suspension of access to your online banking service.

Click the Image to Enlarge

look like the legitimate website. If the victim enters their username and password into these sites, their credentials are recorded so that 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.



Click the Image to Enlarge

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.