DFCU will never ask you to give your personal and confidential information through an email, text, or voice message. If we initiate contact with you, then we already have this information on record and would have no need to ask you for it.

Cybersecurity

Cyber criminals do not discriminate; they target vulnerable computer systems regardless of whether they are part of a large corporation, a small business, or belong to a home user. Cybersecurity is a shared responsibility in which all Americans have a role to play.

The CISA Cybersecurity Awareness Program is a national public awareness effort aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each must do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

The CISA Cybersecurity Awareness Program Toolkit provides resources for all segments of the community. Those segments include:

- Students K-8, 9-12, and Undergraduate
- Parents and Educators
- Young Professionals
- Older Americans
- Government
- Industry
- Small Business
- Law Enforcement

Although CISA's website (Cybersecurity & Infrastructure Security Agency) is well informing and covers most if not all the cybersecurity related attacks and hacks and how to prevent and stop them, here are few tips to protect yourself against major cyberattacks.

➢ **Secure your computer, smartphone, and network**

- Install a firewall on your computer and/or network to prevent unauthorized access.
- Install and run anti-virus, anti-spyware, and anti-malware software on your computer and keep them updated.
- Change all default passwords on your computer, smartphone and network and create complex passwords.
- Note any changes in the performance of your computer such as a dramatic loss of speed, changes in the way things appear, the computer locks up or does not work correctly, unexpected rebooting, or anything out of the ordinary.

- **Be cautious when online**

- Never respond to an email or popup with personal information.
- Make sure you have a reasonable expectation of privacy prior to logging into a website.
- Never open attachments in unsolicited email.
- Never click on links in bulk email.

- **Be cautious when banking online**

- Designate a single computer (Always use the same computer) for your online banking.
- Dedicate a separate web browser to be used exclusively for online banking.
- Close all other browser tabs when banking online.
- Log off your online banking when not in use.
- Monitor and reconcile accounts daily for unauthorized transactions. Report any unauthorized transactions to your bank immediately.
- Discuss options offered by your financial institution to help detect and prevent abnormal activity.
- Never use your online banking password for any other online account or purpose.
- Never share your online banking logon credentials (user ID and password) with anyone.
- Never share your account number with anyone who does not need it.
- Never access your bank account using a public computer (e.g., at the library or a hotel business office).
- Never use a link in an email to visit a financial website. Always type the URL in the browser by hand.
- Be wary of an **unexpected** request for a one-time password or token in the middle of an online session.