National Cyber Security Awareness Month

Do your part, **#BeCyberSmart** throughout October for National Cyber Security Awareness Month (NCSAM). This year, OnPoint is expanding our annual cybersecurity awareness efforts to bring new resources to our membership and community. You can get started today by visiting onpointcu.com/financial-security and following us on Facebook, Instagram and Twitter and LinkedIn for relevant cybersecurity tips and advice throughout the month.

Protecting Your Finances

At the core of your financial security is a secure username and password. Here are guidelines for selecting a username and password to keep your accounts secure from cybercrime.

Selecting a Secure Username

Cybercriminals use common and easily guessed usernames, as well as usernames stolen through data breaches that attack websites. Once a username is validated, the hackers will attempt random passwords or use those stolen through breaches to gain access to new accounts. A unique and complex username can go a long way toward protecting you from brute force attempts.

> *Did you know?* Choosing a unique username will help you avoid a security lock on your OnPoint account. If a cybercriminal repeatedly attempts to access your account, it will be locked. Once your account is locked, we'll need to speak with you directly and verify your identity before unlocking your account.

Selecting a Secure Password

Updating and maintaining strong and unique passwords and keeping track of breaches on all of these accounts is impractical for most people. Most of the time, this leads to repeating passwords or storing unsecured or vulnerable password lists. However, maintaining strong passwords is essential for avoiding identity theft and keeping your financial accounts secure. If you're having trouble keeping track of all of your passwords, consider an encryption device or a reliable password storage service.

> *Did you know?* The average person has 90 digital accounts, and each is a possible avenue to some of your personal information. Keep your accounts safe with our strong password checklist—see back to learn more.

OnPoint® COMMUNITY CREDIT UNION

Strong Password Checklist

- ☐ **Does not contain:**
  - ☐ Birthdate, Social Security number, phone number
  - ☐ Names of friends, family, pets, favorite sports teams, etc.
  - ☐ Common terms or phrases (quotes, clichés, etc.)
  - ☐ Words from the dictionary
  - ☐ Adjacent keyboard combinations (qwerty, 456789, fghjkl)
  - ☐ Less than 10 total characters (letters, numbers, symbols)

- ☐ **Private.** Do not share your username or password with anyone—shared passwords increase the risk of fraud.

- ☐ **Unique.** Use a different username and password for each account—reusing or repeating credentials increases the risk of a fraudster obtaining your information. If an online retailer has a data breach, the credentials obtained from the breach will be used by hackers to attempt to gain access to other accounts using the same information.

- ☐ **Random.** A randomized password makes it harder for criminals to use computer software or knowledge of your personal information to guess your password.

- ☐ **Memorable.** Practice your usernames and passwords and commit them to memory so that you're able to recall your credentials when you need them. Consider using a passphrase with symbols swapped for some characters. For example: *"eYeL1kEf00+B@ll"* is complex, relatively easy to remember and significantly more secure than *"Ilikefootball"*.

- ☐ **Secured.** If you need to store your credentials, they must be stored securely. If you have a physical copy, keep it in a safe or secure place—if possible, write down hints instead of the usernames and passwords. For digital storage, use an encryption device or storage service and commit a single strong username and password combination to memory. If you use security questions, make sure that the answers cannot be found easily through social media or public records.

- ☐ **Variety.** Make use of all available characters in your password, including lowercase letters, uppercase letters, numbers and symbols.

- ☐ **Authentication.** If your password is guessed or stolen, two-factor authentication can create an additional layer of security. Often in the form of a short code sent via call or text to your phone number, dual authentication requires that a fraudster have access to your phone in addition to your username and password.

Here to Help Keep Your Accounts Safe

At OnPoint, we take your account security seriously. Please be aware, OnPoint will never ask for sensitive information via phone, email or text. This includes requests for passwords, secure access codes, verification codes, PIN or credit/debit card 3-digit codes. For more information, visit onpointcu.com/security.

Do your part, **#BeCyberSmart** by learning more about how to protect yourself from cybercrime with The OnPoint Guide to Personal Cybersecurity:

Scan the code and download the eBook today, or visit: **onpointcu.com/security-ebook**