OnPoint COMMUNITY CREDIT UNION

National Cyber Security Awareness Month

Do your part, **#BeCyberSmart** throughout October. You can get started today by visiting onpointcu.com/financial-security and following us on Facebook, Instagram, Twitter and LinkedIn for relevant cybersecurity tips and advice throughout the month.

Protecting your finances

Cybercriminals can use simple and stolen usernames to try to access personal accounts. Hackers will use software to attempt random passwords or use those stolen through data breaches to gain access to new accounts. A unique and complex username can protect 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 username and strong passwords

Maintaining unique usernames and strong passwords while keeping track of breaches on all of these accounts is challenging—this often leads to repeating usernames and passwords. However, avoiding identity theft and keeping your financial accounts secure starts with your login credentials. Consider an encryption device or a reliable password storage service to improve your overall digital security.

DID YOU KNOW?
The average person has 90 digital accounts, and each is a possible avenue to your information. Keep your accounts safe with our strong password checklist—see back to learn more.

Strong Password Checklist

(Password | Username)

- [ ] **Private.** Do not share your username or password with anyone—shared passwords increase 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.
- [ ] **Random.** A randomized password makes it harder for criminals to use computer software or personal information to guess your password.
- [ ] **Memorable.** Memorize your username and passwords. 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.** Store credentials securely. If you have a physical copy, keep it in a safe place—consider using hints instead of documenting usernames and passwords. For digital storage, use an encryption device or storage service. Commit a single strong username and password combination to memory.
- [ ] **Variety.** Use all available characters in your password, including lowercase letters, uppercase letters, numbers and symbols.
- [ ] **Authentication.** Two-factor authentication creates 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 access to your phone or other secure device.

Does not contain:

- [ ] Birthdate, Social Security number, phone number
- [ ] Names of friends, family, pets, favorite sports teams, etc.
- [ ] Common terms or phrases (i.e., quotes, clichés, etc.)
- [ ] Words from the dictionary
- [ ] Adjacent keyboard combinations (i.e., qwerty, 456789, fghjkl)
- [ ] Less than 10 total characters (letters, numbers, symbols)

Here to help keep your accounts safe

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, PIN or credit/debit card 3-digit codes. For more information, please 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