OnPoint COMMUNITY CREDIT UNION

OnPoint's guide to creating strong usernames and passwords.

Now's the time to take action and protect your finances. 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.

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

With so many accounts managed online, it's tempting to repeat your use of login credentials. However, new technology makes it easier for hackers to test one set of stolen credentials on multiple sites, so it's important to use unique usernames and passwords—or better yet, passphrases—for each of your online accounts. You can also consider using 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 username and password checklist.

(Password | Username)

- [ ] **Memorable.** Practice your username and passwords and commit them to memory so 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".
- [ ] **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. If an online retailer has a data breach, the credentials obtained from the breach may be used by a hacker to attempt to gain access to other accounts using the same information.
- [ ] **Secured.** If you need to store your credentials, they must be stored securely. If you have a physical copy, keep it in a safe 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.
- [ ] **Updated.** Changing your passwords every three months can help secure your accounts, especially those holding some of your most sensitive information.

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)

OnPoint COMMUNITY CREDIT UNION

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.

Learn 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