



Partnership • Trust • Community

## It's Time to Discuss Passwords

July 2025 | Issue No. 23

---

Who owns the security of your information?

The answer is that *security is everyone's responsibility* – including you and the businesses that secure your email address online or physically. That may be a big group. Think about how often you log into a website using your credentials. Now, think about how often you reuse the same password.

Odds are, hackers are thinking about it. Between April 2024 and April 2025, in the US alone, security breaches gave threat actors access to 184 million consumer passwords, according to a recent *Yahoo Moneywise* article.

The cybercriminals obtained email addresses, passwords, and login links “tied to major platforms like Apple, Google, Facebook, Microsoft and even government and financial services,” according to the article.

Those credentials can be used to obtain more information about the victims with the goal of accessing their bank accounts.

With so many entities in possession of your credentials, password security is something that you need to manage – but how? By arming yourself with knowledge and making your passwords hard to hack.

### Key Facts:

- The Identity Theft Resource Center (ITRC) Annual Data Breach Report recorded 3,205 cyberattacks (8.7 per day) leading to data compromises in 2024.
- 90% of dark web “access for sale” listings feature stolen credentials, and 60% of Americans reuse passwords. More than four million people use 123456 as a password. (Spacelift)
- According to security researcher, Troy Hunt, 14,986,167,586 passwords and 896 websites have been identified as compromised. (<https://haveibeenpwned.com/>)

### Baseline Security Tips

- The National Institute of Standards and Technology (NIST) recommends passwords of at least 12-16 characters. Some organizations, such as the Cybersecurity and Infrastructure Security Agency (CISA), recommend even longer passwords. At a minimum, passwords should be:
  - **Long** – at least 16 characters (even longer is better).
  - **Random** – use a string of mixed-case letters, numbers and symbols or a passphrase of 4 – 7 random words.
  - **Unique** – used for one and only one account.

- Use Multi-Factor Authentication wherever possible, especially when accessing websites linked in financial records. (<https://www.cisa.gov/MFA>)
- Frequently change your passwords using the above criteria.
- Never click on links or attachments in emails that you are not expecting.

## Common Email Themes

Be aware of the techniques scammers commonly use in emails:

- Urgent messages
- Generic greetings
- Suspicious claims
- Unrealistic promises
- Threatening language
- Typos and grammatical errors
- Suspicious links
- Unsolicited attachments
- Requests for personal information:
- Impersonation of a legitimate organization

## If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to the Internet Crime Complaint Center, (<https://www.ic3.gov>), the police, and file a report with the Federal Trade Commission. (<https://www.identitytheft.gov>)

## Getting Help

If you need help and have identified suspicious activity involving All One Credit Union, contact us immediately at 800-649-4646.