UNITE CREDIT UNION

Quick Links

Website | Rates | Applications | Contact Us

Password Safety: Are Yours Secure Enough?

Most of us have seen the message pop up more than once: “your password needs to be at least 8 characters long,” or something similar.

It might make you roll your eyes but remember: passwords need to be strong in order to help secure your personal information - including emails and files.

Most people know the risks of flimsy passwords. But even knowing the risks hasn’t necessarily changed our behavior. In past years, “123456” and “password” topped the list of the worst passwords of the year, released annually by password management provider Splash Data. Unfortunately, passwords continue to be one of the most common ways hackers break into computers and personal data according to this article from Equifax.

By guessing passwords, hackers can give themselves an all-access pass to your financial accounts, personal documents and files, and possibly your other devices – especially if you reuse passwords across different sites.

It’s no surprise we do reuse them, given the number of sites requiring a login with a password. More than half – 60 percent -- of 3,000 adults surveyed by Google and Harris Poll said they have too many passwords to remember. And 65 percent of respondents to the survey said they reuse the same passwords for multiple accounts.

Even using a slight variation on the same password may not make it harder for hackers, and they may be counting on us to take the easy way out. Reusing passwords, even with slight variations, is like moving your house key from under the doormat to under a flower pot: it may not be secure enough.

If a hacker can access your personal data, they may be able to steal your money – or your identity. If you’re a business owner, cyber criminals can sneak into your data and access client and customer information.

So where do you start? Here are some suggestions for creating and storing passwords:

Creating a strong password

1. Make it memorable – for you.

You can come up with a phrase and turn it into a password by only using the first two digits or first digit of each word:
Example: “My first concert was Blink-182 in Los Angeles. Tickets were only $15”
Password: MyficowaBl182inLoAnTiweon$15.

2. Make it unique.

Use a different password for every important online account you have, such as bank accounts, credit card, and emails. If you can, use a different password for every single account. One way to make it easy to keep track of each password is to use the first letter of the channel or website to begin the password, or something similar so you can easily relate it to each account.

3. Make it longer.

Longer passwords are stronger and much harder for hackers to guess. Use a “pass phrase” you would remember that no one else would. It could be a string of seemingly random words with numbers and symbols, like oneDay2WeCan$G0totheM00n. Aim for at least 16 characters.

4. Avoid personal information and common words.
As you create longer passwords, remember to avoid using personal information like nicknames, names of children or pets, birthdays, or address information. Also avoid common words such as “letmein” or “password,” and avoid keyboard patterns like “qwerty.”

5. Make it complex.
Including upper and lowercase letters, special characters, and numbers are all ways you can make your passwords more complex and harder to guess or hack. Avoid using words that could be found in a dictionary. You can try breaking up a word with a special character or string of numbers. Put your symbols and numbers throughout the password and not just at the beginning or end.

6. Use a password generator.
A password generator can help you create a truly random character combination. There are a number of password generators online. Some are web-based and some need to be downloaded.

7. Consider using two-factor authentication when possible.
Many accounts and applications now offer two-factor authentication. This means you take another step to log in, such as enter a code sent by text to your phone, or you may use your fingerprint. Some other accounts require two-factor authentication if you are connecting from a new device or resetting a password. Consider enabling it when you can. It is an extra step to log in, but it can add an extra layer of security to your accounts.

Strong passwords

Now that you’ve conquered creating a secure and strong password, you’ve just got to remember it (along with all the others)! Mentally keeping track of each password can be difficult, here are a couple ways you can make it easier while keeping your passwords secure:

1. Use a password manager.
In the Google survey, only 24 percent of respondents said they use a password manager, despite many respondents saying they need a better way to track passwords. You can download a password manager for free or pay for a more robust option. Most password managers use encryption to store your data and can sync across all of your devices. They may also come with password generators. Most managers generally require you to simply remember one password: the one you need to get into the manager account.

2. Let your device, browser, or app remember.
Your mobile device may have the ability to auto-fill some passwords and come up with unique strong passwords once you use your fingerprint or a face scan to unlock that capability. In addition, some apps have a “remember me” function, requiring you to sign in

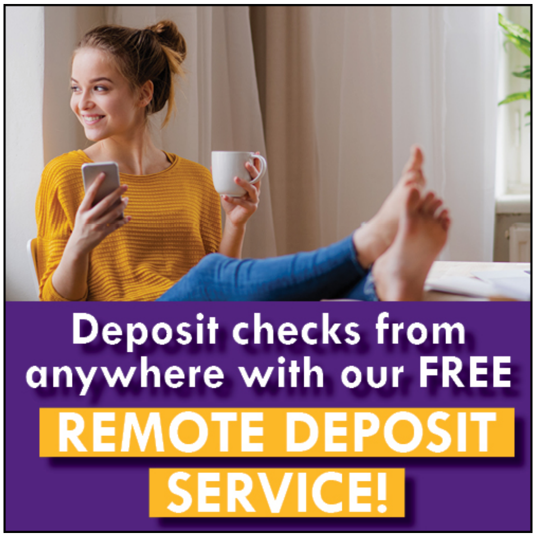
with a username and password once, then using your fingerprint or face scan to sign you in afterward. The key here is to have a strong overall password or passcode on your device. For example, automating passwords might not be a good idea if your passcode is something easy to guess, like “1234.”

3. Lock it up.

If you do need to write your passwords down, don’t create a document on your computer or leave a physical piece of paper near your desk. Instead, store a piece of paper in a secret place or lock box.

We all juggle multiple passwords each day, and sometimes struggle with forgetting them. But taking a few moments to create strong passwords storing them as securely as possible can help make your personal information more secure.

Article source.



About UNITE Credit Union

UNITE Credit Union was established in 1955, and since then has provided financial services to the students, parents of students, alumni, faculty, staff & retirees of the University of Northern Iowa; the employees, families & retirees of MidAmerican Energy & the students, parents of students, alumni, faculty, staff & retirees of the Cedar Falls School District.

Federally insured by the NCUA. Equal Housing Opportunity. NMLS 530628