Creating Strong Passwords

Passwords are the first line of defense in protecting you against cyber criminals (hackers) while conducting online transactions (i.e. banking, paying bills, or making purchases). If hackers gain unauthorized access to your computer, they can view your personal information; impersonate you and send messages to your friends; change your password to block you from accessing your own account; steal your identity; or infect your files with viruses. Therefore, it is vital to pick strong passwords that are different for each of your accounts and to update your passwords regularly.

Update your passwords regularly.

Here are some tips that will help protect your online transactions:

Use a unique password for each of your important accounts like email and online banking

Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office – if a criminal gains access to one, all three are compromised and can lead to identity theft. Do not use the same password for an online newsletter that you use for your email or bank account. It may be less convenient, but picking multiple passwords keeps you safer.

Create a strong password by combining numbers, letters and symbols

Strong passwords are easy to remember but hard to guess. Make your password strong to help keep your information safe. Adding numbers, symbols and mixed-case letters makes it harder for cyber criminals or others to guess your password. Do not use obvious passwords like '123456' or 'password,' and avoid using publicly available information like your phone number or the name of a pet, a child or another familiar person. Likewise, avoid things that can be looked up, such as your birthday or ZIP code.

Longer = stronger. Your passwords should be a minimum of 8 characters, but the longer you can make them, the harder it will be for a thief to crack your codes. While it is best to avoid using real words as part of your password, if you do, you can try substituting characters for some of the letters, e.g. $ for an S, or a zero for an O. Another way would be to insert a string of characters or numbers in the middle of a real word, thus breaking it up into two non-words.

Try using a phrase that only you know

You could start with "**My friends Mary and Jack send me a funny text message every day**" and then use numbers and letters to recreate it into this: **MfM&Jsmaftmed** – a password with many variations that will be hard for cybercriminals to figure out. Another example would be something like **Iam:)2bH!** – this has 9 characters and says "**I am happy to be here!**" Come up with a system to create your own passphrases. That will make it easier to create new passwords as well as help you remember them.

Adding a cell phone number

Sometimes you can add a phone number to your profile to receive a code to reset your password via text message. Having a mobile phone number on your account is one of the easiest and most reliable ways to help keep your account safe.

For example, service providers can use the phone number to challenge those who try to break into your account, and can send you a verification code so you can get into your account if you ever lose access. Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.

Turn on two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

Choosing a unique security question

If you cannot, or do not want to, add a phone number to your account, many websites may ask you to choose a question to verify your identity in case you forget your password. If the service you are using allows you to create your own question, try to come up with a question that has an answer only you would know and is not something that you have posted about publicly or shared on social media. Try to find a way to make your answer unique but memorable – so that even if someone guesses the answer, they will not know how to enter it properly.

Set up your password recovery options and keep them up-to-date

If you forget your password or get locked out, you will need a way to get back into your account. Many services will send you an email at a recovery email address if you need to reset your password. Make sure your recovery email address is up-to-date and is an account you can still access, or have it sent by text to your mobile device.

Never tell a web browser to remember a password

If a criminal gains access to your computer, they may be able to access your online accounts by going to your favorites list and letting the web browser enter the correct password for them.

Keep your passwords in a secret place that is not visible

Writing down your passwords is not necessarily a bad idea, but make sure you put those notes in a secure area. Do not leave them in plain sight or easily accessed.

You may want to consider using a password manager. The most basic password managers are like a lockbox or vault in your computer. You can create unique, complex, strong passwords, even ones you would never remember, for each website you log in to. The manager remembers and stores them so when you need them, the manager enters your login information, including the password, so you can safely log in.

These passwords are stored in the manager, secured by one master password that you will need to remember. This facilitates creating strong passwords that you do not have to remember. A much better way to safely store your collection of passwords than writing them down on a piece of paper! You will need to research the various products available to see which one has the right combination of features that will work best for you.

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftPasswordsCreating658 (rev 10/23)