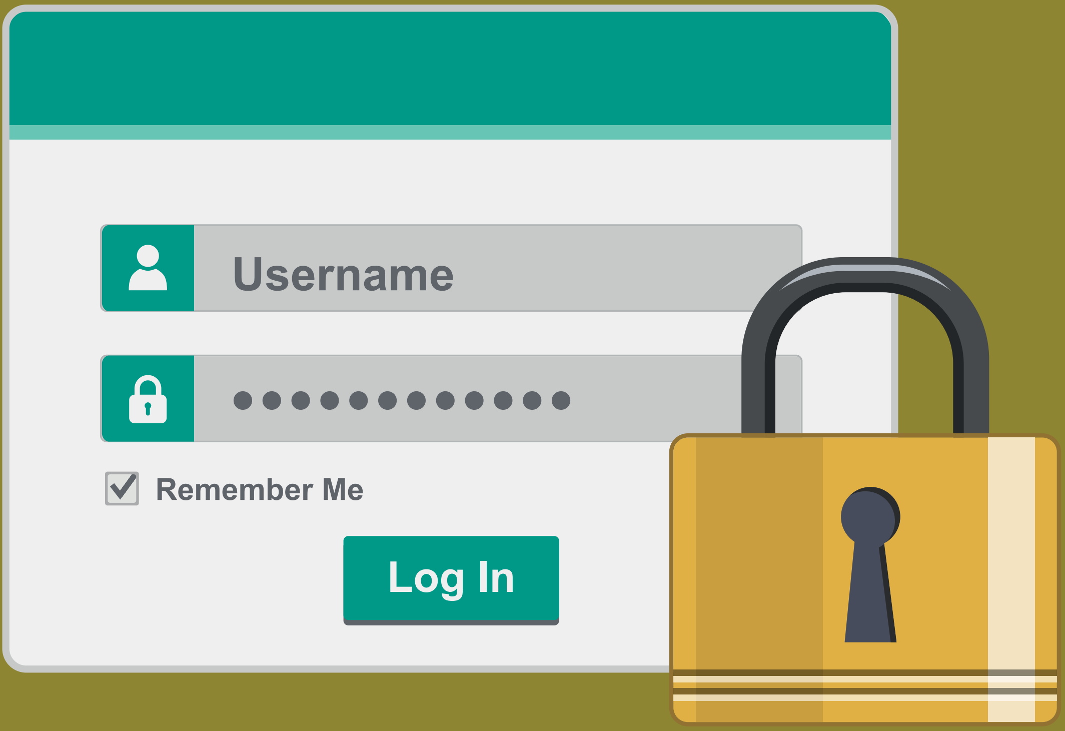


Passwords

Passwords

Passwords are the keys to your kingdom, use them wisely. In this newsletter, we discuss how to create strong passwords that cyber attackers cannot easily guess and how to use them securely.

This newsletter is endorsed by The American University in Cairo, Office of Information Security

For more information, please contact us at:
StaySecure@aucegypt.edu

Passwords

Your passwords are the key to securing your systems, your accounts, and our organisation. Reinforce your shield by using passwords securely. To begin with, you should create and use only strong passwords. Cyber attackers have developed sophisticated methods to guess or brute force passwords, and they are improving constantly. This means they can compromise your passwords if they are short or easy to guess, such as your pet's name. The more characters your password has, the stronger it is and the harder it is for an attacker to guess. However, long, complex passwords can be difficult to remember. To help you create strong passwords that are easy to remember and type, we recommend you use passphrases. Passphrases are nothing more than a sentence or random words. For example, you can use the passphrase

How cold is today?

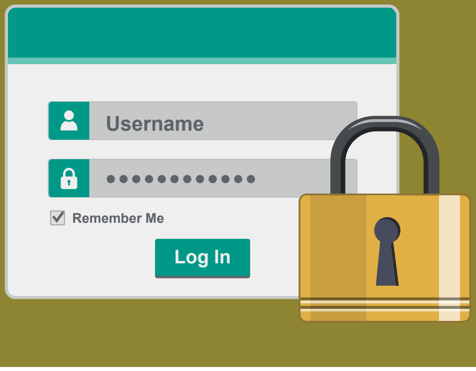
Notice how many characters this password has, yet it's easy to both type and remember. You can make any password or passphrase even stronger by replacing a letter with a number, such as replacing the letter "o" with the number "0," using lower and upper case letters, or adding symbols, such as spaces or punctuation. In addition to creating strong passwords, be careful how you use them. Here are several key steps that will protect your passwords.

Use a different, unique password for each of your accounts. That way, should one of your accounts be hacked and your password compromised, your other accounts will still be safe. Can't remember them all? Consider using a password manager. This is a special program that securely stores all of your passwords for you. You only need to remember the password to your password manager. Check with your supervisor or help desk whether or not a password manager is acceptable to use.

Many online accounts offer something called two-step verification. This is where you need something other than just your password to log in, such as a code sent to your phone or codes generated by a token. Where possible, always use these stronger methods of authentication. Solutions like two-step verification are one of the most effective steps you can take to protect your accounts.

Never share your password with others, including fellow employees. Remember, your password is a secret; if anyone else knows your password, it is no longer secure.

Passwords



Do not use public computers, such as those at hotels or libraries, to log into sensitive accounts, such as those at work or your online bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log in to sensitive accounts from trusted computers or mobile devices you control.

Be wary of websites that require you to provide answers to personal questions. The questions are used if you forget your password and need to reset it. The problem is, the answers to these questions can often be found on the Internet. Make sure that if you answer personal questions, you only use information that is not publicly known.

Should you accidentally share your password with someone else, or believe your password has been compromised or stolen, change it immediately and contact the help desk or information-security team.

Don’t Get Infected

One of the most common ways passwords get compromised is by getting your computer infected. Cyber attackers have developed malware that silently captures and logs all of your keystrokes once it infects your computer, including all of your logins and passwords. It does not matter how strong or long your password is; if someone can monitor all of your keystrokes, they can steal your account information. Once they steal your logins and passwords, they simply log in as you to any of your online bank, email, or social media accounts. This is why it’s so important to protect both your computer and mobile devices. It may sound odd, but one of the most important steps you can take to protect your passwords is to avoid getting infected.

This newsletter is endorsed by The American University in
Cairo, Office of Information Security

For more information, please contact us at:
StaySecure@aucegypt.edu