Objective 7

Password Security

GETTING STARTED WITH TECHNOLOGY

WHAT YOU NEED TO KNOW

Username and password data has become some of the most sought-after information online. Internet traffic has continued to grow, with individuals seeking out sites on shopping, news, athletics, and social media throughout the day. Because of the increased online presence by so many, there is also an increased risk of personal information becoming misused or stolen by someone else. Because we use the internet for everything from shopping to mortgages, there are more opportunities for misuse or deception by others.

It isn't possible to 100% guarantee your safety when online, but there are several ways to protect yourself and your personal information. Simple measures like not using the same password for multiple web pages and changing your passwords frequently can decrease the changes of information getting breached.

HOW THIS HELPS YOU

By utilizing best practices when it comes to passwords, you can better secure your information and data online. Creating long, unique passwords for different websites, changing your passwords frequently, and enabling multi-factor authentication can all increase your security while online. Utilizing a password management tool can help you maneuver this task.

TIPS & TRICKS

Don't Share Passwords
Keep your login credentials private and do not sure your username or password with other individuals.

Never Use Personal Information or Real Words
Cybercrimials use algorithms and software to guess passwords, so avoid using real words and personal information to make a more secure password. Utilizing a phrase as a password is best.

Don't Reuse Passwords
A cybercriminal with an ID/password will likely try that same combination on other websites and accounts. Limit your passwords to a single site.

Use a Password Manager
Password managers can store usernames, passwords, account information and payment information so you don't have to remember them all.

Prioritize Password Length
Make your passwords longer and stronger to get the most protection.

Enable Multi-factor Authentication
Multi-factor authentication, or two-factor authentication, utilizes a second method to verify who is logging into an account. This is usually done by sending a code to a mobile device via text, to an email address or with a second verification question.

THINGS TO KEEP IN MIND

Social media is a great tool to stay in touch with friends and family. It is important to remember important tips to maintain safety. In addition to remembering privacy settings, oversharing can also help hackers guess passwords or better understand your schedule and daily habits.

First, some individuals share too much information online: updating location, shopping habits, or promoting a website. This gives online attackers information about someone and possibly how to gain access to some account information.

A second issue is that individuals often will reuse a password for multiple social media platforms. Therefore, if a password is hacked on one form of social media an attacker can quickly try that same password elsewhere to see if it was reused.

Our emails are also a place where suspicious activity can be found. Electronic messaging can pose a risk to someone's passwords and online security. Many online attackers will attempt to gain information from an email by posing as a reputable person or business. If they can persuade you to share information, sometimes even a minor detail, they can gain access to other sensitive information.

Typical good-standing businesses will not ask you to share your username or password without you prompting them to do so. Therefore, if someone is using email to ask for a password or username, it is possible that someone is attempting to get some personal data. If there is doubt about the authenticity of an email, attempt to validate the information.
Start by contacting someone trusted that might know more about the message in question. It can also be helpful to verify any links in an email by copying and pasting the link somewhere to see if the text written in the message match the web address in question.

RESOURCES

National Institute of Standards and Technology
https://pages.nist.gov/800-63-3/sp800-63b.html#appA

Security.org Password Tester
https://www.security.org/how-secure-is-my-password/

CNET - Best Password Manager
https://www.cnet.com/tech/services-and-software/best-password-manager/