Cyber Security Guide

Protecting logins

Your login information (your "credentials") is the first stage to protecting your digital life from being hacked or compromised.

Usually, your username will be your email address, but sometimes it's just a shorter name. The advantage of your email address is that its unique; the disadvantage is that it's often public knowledge. If you have the choice, we'd recommend using either a short-form username or a unique email address for that service. Some email providers, such as Apple, allow you to hide your email address or create multiple aliases, which means if the service you are using gets hacked, the hackers will have, at most, your username for that single service and not your entire digital life.

When it comes to choosing a password, it should be unique for that service (never re-use passwords) and be sufficiently hard to guess. Never use single words or personal information, and **we recommend using a password manager app** to help you store, generate or remember them. Password best-practice has changed in recent years, and the thinking is that now, if you are using good, unique passwords, there is no need to change them regularly, provided the service you are using hasn't been compromised. One of the most popular current recommendations is to use three random words together, e.g. "LuckyMachineWeather"

Username and password security can be greatly enhanced with Multifactor authentication (MFA). It is a security mechanism that requires the user to provide multiple forms of identification to access a digital account or system. This authentication method adds an extra layer of security to the login process and helps to ensure that only authorized users can access sensitive information.

MFA typically requires the user to provide two or more of the following factors of authentication:

- Something you know, such as a password, PIN, or security question
- Something you have, such as a security token, smart card, or mobile device
- Something you are, such as biometric identification like fingerprint, facial recognition, or iris scan

By requiring multiple factors of authentication, MFA significantly reduces the risk of unauthorized access to an account, even if one of the factors is compromised. For example, if a hacker obtains a user's password, they would still need to provide additional authentication factors to gain access to the account.

Nearly every service supports MFA, but it's not always turned on by default, so search the settings or help for MFA or 2FA and turn it on. Critical services such as your email accounts should always be protected with MFA, as if they are compromised it's likely the hackers would have access to all your services via the "I've forgotten my password" option.