THE ROMAN CATHOLIC ARCHDIOCESE OF ATLANTA

INFORMATION TECHNOLOGY
ARCHDIOCESE OF ATLANTA

# Password Managers

## What is a password manager?

A password manager is a technology tool that helps internet users create, save, manage and use passwords across different online services.

Many online services require a username and password to create an account and gain access to a specific service. Over time, users face a recurring choice: create unique passwords for each site, a challenge to remember, or reuse a single password repeatedly, a challenge to secure.

If a site is breached, exposing usernames and passwords, attackers try those passwords on other sites. These tactics accounted for nearly half of the cyber-attacks in the past few years. Of course, sometimes, users simply forget a password, and the password reset cycle takes time, diminishing a user's overall experience.

A password manager is an attempt to improve password usability and security, enabling users to create unique, complex passwords for every online account without needing to remember them. All information is securely stored in a password vault and accessible via the password manager.

Password managers also help users manage accounts for online services and include the site or service name, web address, user account name and password. This makes a password manager crucial, even essential to users dependent on a variety of services requiring usernames and passwords.

## How does a password manager work?

The first time a user visits a site that requires a username and password while using a password manager, various outcomes can occur.

If the user has not previously created a username and password for the site, the password manager can help create a highly randomized and unique password. When the user puts the cursor in the input field for the password, the password manager prompts the user to create a new, strong password. Once the username and new password have been entered, the password manager typically prompts the user to save the information. The username and password are then securely stored in the password manager. The next time the user visits the same site, the password manager opens a prompt window, typically above where the user input is required, asking if the user wants to input the previously saved information.

On the other hand, when the user already has a username and password but visits a site for the first time with a password manager installed, it prompts the user to save account information for future visits.

June 2024

**How does a password manager detect if a password is needed?**

Websites generally use a standard Hypertext Markup Language form for the username and password fields. Password manager technologies detect that username and password fields are present. The password manager also identifies the web address visited, matching it to a list of known credentials and determining if a password credential can be input or if a new password is needed.

Browser developers and third-party password managers have different mechanisms for detecting username and password fields. Google has published a set of best practices to help developers build reliably detected username and password forms. Third-party password manager tools, including both 1Password and LastPass, have also published information to help developers build compatible forms.

**How does a password manager secure access to passwords?**

Password managers themselves need to be secured as well, typically with a master password used to access the password manager. Additionally, the best password managers use multifactor authentication (MFA) or two-factor authentication (2FA), such as a second password or a biometrics measure, like facial recognition. All username and password information in the password manager is typically secured with Advanced Encryption Standard 256.

strongdm