Password Management & Security

A Practical Guide for Individuals, Businesses, and Ministries
Prepared by LaFaries Mortimer LLC

Why Passwords Matter

Passwords protect far more than just email accounts. They guard financial data, personal identities, ministry records, donor information, internal systems, and private communications. Weak or reused passwords are one of the most common causes of data breaches and identity theft.

In many cases, cyber incidents are not caused by advanced hackers but by simple mistakes such as reused passwords, predictable patterns, or storing credentials in unsecured locations.

Common Password Mistakes

Many people unknowingly weaken their own security. Common mistakes include using the same password across multiple platforms, choosing passwords based on personal information, storing passwords in plain text files, or sharing credentials via email or text message.

Even passwords that seem complex can be compromised if reused or exposed through a breached website.

How Passwords Are Compromised

Passwords are often stolen through phishing emails, fake login pages, malware, or data breaches from third-party services. Once obtained, attackers frequently test stolen passwords across multiple sites to gain broader access.

Because of this, unique passwords for every account are essential.

Creating Strong Passwords

A strong password is long, unique, and unpredictable. Length is more important than complexity. Passphrases made of multiple unrelated words are often stronger and easier to remember than short complex strings.

Avoid using names, dates, locations, or repeated patterns. Each account should have its own unique password.

Password Managers

Password managers securely store and generate passwords so users do not need to memorize each one. They reduce risk, improve consistency, and make secure practices practical for daily use.

When used properly, password managers significantly reduce the likelihood of credential compromise.

Multi-Factor Authentication (MFA)

Multi-factor authentication adds an additional verification step beyond passwords, such as a mobile app approval or security code. Even if a password is stolen, MFA can prevent unauthorized access.

Whenever available, MFA should be enabled for email, financial, and administrative accounts.

If a Password Is Compromised

If you suspect a password has been exposed, change it immediately, review recent account activity, and update any other accounts that used the same or similar credentials.

Regular reviews and updates help maintain long-term security.

Prepared by LaFaries Mortimer LLC

Professional administrative and IT guidance for modern organizations.