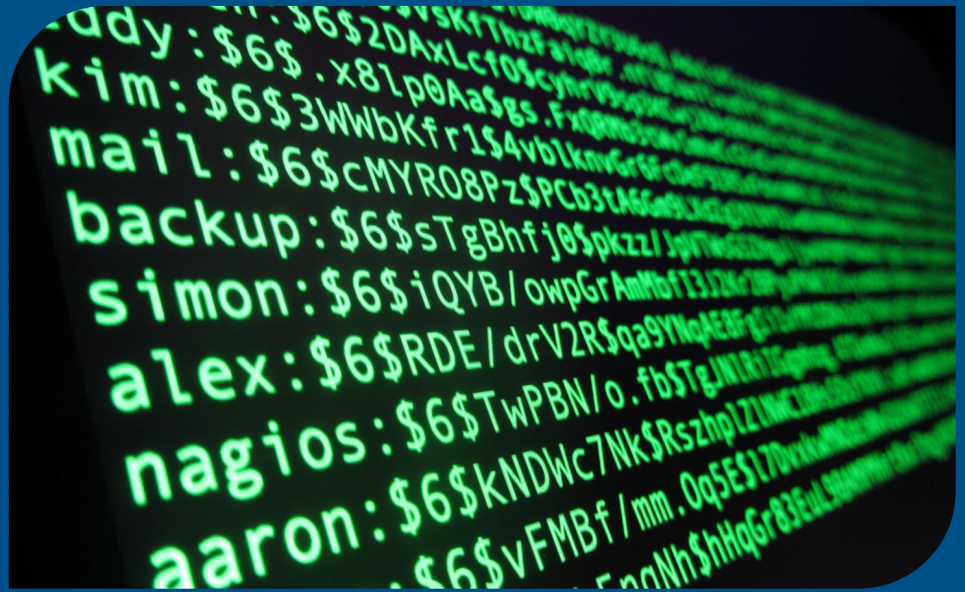
Galway IT
Meetup

Committing to Better Passwords

A Guide to Professional + Personal Security Habits



Aisling Krewer

Galway IT Meetup

Not your standard security training

How one small change saved me a ton of headaches and time at home and work

Aisling Krewer

This doesn’t really apply to me.

Everyone reused passwords.

Many people reused passwords for personal and work accounts.

Almost nobody used a password manager.

You are high value targets.

If you work in the tech space, you are a potential target.

Access to codebases, production systems, and/or sensitive data.

Even internal documentation is useful.

Threats

Phishing

Public Wi-Fi

Credential Reuse

Hey, we were promised an easy solution.

Password Managers!

Benefits:

- Remembers your passwords so you don’t have to
- Browser extensions generate passwords and autofill
- Works and syncs across platforms
- Many notify you if the log in has been connected with a leak
- Warn about password reuse

Password Managers

- 1Password (Paid)
- BitWarden (Free for personal)
- ProtonPass (Free)
- Dashlane (Free, with limits)
- NordPass (Free)
- Built in browser options

MFA
(Multi Factor Authentication)

Benefits:

- An important second layer of defence
- You'll still need to change your password, but it will stop attackers getting access

Types of MFA:

- Hardware tokens (e.g., YubiKey)
- App-based authentication (e.g., Authy, Google Authenticator)
- Avoid SMS when possible
  - Most vulnerable
  - Sim-Swapping
  - Lack of Encryption
  - Most importantly - network outages

To Conclude

Use a password manager for work and personal accounts

Enable MFA on critical systems and personal accounts.

Regularly check for leaked credentials.

Avoid reusing passwords across accounts.