

Password Management

Shelley Garrett - Compliance and Assurance Analyst
Office of the Chief Information Security Officer
University of Alberta



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES

VS

SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES

1. USE ANTIVIRUS SOFTWARE



2. USE STRONG PASSWORDS



3. CHANGE PASSWORDS FREQUENTLY



4. ONLY VISIT WEBSITES THEY KNOW



5. DON'T SHARE PERSONAL INFORMATION



1. INSTALL SOFTWARE UPDATES



2. USE UNIQUE PASSWORDS

2

3. USE TWO-FACTOR AUTHENTICATION



4. USE STRONG PASSWORDS



5. USE A PASSWORD MANAGER

Why should I install Updates?



What is MFA?



123456 Reasons to change your password

25 Of The Most Popular Passwords

| | | | | | | | | | |
|---|----------|----|-----------|----|---------|----|----------|----|----------|
| 1 | 123456 | 6 | 123456789 | 11 | admin | 16 | starwars | 21 | hello |
| 2 | password | 7 | letmein | 12 | welcome | 17 | 123123 | 22 | freedom |
| 3 | 12345678 | 8 | 1234567 | 13 | monkey | 18 | dragon | 23 | whatever |
| 4 | qwerty | 9 | football | 14 | login | 19 | passw0rd | 24 | qazwsx |
| 5 | 12345 | 10 | iloveyou | 15 | abc123 | 20 | master | 25 | trustno1 |

Don't Recycle! Don't Reuse!



Use Passphrases

Password

S3cur1ty&Pa\$\$w0rd!

Difficulty to remember

Hard

Difficulty to hack

Easy

Passphrase

Goblet Foamflower Maple Engine

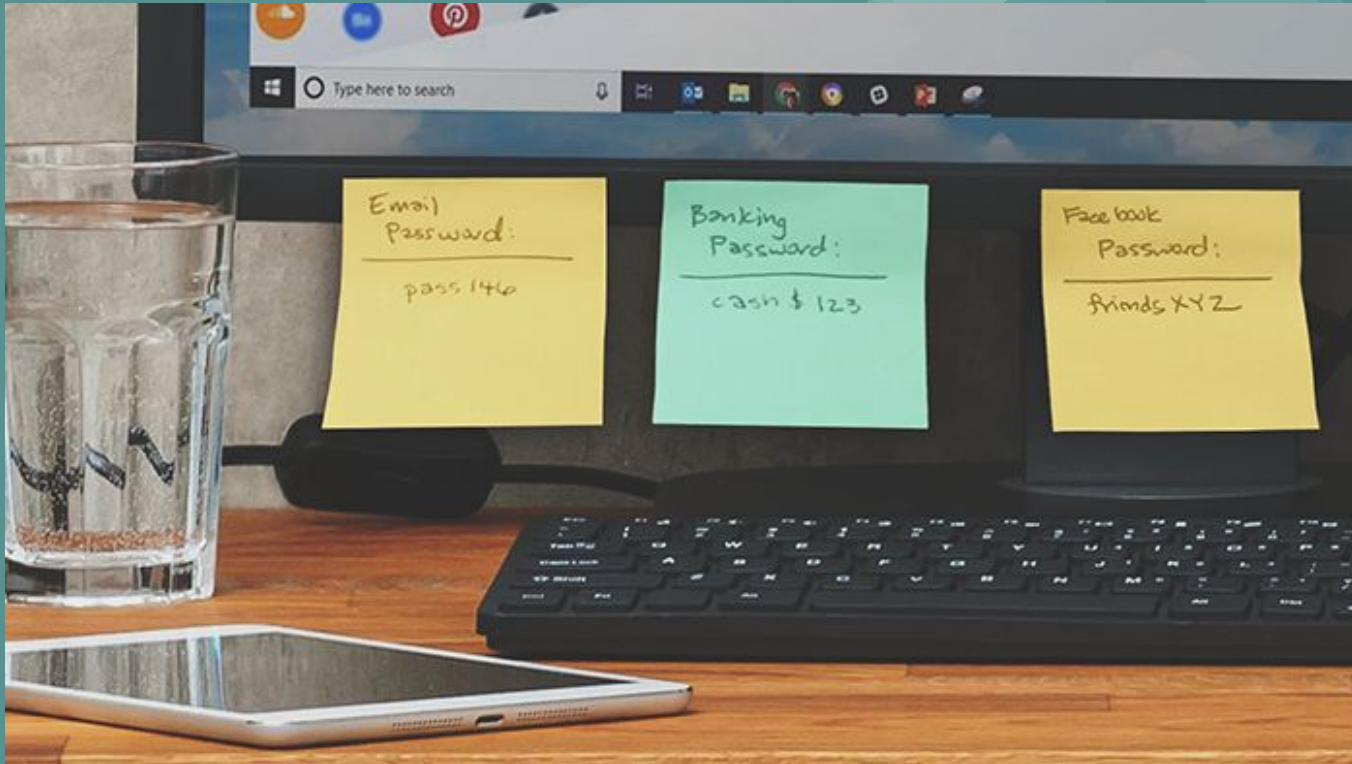
Difficulty to remember

Easy

Difficulty to hack

Hard

Don't write it down and Don't share it!



| |  LastPass |  dashlane |  keeper |  1Password <small>(consumer product, for comparison)</small> |
|--|--|---|--|--|
| Free Tier | Available | Available | Available | Not Available |
| Number of Devices | Unlimited | One | One | Zero |
| Sync Across All Devices | Yes | No | No | No |
| Ad Supported | Yes | No | No | No |
| Personal Vault | Yes | Yes | Yes | Yes |
| Auto Fill and Auto Save | Yes | Yes | Yes | Yes |
| Password Generator | Yes | Yes | Yes | Yes |
| Encryption (in cloud) | AES-256 | AES-256 | AES-256 | AES-256 |
| Subscription Tier | | | | |
| Number of Devices | Unlimited | Unlimited | Unlimited | Unlimited |
| Sync Across All Devices | Yes | Yes | Yes | Yes |
| Shared Vaults | Yes | Yes | Yes | Yes |
| Unique Features | | | | |
| Auto Change Passwords* | Yes | Yes | No | No |
| Built-in TOTP Generator | Yes* | Yes | No | Yes |
| Universal 2nd Factor Authentication (e.g. YubiKey) | Yes | Yes | Yes | No |
| Miscellaneous Features | API access | Dark web monitoring for compromised credentials VPN service | Software developer's kit available | WatchTower to monitor for weak and/or compromised credentials |

PASSWORD TIPS

1

Don't rely on passwords alone to protect anything you value. **Turn on multi-factor authentication wherever possible.**

2

Use a phrase with multiple words that you can picture in your head, so it's difficult to guess but easy to remember.

3

Protect your most important accounts, like banking and primary email, by giving each a **unique passphrase**. A password manager can help.



Password:



Thank You!
Q & A

