CENTER FOR
DEMOCRACY
& TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.
VOL #2

PASSWORDS

[The Problem with Passwords]

- ➢ Passwords can be both easy and frustrating. They’re widespread, so most users understand how to use them. But making them strong enough to be protective can also make them difficult to remember. To prove a user is authorized to access an account or device, they type in a series of characters – like using a key to open a locked door. Characters can be letters (*abc*), numbers (*123*), and special characters (*@#$*). The idea is to **use a password that is difficult to guess**. Weak passwords are short or not very creative, such as “*1234*” or “*password*”. Strong passwords are longer and contain a mixture of characters and case, such as “*ZX2Jh7nx39*” or “*?#KJ*M]TmQ\U*”.
- ➢ Storing passwords in a spreadsheet called “Important” on your computer is the digital equivalent of a sticky note on your monitor. It can be much easier to **use a digital password manager** – an application or service on a computer or mobile device that can create, store, and manage passwords for a single user or group of users. This means you only ever have to remember one strong password: the master password, which opens your password manager and unlocks access to all other passwords [like keeping your keys in a locked safe with a master key].

[Why Password Hygiene is Important]

- ➢ Memorizing a strong password for hundreds of accounts can be difficult, if not impossible. And a strong password is only the beginning. Reusing the same password for multiple accounts is risky because when just one of those accounts is compromised, any other account sharing the same password can also be compromised. To prevent this, **every user should have a unique strong password for each account or device**. Research shows that 38% of passwords are reused across multiple websites. Once breached, these user names, passwords, or personal details can then be resold or even posted online in publicly for anyone to view. Similarly, computers are becoming faster at guessing passwords using brute force (trying every character incrementally) or dictionary (trying common words from a dictionary) attacks. Skilled criminals are getting better at stealing passwords using social engineering or phishing emails. This requires we pick stronger passwords, and guard them more carefully.

[What Are Your Options]

Built-in feature: Apple, Google, and Microsoft platforms include a built-in password manager with their operating systems and web browsers that offer ability to create and securely store unique passwords for websites you visit.	
PRO *Free, already installed, simple to use, accessible across many devices, and can be linked to other services on the same platform.*	*Can’t be accessed from devices on different platforms, must first be able to successfully login to computer or device, limited configuration capabilities, and losing access to the device may cause account lockout.* CON
Third-party Services: Several vendors offer subscription services to securely store your unique passwords in an encrypted vault that is synchronized to the cloud.	
PRO *Non-website passwords (wifi logins, physical lock combinations, grid card images, etc.) can be stored and shared, accessible via any web browser or most devices, centralized admin for multiple users, password policy enforcement, and screens for duplicate or compromised passwords.*	*Monthly cost of $2-4 per user, may rely on the security of servers outside of your control, loss of master password may cause account lockout, and requires setup of recovery options.* CON

Paper Journal: Universally available journals can record handwritten passwords generated using any method.			
PRO	*Simple, reliable, portable, easily replicated locally, can be protected by a range of physical security measures, and safe from remote hacking.*	*Relies on user to generate unique passwords, vulnerable to damage, theft, or snooping, and doesn't work well with multiple users.*	CON

[The Best Option]

- ➢ Third-party services like **LastPass** offer the advantage of being able to generate strong unique passwords, access those passwords from several devices, and scale to manage passwords for offices with multiple users. LastPass can be configured to meet the password requirements of your password policy or other security requirements like NIST. Importantly, LastPass will continually scan your passwords to compare them locally to identify when you may have reused the same password for different accounts or compare them globally to a publicly-available database of passwords that are known to have been compromised – in either case, LastPass will prompt you to change the password.

[The Alternative Option]

- ➢ Built-in password management by **Google** can be used on any device that can supports the Chrome web browser. Saved passwords can be synced across devices and even accessed directly within Chrome. Chrome generates and stores strong passwords for individual users, and can be used to give an app or device permission to access your Google Account.

[What's Next]

- ➢ Policies and guidance on passwords are regularly updated. The National Institute of Standards and Technology (NIST) previously recommended using complex passwords *that are changed several times a year*. For many users and IT support staff, this frequency led to frustration and ultimately a lower level of security as users looked for ways to bypass memorizing passwords – like using a handwritten sticky note on their monitor. NIST recently updated its guidance to instead recommend using a long, memorable passphrase that is only changed when a compromise is suspected. A **passphrase** can be as simple as several random words, the lyrics of a favorite song, or a passage from a book. The key is to make the passphrase at least 12 characters long so it is difficult to guess. Sensitive accounts or critical devices may have higher standards for passphrase length and/or complexity.

- ➢ Strong unique passwords or passphrases are the first step in a multi-layered approach to securing your accounts and devices called **two-factor authentication (2FA)**. 2FA helps prevent someone else from accessing your account by guessing or stealing your password or passphrase. It relies on two different kinds of keys (something you have, you are, or you know) combine to unlock your account or device.

[More Information]

- ➢ Sign-up for LastPass password manager service: https://www.lastpass.com/
- ➢ Learn how to manage saved passwords in Google Chrome: https://support.google.com/chrome/answer/95606
- ➢ Explore Identification as a Service (IDaaS) options for sophisticated IT environments: http://bit.ly/2uZXH5L
- ➢ A publicly-available database of millions of compromised passwords: https://haveibeenpwned.com/
- ➢ Protect your password with tips from the National Cyber Security Centre Password Security infographic: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

For more info, please contact Maurice Turner, CDT Senior Technologist, at maurice@cdt.org, and Joseph Lorenzo Hall, CDT Chief Technologist, at joe@cdt.org. Additional election security resources: http://bit.ly/CDTelectsec.