CENTER FOR
DEMOCRACY
& TECHNOLOGY

ELECTIONS

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

VOL #1

2FACTOR

[What Is Two-Factor Authentication]

Authentication allows you to prove you are who you say you are. You do this by demonstrating access to a particular credential, for example a username and password. Some accounts or devices require that you have access to more than one credential – something you have, something you are, and/or something you know. All three may be required in the most high-security scenarios, in order to make absolutely sure that the person presenting the credentials is the person who can legitimately access the account or devices. For gaining access to most accounts or devices, this is usually something you know: a password. Two-factor authentication combines another piece of information from those categories in to supplement a password; essentially, it adds an **extra layer of security** for your accounts – for example, requiring a password plus a 6-digit code sent to your phone. Two-factor authentication is also called multi-factor or 2-step verification, but is commonly known as 2FA. Think of 2FA as two different kinds of keys that need to be combined to unlock your account or device.

| Why 2FA Is Important |

2FA helps **prevent someone guessing or stealing your password** in order to access your account or unlock your device. Criminals may get your username and password along with millions of other stolen credentials as part of a large data breach or may target you specifically by tricking you using phishing emails. **Phishing emails** are the most likely cybersecurity threat that you will face. 2FA helps ensure that, even if someone knows your password, you're the only person who can access your account and guards against unauthorized changes to or theft of election data like voter registration information or voting machine configuration files.

| What Are Your Options |

There are three basic categories of 2FA: Security keys (something you have), Biometrics (something you are), or One-time passcodes (something you know).

Security keys – Hardware token, like a keychain or fob, that is typically plugged into the USB port of a computer	
PRO *Low-cost ($20-50), configurable to grant access to individual applications or the entire system, portable, difficult to damage*	*May be lost or stolen, requires an open & compatible port on your computer to plug into* CON
Biometrics – Active scanning & recognition of your finger, face, eye, or voice	
PRO *Reasonably unique to every person, built into widely-available commercial products, nothing to remember (or forget)*	*Poorly implemented systems can be tricked on purpose or accidentally, not changeable if enrollment data is stolen, raises privacy concerns for some users, not considered a full authentication factor by robust security standards* CON
One-time passcodes – A unique code sent to a trusted device or selected from a list of pre-approved codes and entered like a second password	
PRO *Works with a variety of devices that you already own (via SMS text, authentication phone app, phone call, email, list of codes on paper), difficult to fake, passcode may expire after set time period*	*Most options require Internet access, can be intercepted if a criminal has compromised your email account or phone, physical or digital codes can be copied & shared* CON

2FACTOR

| The Best Option Is |

Security keys like **YubiKey** provide the best combination of protection, ease-of-use, and compatibility. They can be physically carried on a keychain, locked away securely in a cabinet, and survive being dropped (even into water). Security keys cannot be copied or have their data intercepted when plugged-in. They do not store your private or biometric information and are not phishable. A security key that supports Universal 2nd Factor (U2F) will compatible with the broadest ranges of services.

| The Alternative Option Is |

One-time passcodes are an alternative to consider for situations where access to multiple accounts & systems is a requirement or low-cost is the top priority.

- **For multiple accounts & systems:** A cloud-based authentication service like **Authy** is the alternative to consider if you want the flexibility to use multiple devices for 2FA access into several accounts and systems. Authy stores the individual 2FA token for each account and system in a password-protected database online. This gives you the ability to login into the Authy service from a phone, laptop, tablet, or desktop instead of just relying on a single device or security key.
- **For temporary users at a low-cost:** A grid card from **Entrust** is low-cost, easy-to-use system that uses an array of codes within a labeled grid printed on a card. Each column is lettered, each row is numbered, and each cell has a unique two-digit code. When prompted, you input the code in the cell where a specific row & column intersect – for example: “Type the codes in cell B1, F3, and J4”. Every card contains a unique array codes so that no individual user has the exact same card. The cards can be replaced or deactivated individually or in batches immediately or on a schedule (such as the day after an election). You can carry the printed card in your wallet or save the pdf on your phone.

| What’s Next |

Confirm with your IT department that your current accounts & systems support 2FA. Prepare to manage the inventory of 2FA devices and reinforce strong password policies with your users. Consider how 2FA may require changes to your business recovery and operations continuity plans if you are locked-out of your accounts because you cannot complete the second authentication step.

Expect 2FA to become **more prevalent** as biometric security gains popularity on consumer devices and popular services (like major software vendors and financial institutions) push public adoption in an effort to reduce fraud while improving privacy.

| More Information |

- List of websites and whether or not they support 2FA: https://twofactorauth.org/
- Purchase Yubikey security keys: https://www.yubico.com/why-yubico/
- Sign-up for Authy authentication service: https://authy.com/
- Purchase Entrust GridCards: https://www.entrust.com/gridcard/
- Lock Down Your Login strong authenication tips: https://www.lockdownyourlogin.org/strong-authentication/
- NIST Digital Identity Technical Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html
- Best 2FA phone apps https://www.pcworld.com/article/3225913/security/what-is-two-factor-authentication-and-which-2fa-apps-are-best.html

For more information, please contact Maurice Turner, CDT Senior Technologist, at maurice@cdt.org, and Joseph Lorenzo Hall, CDT Chief Technologist, at joe@cdt.org.