Anderson County Board of Commissioners
OPERATIONS COMMITTEE
AGENDA
May 9, 2022
6:00 p.m. Room 312

1. **Call to Order**

2. **Prayer / Pledge of Allegiance**

3. **Approval of Agenda**

4. **Appearance of Citizens**

5. **Tourism** – requested by Stephanie Wells, Director

6. **Mayor**
   - Multi-Factor authentication

7. **Anderson County Animal Shelter Social Media Claims**– requested by Chairman Wandell

New Business

Old Business

Adjournment

ANDERSON COUNTY GOVERNMENT

TERRY FRANK
COUNTY MAYOR

May 4, 2022

Commissioner Tim Isbel
Chairman, Operations Committee

RE: Agenda

Dear Chairman Isbel,

I wish to request the following item be placed on the agenda:

1. Multi-Factor authentication. Anderson County's Insurance Company is strongly recommending that Anderson County implement MFA and has put us on notice that our lack of MFA seriously hampers the ability of Anderson County to secure adequate cyber coverage. Director Young will be on hand to discuss. Most departments could inexpensively implement this with a policy change. Some departments may take longer to design an implementation strategy. MFA not only protects the county systems from unauthorized use, it protects the employee by ensuring the identity of the employee. (See attachments for background on MFA)

100 NORTH MAIN STREET, SUITE 208 • CLINTON, TENNESSEE • 37716
PHONE: (865) 457-6200 • EMAIL: TFRANK@ANDERSONTN.ORG

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

Why should State and Local Election Officials be interested in MFA?

Implementing MFA makes it more difficult for an adversary to gain access to secure databases, applications, and other election infrastructure assets. MFA can help prevent adversaries from gaining access to your organization's assets even if passwords are compromised through phishing attacks or other means.

Increasingly, a user ID and password combination alone does not provide enough protection against unauthorized login. One of the major drawbacks of using an ID and password system alone is the requirement to maintain a password database. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. These factors reduce the security of password protected systems and resources more each day.

How does MFA work?

MFA requires system or network users to present two or more credentials at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- **Something you know:** like a password, Personal Identification Number (PIN), or answers to security questions;
- **Something you have:** like a smart card, mobile token, or hardware token; and
- **Some form of biometric factor** (e.g., fingerprint, voice recognition).

For example, MFA could require users to insert a smart card ID into a card reader (first factor) and then enter a password (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

The added security offered by MFA can simplify the user login process by using single-sign on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time.

Consider deploying an MFA capability to cover voter registration systems, election night reporting systems, or other election office IT systems. Implementation schedules and costs vary depending on the MFA solution your organization chooses and the assets that it covers. These options range from implementing a single sign-on environment to supplementing an existing password-based login system with a second authentication factor, such as a time-limited, single-use code delivered by token or through a smartphone app generator.

CYBER LESSONS

Arm yourself with knowledge to stay ahead of the game.

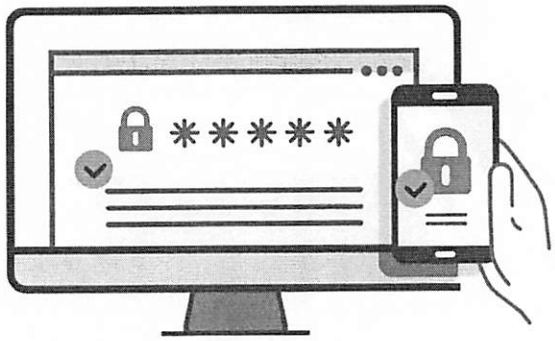
Multi-Factor Authentication

Double your login protection.

No matter how long and strong your password is, a breach is always possible. All it takes is for just one of your accounts to be hacked, and your personal information and other accounts can

become accessible to cyber criminals.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is *you*. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. This way, even if cyber criminals guess your password, they're still out of luck!



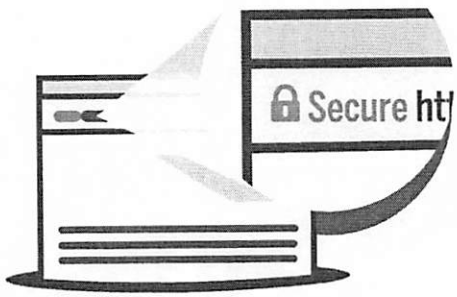
Sometimes even long and strong passwords aren't enough. Step up your game with MFA and keep all your private bits ... private.

Wi-Fi Safety

Stay protected while connected.

The bottom line is that whenever you're online, you're vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection. When you find yourself out in the great "wild Wi-Fi West," avoid free internet access with no encryption. If you do use an unsecured public access point, practice good internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.



Make sure you go green—green lock, that is—for a trusted internet connection, and make this step a habit in every new environment.

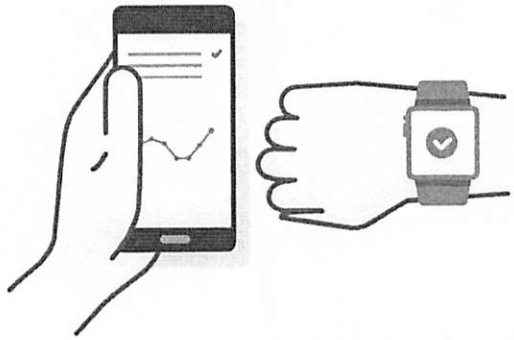
App Security

Keep tabs on your apps.

Have you noticed that apps you recently downloaded are asking for permission to access your device's microphone, camera, contacts, photos, or other features? Or that an app you rarely use is draining your battery life?

Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Don't give your apps an all-access pass. The following are some steps to avoid "over-privileged" apps:

- Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use.
- Learn to just say "no" to privilege requests that don't make sense.
- Only download apps from trusted sources.



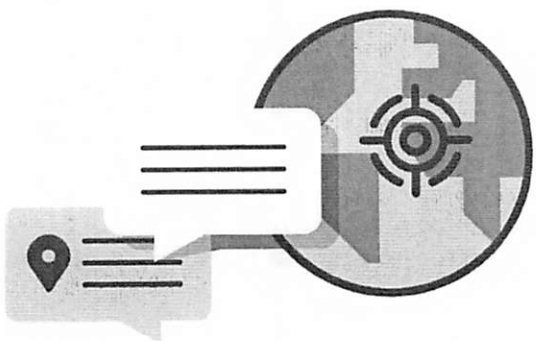
Enable automatic app updates in your device settings or when they pop up, because having the most up-to-date software doesn't just make things run smoother—it helps keep you patched and protected against ever-evolving cyber threats!

Oversharing and Geotagging

Never click and tell.

Everyone seems to be posting their information on social media—from personal addresses to where they like to grab coffee. You may figure, if everyone's doing it, why can't I?

What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and even your physical belongings—online and in the real world. Avoid posting names, phone numbers, addresses, school and work locations, and other sensitive information (whether it's in the text or in the photo you took). Disable geotagging, which allows anyone to see where you are—and where you aren't—at any given time.



While it's tempting to do otherwise, limit your social networks to people you actually *do* know in real life, and set your privacy preferences to the most restrictive settings.

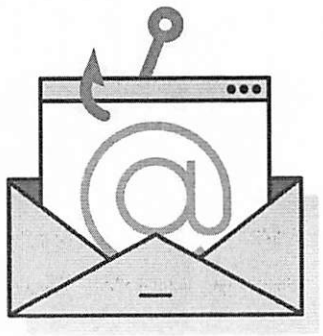
Phishing

Play hard to get with strangers.

Cyber criminals cast wide nets with phishing tactics, hoping to drag in victims. Seemingly real emails from known institutions or personal contacts may ask for financial or personal information.

Cyber criminals will often offer a financial reward, threaten you if you don't engage, or claim that someone is in need of help. Don't fall for it! Keep your personal information as private as possible. If they have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Always avoid sending sensitive information via email.



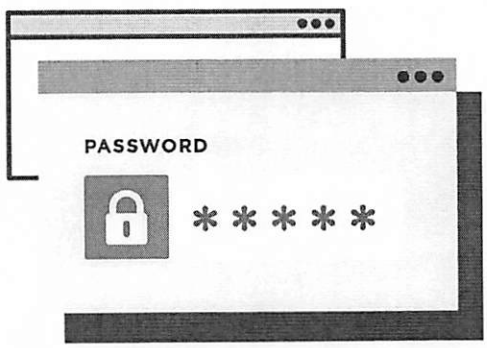
If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks 'phishy,' reach out to them via customer service to verify the communication.

Passwords

Shake up your password protocol.

Gone are the days when you needed to come up with a frustrating mixture of letters, numbers, and symbols. According to NIST guidance, you should consider using the longest password or passphrase permissible. NCCIC guidance suggests 16-64 characters.Some sites even allow for spaces. Easy-peasy!

It's important to mix things up—get creative with easy-to-remember ways to customize your standard password for different sites. Having different passwords for various accounts can help prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Always keep your passwords on the down-low. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.



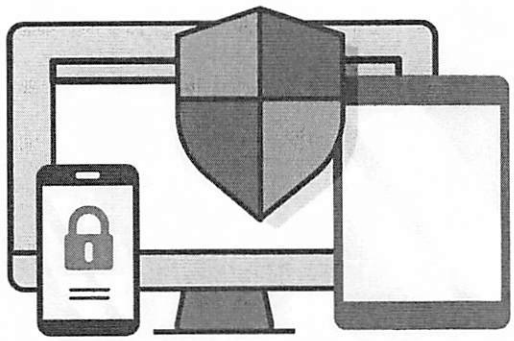
Ready for extra credit? The most secure way to store all your unique passwords is by using a password manager. With just one master password, a computer can generate and retrieve passwords for every account you have—protecting your online information, including credit card numbers and their three-digit CVV codes, answers to security questions, and more.

Device Protection

If you connect, you must protect.

Our devices are great at making our lives easier and fun, but it's important to be conscious about all the information you are generating and where it's headed. Once your device plugs into cyberspace, you and your device could potentially be vulnerable to all sorts of risks.

These include malware that can steal information and data, destroy your hardware, log keystrokes, and infect other devices connected to your compromised device. Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you're putting something into your device, such as a USB for an external hard drive, make sure your device's security software scans for viruses and malware. Finally, protect your devices with antivirus software. There are many kinds of antivirus software available, so find one that fits your needs and your devices.



Cyber threats may be evolving, but you can outsmart them with a savvy security protocol.

TLP:WHITE