be cybersmart

You don't need to worry constantly about every imaginable threat. But good digital habits and practices will help keep you and your data safe and private.

Passwords

1 **Use strong passwords**. Hint: "1234" is not a strong password.

Select user-friendly passwords with a minimum of 8 characters and a maximum of 64 characters. The password should contain at least one, preferably more, lowercase letters, uppercase letters, numbers, and symbols. In any case, choose something that is easy to remember, reset your password when you forget it, and change it once per year minimum.

There are many tools on the internet that can be used to break or decode weak passwords. The vast majority of passwords used in the world are weak passwords because people are worried they will forget a stronger password. The TOP 10 weak passwords used in the world are:

1. 123456
2. 123456789 (longer, but no more secure)
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. lloveyou
9. 111111
10. 123123

It would take 1/50th of a second for a hacker to figure out one of these passwords as they can run through a database scan lists of thousands of such common, weak passwords. You should consider using a password manager that will safely create a very strong and unique password for every account you have online.

2 **Don't reuse passwords**. If you are reusing passwords across multiple platforms, a single compromise can cause problems across the board.

Avoid using variations of the same password which only change a few characters. Example: MyBankPassword_2020, MyBankPassword_2021. This is an obvious step but is often overlooked.

Each account should have a unique password. If one company you use happens to get attacked, then the data stolen about you and your account will not help them breach your other accounts. For example, if you always use 123456 as your password for every account, and your favorite clothing store gets hacked, the hackers can steal your username and password and immediately try them to access your other accounts. Keep your passwords strong and unique for each account. See more information about this at the following link:

https://www.helpnetsecurity.com/2019/11/12/password-reuse-problem/

3 **Use a password manager**. Password managers keep track of all your passwords, can generate secure passwords, and warn you if you have duplicates. Password managers can work across all your devices.

This is an easy practice to adopt and will make your passwords safe and keep your digital life secure and protected. Some of the best tools in this space are:

LastPass	https://www.lastpass.com/password-manager
Keeper	https://www.keepersecurity.com/
Dashlane	https://www.dashlane.com/
1Password	https://1password.com/

4 **Use 2-factor authentication** (also known as **Multi-Factor Authentication**). This means that, in addition to standard login credentials, you must provide an additional piece of information (a "second factor"), usually a numeric code. This code is sent to you directly via text/SMS or email when you attempt to log in.

You can make an online account much more secure by using 2-factor/multi-factor authentication (2FA/MFA). With 2FA/MFA, you are protected even in cases where a hacker has stolen your login credentials. In such cases, when the hacker attempts to log into your account, the second factor (the numeric code) needed to log in will be sent directly to you, not them, thus blocking their access to your account and data.

Most online accounts now offer 2FA/MFA. It may slow down your login by a few seconds, but can prevent hundreds of hours spent recovering from the damage to your financial, social, or medical information caused by a successful hack. Imagine your savings account or retirement savings being stolen, or all your family pictures deleted, etc. This extra step is a strongly recommended safeguard to protect you and your information.

Once 2FA/MFA is enabled for an account, the typical login is as follows:

1. You login with your username and password (hopefully a strong one) as always.
2. You will immediately receive a numeric code texted to your phone (or received via an authentication app such as Authy or Duo Mobile).
3. You then enter this numeric code in the same webpage/app. You will then be logged in to your account.

More on 2FA can be found at: https://authy.com/what-is-2fa/

Away from home

1. **Be careful with free Wi-Fi**. If you are using free/open Wi-Fi (at the airport, coffee shop, school, hotels, etc.), ensure you are using a VPN to protect your privacy.

The more public the location, the more likely that there is someone trying to steal your data. One common hacker tactic in public places is to set up fake "Free Wi-Fi" or "Airport Wi-Fi" networks that actually connect to their hotspot. At that point, they can attempt to compromise your device in various ways. For example, they may generate a pop-up on your screen that says something like "Google has detected that you are in a new location. Please re-login for your safety." In reality, the hacker is hoping to trick you into giving them your username and password for your Google account. Be careful. You can also see how 2-factor authentication can protect you here. Even if you give the hacker your username and password, they will not have your second factor (which is the code sent to your phone or email). Once you realize you may have been spoofed, you can just change your password and the hacker has nothing of use.

A VPN (Virtual Private Network) uses encryption to make it much more difficult for someone to intercept your data when using a public network. Various VPN options are available. Here are some of the most popular VPNs available: https://www.techradar.com/vpn/best-vpn

2. **Secure your devices**. It's obvious, but leaving your laptop or phone unlocked and unattended, even for a short period of time, is a recipe for trouble.

Password protect your devices and don't leave them unattended in public places. Even in your home, you should have a password on your desktops and laptops. Also, in many cases, it is advisable to encrypt data stored in certain files or folders so the data is secure even if stolen. More information on this can be found at the following link: https://community.windows.com/en-us/stories/file-encryption-windows-10

Your devices

1. **Passwords** Configure passwords and screen timeouts on all devices to reduce the possibility of improper access.

A recent study by Kaspersky Labs shows that only 48% of cell phone owners have a passcode or password set on their device. In 2019, over 70 million phones were lost or stolen. You do the math. If half of those did not have a password, then imagine the cyber theft that may have occurred on those 35 million phones by the person who found them. They would have access to social media accounts, medical information, email, shopping accounts, etc. It takes an average of 2.2 seconds to type in a 6-digit passcode and can save you hundreds of hours working to get out of an Identity theft situation. Use a passcode, password or face recognition to unlock your phone, along with a fairly short screen time-out which locks your phone. https://www.itproportal.com/2015/04/28/how-to-set-up-passcode-android-ios/#:~:text=Here's%20how%20to%20set%20it,it's%20one%20you%20will%20remember)

2. **Keep your software up to date**. Old software is unpatched, vulnerable software. Ensure that the operating system, apps, programs, etc. on your systems are updated regularly.

It is unwise to use computers or cell phones with operating systems so out-of-date that they are no longer supported by the vendor with security patches. Yes, it may seem simpler to keep using Windows 98, but you'll likely pay a price in the long run. Go ahead, bite the bullet, and update your OS and/or device. If this is your phone or tablet, just take the time one evening to fully charge the device and then select to perform the update from the settings page on your device. https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html

3 **Ensure that your device has appropriate virus and malware protection**. In many cases, modern operating systems have acceptable levels of protection built in, but you need to verify.

Operating Systems (OS) and their built-in capabilities have progressed to the point where add-on virus and malware software protection is not always needed. Of course, this depends on the OS being updated regularly and configured properly. If you choose additional protection, some of the best tools for Windows and Android are easy to install and will keep your systems and data safe.

The top tools you can use are listed below:

Windows:
- AVG Antivirus https://www.avg.com/en-us/free-antivirus-download
- Avast Antivirus https://www.avast.com/en-us/free-antivirus-download#pc

Android:
- AVG Antivirus (Play Store)
- Avast Antivirus (Play Store)

Apple Devices:
- AVG Antivirus (APP Store)
- Avast Antivirus (APP Store)

4 **Bluetooth safety**. Consider disabling some or all Bluetooth features on your devices by default, and only enabling them when needed. Bluetooth has been used as a pathway to access devices in certain cases.

Bluetooth is a very powerful and flexible way to connect headphones, speakers, etc, to your phone, tablet or other mobile device. However, Bluetooth can be exploited if you do not have the correct security settings. These settings differ between Apple (iOS and macOS), Android, and Windows products, but you should disable Bluetooth settings that say things like "Allow friends to play music on your speakers". See the article below about some recent hackers exploiting Bluetooth on millions of devices.
https://thehackernews.com/2020/05/hacking-bluetooth-vulnerability.html

Your home network

1 **Passwords.** Make sure that your Wi-Fi network is password-protected, and consider rotating that password periodically, especially if you have a guest network in place.

Having a strong password on your wireless network is vital. There are many easy-to-get password cracking tools available to discover and steal simple Wi-Fi passwords. If your password is a name followed by a few numbers, these can be cracked by a hacker or neighbor in less than a day. We recommend 12 digit or larger passwords that include special characters (!#) and do not contain names, birth dates, etc. If you don't know how to change your password get in touch with the company providing your service and ask them to help you.
One tool we like to use to see what devices are on your network is a free tool called FING. You should periodically check and make sure unrecognized devices are not on your network. https://www.fing.com

2 **Use a firewall**. A firewall is a device or piece of software that monitors all in/outbound network traffic. Based on a defined set of security rules, a firewall will either allow or block the network traffic.

A firewall, simply put, can control who gets into your system and what data or application can send data out of your system. Windows has a simple, built-in firewall that is easy to enable and you should verify it is turned on for all of your Windows devices.
https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f

3 **Keep your software up-to-date**. Even your network equipment (router, etc.) needs to be updated and/or patched occasionally to ensure proper security and performance.

Spend some time each month to check all of the key software programs on your computers, phones and tablets to make sure they are updated to the latest versions. This small amount of time can save a lot of aggravation and will often come with bug fixes and new features.

Most modern routers can be configured to auto-update. If you have equipment from your internet provider, you can contact them to ensure that your equipment is up to date. There are thousands of exploits each year, and the most reputable router companies will update their software several times a year to fix any exploits.

4 **Ensure that your network router is not using the default admin password.**

It is quite common to find routers with the default factory passwords still in place. Tthis means that someone with access to your network can, with a simple guess, gain full access to modify your network configuration, including locking you out of your own network, redirecting your data, etc. If your router came from your internet provider, ask them to verify that this default password has been changed.

Safeguard your data

1 **Back up your data**. Digital data, on your hard drives, flash drives, and phones is easily stolen or lost (device failure or accidental incidents). At a minimum, your important data should be backed up to a second device or cloud service.

There are many ways to back up personal, important data. Phone data can be backed up to iCloud or Gdrive/Google Photos. Locally, you can back up to external hard drives or even a dedicated network storage device (NAS).

There are many different ways to utilize the cloud for data backups/redundancy. For standard backups, services such as Backblaze or Carbonite will automatically back up selected data on a continual basis. Backups can be encrypted if desired for even higher levels of safety. Alternately, you can choose to keep your important data in the cloud from the start using services like Gdrive, iCloud, Dropbox, as the actual home for all your data, rather than a local computer/hard drive.

Of course, when utilizing any online services as a part of your data safety strategies, use of appropriate and strong passwords (as described above) are essential.

2 **Be suspicious of emails**. Don't be paranoid, but suspicious. Emails can be like people, if it seems odd, it might be. Do you regularly receive emails from a "Nigerian Prince"? No? Well, then you might be wary of this one.

- Unexpected emails are to be considered suspicious.
- Never click a link in an email unless it is completely trusted, and even then, hover over the link to view the true URL.
- All links in emails should be treated as guilty until proven innocent.
- Do not open unknown email attachments.

The most common way to inject malware into a network and compromise its security is for a user to click on a seemingly innocent link in an email and unwittingly download a malware agent. This is known as "phishing."

3 **Keep your software up to date**. Even your network equipment (router, etc.) needs to be updated and/or patched occasionally to ensure proper security and performance.

Most modern routers can be configured to auto-update. If you have equipment from your internet provider, you can contact them to ensure that your equipment is up to date.

Always take the time to update your software for your desktops, laptops, phones and tablets. This can avoid critical security issues and many times comes with new features and bug fixes in the current version.

In general, let common sense be your guide. Don't be overwhelmed with all the things that *might* happen – just take a first step towards better data safety and privacy. And don't be afraid to ask for help.

For more information…

If you'd like to find out more about how you can protect yourself or your business, contact us at https://www.texas-act.com/contact-us/.