WICTRA TECH

WICTRA home or small business cyber security checklist.

info@wictra.org

Checklist Item	Yes	No	Notes
Router Security			Link to router guide
1.1 Do you have a router and know where it is?			
1.2 Update Firmware on router			
1.3 Maintain Firewall on router			
1.4 Change default admin user ID and password of router?			
1.5 Create unique SSID for Wi-Fi on router.			
1.6 Have changed your Wi-Fi login from factory default?			
1.7 Guest Network Do you have or need a guest network			
1.8 Is your guest network secure?			
1.9 Take inventory of all devices that are connecting to ensure that there are no unauthorized devices			
1.10 Do you use VPN or need one?			
1.11 Do you turn your router off during non-use hours?			
End point / desktop/ laptop			Endpoint guide
2.1 Do you have a current up to date operating system (OS)?			
2.2 Does your PC check for updates?			
2.3 Is the PC firmware current?			
2.4 How secure is your login information?			
2.5 Do you have personally Identifiable information on your computer (PII) aka things like taxes, social security numbers, bank account numbers, credit card numbers, website login information?			
2.6 Does your PC have a firewall? Is it up to date and functioning?			
2.7 Have you scanned your PC for vulnerabilities?			
Home Automation			Automation guide
3.1 Do you have home automation?			
3.2 Is it connected to a guest network?			
3.3 Cameras /Doorbell			
3.4 Garage door opener			
3.5 Smart thermostats			
3.6 Smart TV			
3.7 Automated lighting			
3.8 Smart fire / smoke detectors			

Checklist Item	Yes	No	Notes
3.9 Other smart devices not listed above			
Passwords / Security			Password guide
4.1 How strong are your passwords?			
4.2 Have you checked the strength of your passwords?			
4.3 Are you using the same password over and over?			
4.4 Do you use a password manager?			
4.5 Do you have a list of passwords laying around?			
Cell phones			Cell phone guide
5.1 What about your cell phone?			
5.2 Does your phone connect to your home network?			
5.3 Is your phone current on updates?			
5.4 Are you using a lock screen with a PIN?			
Email			Email guide
6.1 How are your email practices?			
6.2 Use caution when clicking on items in your email, make sure that what's in your mail is from a reliable source.			
6.3 If you need to forward information, copy the information out of the email and start a new email. This will break the chain and limit visibility to other email addresses			
6.4 If you need to send information to a group use the BCC function. This will limit visual information to wrong people. The receiver then will only see their email address.			
6.5 Are you aware of phishing schemes?			
Backups			Backup guide
7.1 Are you backing up your data?			
7.2 Where are you backing it up?			
7.3 Are you backing up to an external hard drive?			
7.4 Are you backing up to a network location?			

Checklist Item	Yes	No	Notes
7.5 Is your backup location secure?			
Antivirus protection			Antivirus guide
8.1 Do you have antivirus protection?			
8.2 Is it active / on?			
8.3 Is it up to date?			
Social media			Social media guide
9.1 Are you using Social media?			
9.2 Is your account secure?			
9.3 Is it up to date?			
9.4 Is your personal information secure?			
9.5 Are you posting personal information?			
Internet browser / Adware / Popup blockers			Internet guide
10.1 Is your Internet browser up to date? Most browser have an update process			
10.2 Do you use an ad blocker?			
10.3 Do you use a pop-up blocker?			
Definitions			
Resources			

Add additional notes as needed

This list is not intended to cover every aspect of your home or small business cyber security, but meant to get you thinking about all of the potential vulnerabilities you may have. With an ever-evolving world this is not meant to be the only answer to your cyber Security.

Router security

- Have you updated the admin / password from the factory settings? Most newer routers have the capability of being able to log in and see all of the devices connected to your router.
- Be smart about choosing an SSID (network name). Don't identify yourself and don't use the default
- Take inventory of all device that are connecting to ensure that there are no unauthorized devices. Most routers will allow you to name the devices attached to your network. If your router doesn't do this, consider an upgrade.
- How is your guest network setup?
- Use your guest network for connecting home automation.
- Is it secured vs. open to the public (no password)?
- If you work from home and have children, do they connect to the same network that you use for work. Make sure they log into a guest network to separate work from play especially if you have gaming consoles.
- If the router does not self-update, then check for new firmware every month or two. Also, register it with the hardware manufacturer on the chance that they notify you of firmware updates. Netgear, for example, has a security newsletter that announces bug fixes. Even if the router does self-update, check every now and then that the self-updating system is actually working
- Verify that your router firewall is enabled, functioning and up to date.

PC / Endpoint

- Do you have a current up to date operating system?
- Does your PC check for updates?
- Is the firmware current? Most manufactures' offer support for their devices. A good practice is to check periodically to see if they can be updated
- How secure is your login information? Use strong passwords or even better use 2FA to add an additional layer of security.
- Do you have personally Identifiable information on your computer (PII) aka things like taxes, social security numbers, bank account numbers, credit card numbers, website login information. Protect your data
- Perform routine updates and patches provided by either the software company or the pc manufacturer.
- Does your PC have a firewall and is it up to date and functioning?
- Empty the trash. If a criminal would gain access to your pc, the trash contains anything that you recently deleted. It stays there until you empty it.
- Do you have any antivirus program? Is it enabled and up to date?

Home Automation

Knowing what devices are connected to your wireless home network and making sure all of those devices are trusted and secure. This used to be simple when the only device you had was just a computer. However, today almost anything can connect to and use your home network, including your smartphones, TVs, gaming consoles, baby monitors, printers, speakers, or perhaps even your car.

- Once you have identified all the devices on your home network, ensure that each of them is secure.
- Change any default passwords on them and enable automatic updating wherever possible.
- Review these devices in your router settings and assign names to them for easy inventory of your connected devices.
- Disable features you may not need some devices allow you to change default settings.
- Watch out for outages. Ensure that a hardware outage does not result in an unsecure state for the device. No doubt more IoT devices are coming and will angle for a place in your home. If they make your life more convenient — even happier — great. But don't forget to secure your increasingly smart home and your IoT devices.

Password Security

One of the easiest ways to practice good password security is to use a **password manager** and 2 factor authentication (**2FA**). There are a number of excellent password managers out there, some offer free versions which will work well for a number of people. Most password managers will also advise you on your password strength and if you used the same password more than once.

If you choose to maintain your own passwords there are a number of things you can do to protect yourself. Here are some recommendations of what you can do.

If you choose to write them down, keep them in safe place to prevent them from accidentally being lost or stolen. DO NOT KEEP THEM ON YOU COMPUTER.

In all cases whether you use a password manager or a manual list, make sure that someone you trust knows where and how to access them in the event something happens to you, even if it isn't long term that they would need to do things like pay bills.

Common passwords mistakes

- **Too short**. Bottom line, longer is better. Don't just do the minimum to access a device, system or website.
- **Too simple**. 123456 is not a good password. This represents what a number of people do, it can be cracked almost instantly. Using a combination of numbers, uppercase, lowercase letters and special characters will help to minimize passwords from being cracked. DO NOT USE THE WORD PASSWORD OR QWERTY as part of your password. These are the number 1 common error made.
- **Too obvious**. Simple words are easily cracked. Don't use street names, colleges, spouse names or common slogans.
- **Too topical**. Using popular headlines in the news is always a bad idea. Another source of this is trending topics. Do not use these as they are easy targets for hackers.
- **Not private**. In one report it has been noted that more than 25 percent of the people have shared one or more of their passwords with other people.
- **Forgettable**. Just because you find something memorable doesn't mean you should use it in your password. Along with trying to remember groups of different passwords come the challenge now of remembering these memorable items and how you would have grouped them together.

Simple guide to creating your own passwords

- Has minimum of 12 characters, once again longer is going to be better
- It includes numbers, symbols, capital letters and lower-case letters

Password Security continued

- Isn’t a dictionary word or combination of dictionary words
- Shouldn’t have obvious substitutions, an example of using the number Zero 0 in place of the letter o. Try to mix it up.
- Combine things to create a passphrase. Create a memorable sentence and use the first letter in each word to create your passphrase / password. My first car was a Chevrolet back in 1981 it cost me $100. **MfcwaCi1981icm$100**.
- The dice game. Putting random words together to create a single passphrase. Leaf, coal, job, lasagna.

Cell Phones

- **Lock your phone - Enable** a lock screen. Set a PIN. By enabling the lock screen, you greatly reduce the risk of becoming a victim. This becomes a valuable piece of protection. If you should happen to misplace your phone, it can't be easily accessed.
- **Encrypt your device - Encrypting** your phone will scramble all files so that only you have access to them. You'll need to enter a PIN or password to decrypt your phone every time you want to use it.
- **Be wary of public Wi-Fi hotspots -** Do not access any sensitive information through public Wi-Fi, such as logging into your bank or checking sensitive work emails, as a hacker may be able to intercept your communication through a "man-in-the-middle" attack. It is far more secure to use a cell phone data, or to use a VPN.
- **Only download apps from trusted app stores -** Savvy hackers have been known to slip past the walled garden of the App Store and the security measures of Google Play Protect, but your chances of downloading a malicious app are far lower if you stick to the official app stores.
- **Keep your phone apps up to date -** Apps that aren't updated can be vulnerable to hackers. You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing
- **If you don't use an app, uninstall it - Unused** / obsolete apps can lead to creating vulnerabilities' in your phone
- **Charge your phone from an adapter and not your pc - by** using a wall charger instead of connecting to your pc will eliminate potential security problems. Remember that when you connect through USB you potentially leave an open door to transfer problem from one device to another. Your USB cable can do more than charge your phone, it can also transfer data.

Email

- Use caution when clicking on items in your email, make sure that what's in your mail is from a reliable trusted source.
- If you don't recognize the sender delete it.
- Do not forward email if at all possible. If you forward emails you put everyone listed in the address block at risk. If you need to send information to a group use the BCC function. This will limit visual information to wrong people. The receiver then will only see their email address.
- Phishing schemes pray on people clicking on things that look legitimate. Beware! If it looks to good to be true, it probably is.
- Spam, malware and ransomware love people that click on these gimmicks. If you need to forward information, copy the information out of the email and start a new email. This will break the chain and limit visibility of other email addresses.
- When in doubt, throw it out: Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email.

Backups

Sometimes, no matter how careful you are, you may be hacked. If that is the case, often the only way you can recover your personal information is to restore from a backup.

- Make sure you are doing regular backups of any important information and verify that you can restore from that backup.
- Most mobile devices support automatic backups to the Cloud.
- For most computers, you may have to purchase some type of backup software or service, which are relatively low-priced and simple to use. Backups.
- Are you backing up your valuable information?
- A good practice of backing up is copying your data to an external thumb drive or hard drive. By doing this you remove your information from catastrophic failure.
- Back it up in more than place. This isn't just good for cyber security, but also if you should happen to have hardware failure of your computer.
- I can't stress enough the importance of backing up. It's probably the easiest thing to do to keep your important items safe.
- If you choose to back up your data to a removable device ensure the device physically secure (don't leave it laying around for prying eyes).
- Verify that your backup data works.

Internet and Internet browser

It's almost impossible to accomplish anything today without the necessity of going to the internet. When using the internet, it's important to follow a few guidelines to protect yourself.

- **Install a popup blocker**, a popup blocker will limit the number of unwanted ads from showing up in your webpage.
- **Beware of ads encouraging users to click on links**. If you receive an enticing offer, do not click on the link. Instead, go directly to the company's website to verify the offer is legitimate.
- **Spyware:** The two important things to know about them are that:
- They can download themselves onto your device without your permission (typically when you visit an unsafe website or via an attachment).
- They can make your computer do things you don't want it to do, such as as opening an advertisement you didn't want to see. In the worst cases, spyware can track your online movements, steal your passphrases and/or compromise your accounts
- **Unknown questionable websites:** Unknown questionable websites. Stay clear of these sites. The owners of some of these sites aren't looking out for your best interest and are usually not secure, allowing malicious code to added to their site. If you see something that looks too good to be true, it probably is and clicking on these types of sites can potentially cause damage to your PC or even trigger ransomware.
- **Ad blocker** an ad blocker can help limit the amount of malicious adware that pops up on some websites. Some browsers will have this as an extension that can be added in**.**
- **Do your homework:** Fraudsters are fond of setting up fake e-commerce sites. Prior to making a purchase, read reviews to hear what others say about the merchant. In addition, look for a physical location and any customer service information. It's also a good idea to call the merchant to confirm that they are legitimate.

Antivirus Protection

Running an antivirus program adds an additional layer of protection to your computer. Modern antivirus utilities handle Trojans, rootkits, spyware, adware, ransomware, and more. Don’t run a computer without having some form of protection installed. Most newer computers come preinstalled with their version of Antivirus protection. Learn how it works and ensure that it’s running whenever you use the computer.

- Make sure that you have some form of antivirus software installed on your computer.
- Ensure that the protection software you’re running is kept current, most software will update definitions on a daily basis.
- Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
- Setup software to scan USB devices being plugged into your computer before you use that device.
- Develop a routine to scan your computer on a regular basis to help minimize risk.
- Use security software that provides layered defense via anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities.
- The security suite may be built into the operating system or available as a separate product.
- Modern endpoint detection and response software uses cloud-based reputation service for detecting and preventing execution of malware.
- To prevent data disclosure in the event that a laptop /desktop pc is lost or stolen, implement full disk encryption.

Social Media

Spending time (some would say waste time) fooling around on Facebook, Twitter, and other services. We also use these sites for serious, professional reasons. But like almost everything else on the Internet, they're inherently dangerous. Hackers can use social media to discover your private information and to deliver spam or malware. You can be stalked and bullied through social media. It can ruin your reputation, your career, and your life.

- **Protect your account -** Don't give anyone else your password to a social network. And you shouldn’t let them steal it, either. Use a long, strong password containing upper- and lowercase letters, numbers, and punctuation. And use a unique password for every site. Don't depend on just the password. Most sites offer some form of two-step authentication, which requires you to prove your identity using both a password and an external factor, such as a text sent to your smartphone.
- **Be careful about what you post -** Sharing too much personal information can cause considerable harm. If you let your social media network know that you're on vacation, someone may take that as an invitation to burgle your house. Your physical address, your phone number, and even your birthday can be used against you by an identity thief. Control who can see what on a social network; some posts may be for everybody, others for friends, and still others for only very good friends. If you use a social network, learn its privacy settings. The links below will take you to the various services' privacy pages.
- **Keep your eyes out for scams** - Stay away from Fill in questionnaires. In the wrong hands, that information can be used against you. More serious scams can trick you into giving away your credit card number or password.
- **Make sure your computer or device is protected -** Social networks constitute one more path for malware to make its way to your computer or device. If you're using social media, keep a good, up-to-date antivirus program running at all times. The best programs offer tools specific to social networks. For instance, Bitdefender Total Security uses special filters to look for and stop social network-specific attacks and warn of potential fraud.

Definitions

- **2FA -** Two Factor Authentication (2FA) refers to needing a password and form of authentication to gain access to a system. A user id and password are considered a single form authentication. 2FA requires and additional form such as a text being sent to your phone to confirm your identity.
- **BCC** - Blind carbon copy (abbreviated Bcc) allows the sender of a message to conceal the person entered in the Bcc field from the other recipients.
- **End point** - An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include: desktop, laptop, tablets, servers and anything that connects to the internet
- **Firewall -** A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- **Firmware -** Firmware is a software program permanently etched into a hardware device such as a keyboards, hard drive, BIOS, or video cards. It is programmed to give permanent instructions to communicate with other devices and perform functions like basic input/output tasks
- **OS -** Operating System (OS) Android, Microsoft, Linux and Apple are all examples of the OS. The OS controls your computer.
- **Phishing -** Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.
- **PII -** Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Bottom line, anything that can Identify who you are, where you live, who you bank with or anything else that can Identify you.
- **Ransomware -** Ransom, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- **Spam** - SPAM is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk. Spam is a huge waste of time and resources.
- **Spyware -** spyware is simple: it's **spying software**. Typically running unnoticed in the background while it collects information, or gives remote access to its author.
- **SSID** - The easiest way to describe an SSID is to say it is the name given to your WiFi network. SSID = service set identifier.
- **VPN -** A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.

Resources

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

https://www.cisa.gov/

The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging, and our goal is clear - keeping America safe.

https://www.dhs.gov/

Router security

This site focuses on the security of routers. Period. If you are interested in faster Wi-Fi, look elsewhere. And, to be clear, this site is about ROUTER security

https://www.routersecurity.org/index.php

Defensive Computing checklist

This is a list of both things to be **aware of** and specific **defensive steps** that we can take in response to the common threats of 2019. No list like this can ever be complete, nor would anyone want it to be complete as *that* list would never end.

https://defensivecomputingchecklist.com/