The Definitive Cybersecurity Guide

MAXtech

Arm Yourself with Knowledge

To get into the holiday spirit, we've put together some best practices to protect your devices and—more importantly—your personal information.

Securing Your Devices at Work or at Home

It doesn't matter where you are or what device you're using; if you connect it, protect it. Follow these guidelines to keep your stuff safe!

Computers

Passwords

The first line of defense is a good password. Not just to unlock the device itself, but also for any login credentials you may use.

If you don't have strong, unique passwords, you're leaving yourself open to attack from cybercriminals and malware.

Instead, keep yourself protected with these basic password guidelines:

- Use longer, complex passwords with a combination of upper and lower-case letters, numbers and special characters.
- Passphrases, which are a string of unrelated words, make even more secure passwords. Use them in conjunction with the above advice.
- Don't use password hints and reminder questions if at all possible (e.g., "What's your mother's maiden name?"). They're a huge security risk.
- Password managers like LastPass and Myki can generate strong passwords and save them for you.

Multi-Factor Authentication (MFA)

MFA adds another layer to the security of your login credentials. It requires an additional bit of information (or 2 or 3) from you besides your password to gain access.

In most cases, MFA is a code sent either via SMS or email that you must confirm to log in. It can also verify that you're in possession of your mobile device by sending a popup notification to your device to approve the login.

Enable Your Firewall

A firewall is a security device—usually software—that helps protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to private data on your computer.

Both Mac and Windows computers come with a firewall installed and enabled by default. To make sure they're enabled and working properly, check these settings:

- **Windows computers:** Open the Start menu and type "firewall." This will lead you to the Firewall & Network Protection settings. From there, you can see that the firewall is enabled.
- **Mac computers:** Hold Command (⌘) + Spacebar to bring up Spotlight and search for "firewall." This will take you to the Firewall tab in the Security & Privacy settings where you can enable or disable the firewall.

Antimalware

While computers these days are far better equipped to protect your information out of the box, there are still a lot of nefarious folks out there cooking up new ways to get to your stuff.

Again, both Mac and Windows computers have good built-in security, but another layer of protection certainly doesn't hurt. Check out these free, trusted antimalware services:

- Bitdefender Free Edition
- Avast Free Antivirus
- AVG Free Antivirus

Web Privacy Plugins

Whenever you browse the web, your activity leaves a trail of breadcrumbs called "cookies." Cookies can tell someone a lot about your interests and browsing habits.

Social media platforms like Facebook and search engines like Google scoop up these cookies across the web and use this information to build scarily accurate profiles for "marketing purposes." They can also sell it off to the highest bidder to do whatever they want with it.

Thankfully, a number of web browser plugins exist for all major browsers to keep your information away from prying eyes:

- uBlock Origin
- AdBlock Plus
- Privacy Badger
- Ghostery

Virtual Private Network (VPN)

VPNs have been popular for a while now, but with many of us working from home they've become even more common. VPNs help protect your privacy by routing your web traffic through an encrypted 3rd-party server before it reaches its destination.

The end result is your IP address and all of your web traffic are encrypted, thus protecting it from hackers, trackers and even your ISP's wandering eyes.

We'll note that while there are free VPN services available, in this case you're better off opting for one with a paid model. Free VPNs (and most other free services) tend to make the user their product by selling the information gathered by using the service.

Check out these paid VPNs if you're interested in keeping your online activities under wraps:

- NordVPN
- ExpressVPN
- IPVanish
- VyprVPN

Mobile devices

Passwords

While you have a couple options to lock your phone, not all mobile passwords are created equal. There are varying degrees of security and convenience that each password type offers:

- **Password:** As we said above, a long, complex password is the best practice, but it's not the most convenient thing to type in every time you need your device.
- **PIN:** PINs offer a little less security than a full password, but they're much more convenient to use a hundred times per day. While a 4-digit PIN has 10,000 possible combinations, most devices allow you to use up to 8 digits (10,000,000 combinations).
- **Pattern:** Pattern locks are intuitive and convenient. But while the pattern lock gives you 389,112 combinations, many people draw simple patterns that can easily be guessed.
- **Biometric:** Most newer phones offer some sort of biometric lock, whether it's a fingerprint or face/iris scanner. While these seem like the best and most secure option, they do have their weaknesses. For some somewhat extreme (but not implausible) examples, someone could force your finger over the scanner or simply hold the phone in front of your face to unlock it—even if you're sleeping.

Password Protected Apps

Most of us have apps that house all kinds of our private information. Even if you have your device password protected, it's still a great idea to keep your important apps locked up.

Mobile banking and payment apps (like PayPal and Venmo), email apps, cloud drives and other services that keep your private data are all prime targets for exploitation.

While some of these apps offer built-in password or biometric protection, you can download 3rd-party locking apps to protect the ones that don't.

Remote Track/Lock/Wipe

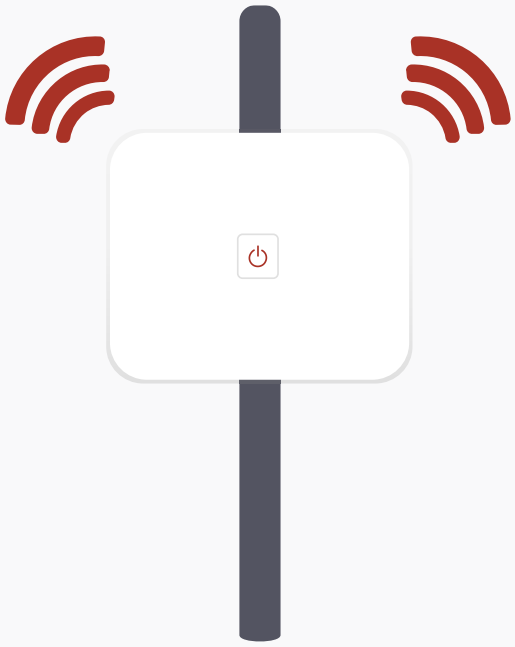
There are few feelings worse than realizing you've lost your mobile device. Whether you misplaced it or it was stolen, having a remote tracking/ service can be a lifesaver.
Both iPhones and Android have free, built-in tracking services that you can access from any device. These services allow you to not only see your device on a map (to within 60 feet or so), you can also have the device ring loudly, lock it down or wipe all its data completely.

Cloud Backup

If your phone is indeed gone for good, having a good cloud backup is critical. There are more cloud services out there than you can shake a stick at, but the standard iCloud or Google Backup services will keep your photos, contacts, text messages and other important information safe and ready to download to a new device whenever you need it.

Home Wi-Fi

Regardless if you're working from home or not, having a secure home Wi-Fi network is a must for everyone. Weak network security can leave your connected devices vulnerable to cybercriminals and other snoopers.



Follow these suggestions to keep your home network safe:

Change Your Default Network Name (SSID) and Password

Your Wi-Fi router came with a default SSID (the name you see in the list of available networks) and password. This information is also printed on the bottom or back of the router, which is not the best security feature.

Make sure when you're setting up your router that you make your own SSID and password, following the above advice regarding password complexity. If you've already set the router up, you can change these by accessing your router's admin panel (usually by just entering "192.168.0.1" into a web browser).

Enable Encryption

Every Wi-Fi router has some sort of encryption protocol, and chances are if you've password-protected your network, it's encrypted using WPA2 (Wi-Fi Protected Access II). WPA2 provides strong data protection and network access control, which means both your network and the devices on it are transmitting encrypted data.

If you want to check that your network is using WPA2, you can check this in the same admin panel mentioned above. If you notice that your network is protected using WEP or WPA (that's the first generation), you will definitely want to change it to WPA2.

Disable Network Name Broadcasting

If you want to take your network security another step further, you can choose to stop your router from showing your network name to other devices looking for a wireless network. You've probably noticed that when you go to connect to a network, you might have a bunch of network names to choose from, likely from neighbors or nearby businesses. If you disable network name broadcasting, your network will not show up on that list. Anyone wanting to connect to it will need to set the network up manually on their device using the correct SSID, password and security protocol.

General Security Tips

Update Your Security Software Often

Technology evolves fast, and unfortunately, hackers and other malicious actors evolve along with it as they try to best it. Make sure you're updating your security software regularly to close any newly formed security loopholes.

Avoid Clicking Pop-Up Ads, Emails from Unknown Senders & Suspicious Links

Pop-up ads have been the bane of internet existence for as long as they've been around—the dude that invented them even hates them. They almost never lead anywhere good. As a general rule of thumb, don't click on anything that you're unsure of or that looks suspicious.

Never Write Down Passwords or Other Login Information

Complex passwords are critical for good security, but they're also hard to remember. That being said—never write any login information down. We can't tell you how many security breaches have resulted from someone writing their password down. If your password is too complex to remember (and if you type it in enough, muscle memory should kick in eventually) use a password manager like those we've mentioned above.

Beware Phishing and Other Social Engineering Techniques

With many people working from home, phishing and other social engineering attacks have been on the rise. With phishing, cybercriminals exploit the gullible or uninformed. They try to get you to download malware or give away personal information by exploiting your emotions—be they fear, anxiety, curiosity or trust.

Cybercriminals using phishing attacks or other social engineering techniques will pose as friends, government officials, representatives from big-name companies, or even colleagues, executives or IT workers from your own company.

Be wary of any communication asking for personal information and login credentials, and keep these things in mind:

- Your boss probably didn't email you asking for $500 worth of gift cards to Sephora with a promise to repay you.
- Your IT department will never ask for your password.
- Payroll won't ask for your banking information via email.

MAXtech Is Here to Help

With so much of our personal and work lives online and accessible from multiple devices, good cybersecurity is critical to keep your information safeguarded. While these basic recommendations will keep most people generally safe, you still need to exercise due caution whenever you're online.

If you're a small business and you need help setting your employees up for remote work, don't skimp on security! MAXtech is here to help you get everything set up correctly and securely. Contact us here or call us at 614-401-8800 to see what we can do for you.