YOUR ULTIMATE CHECKLIST
END USER SECURITY

AMTRA SOLUTIONS

Are you doing all that you can to help keep corporate data secure? Follow these simple steps to make sure you are part of the solution, and if you have questions, ask your IT team or call an AMTRA security expert.

1. **Policies and Procedures.** Review your IT security policies. If you don't know where they are, ask. Below are best practices, but your IT team likely has organization-specific policies in place. Knowing and following these policies will be helpful for your IT team, and—more importantly—should something go wrong, you'll know the procedure to follow to help expedite remediation.

2. **Unplugging.** If you think you might have a virus, or there is anything suspicious happening on your computer, disconnect from the network immediately! Shut down your computer and unplug it. Should it turn out to be a virus or other malicious activity, these actions will help to contain it. Then, notify your IT team right away.

3. **Plugging In.** Did you know that viruses can be transmitted via external hard drives, mobile phones or even flash drives? Make sure you trust the source before you plug it in!

4. **Be Password Smart!** For more information on password best practices, check out our blog, which includes a link to a full paper from Microsoft for both end users and IT.

5. **Back It Up.** It is likely that your company is spending a significant amount of money for a back-up and disaster recovery solution. If something goes wrong, this is one of the best ways to make sure you don't lose your data, but if you have files sitting on your desktop, it isn't going to work. If someone else, connected to the network, gets a virus, it could spread to your devices and corrupt your files.

6. **Be Aware.** The more aware we are of potential threats, the more likely we are to avoid them. Don't become complacent. That includes being aware of the risks associated with connecting to an unsecured or unfamiliar WiFi network, using a shared device, or even sharing information on social media. If it is open to the public, it is open to a hacker.

7. **Lock It Down.** Walking away? Lock your computer. Put a passcode on your smartphone. All of your devices are just as vulnerable as your PC, so don't leave them unlocked or unattended.

8. **Stay Current.** Keep your software and anti-virus up to date. If your anti-virus is doing a scan, don't cancel it—it is doing it for a reason! And do us a favor, double check that you don't have Apple Quick Time for Windows software on your computer. If you do, remove it immediately! No, really, do it now!

9. **Verify.** Do you know the sender? Are you expecting that attachment from that sender? If you receive an unsolicited email, treat all files and links within as potentially dangerous. This is also true for offers found online and even callers. Be cautious of free offers, competitions, or file sharing sites, as well as callers asking for any contact details or data. These are often methods used by hackers to gather information that will help them gain access.

At AMTRA we believe in combining people, processes, and technology to keep organizations secure. If you have any questions, or would like a security assessment for your organization, give us a call.

www.amtrasolutions.com | 855.326.0533