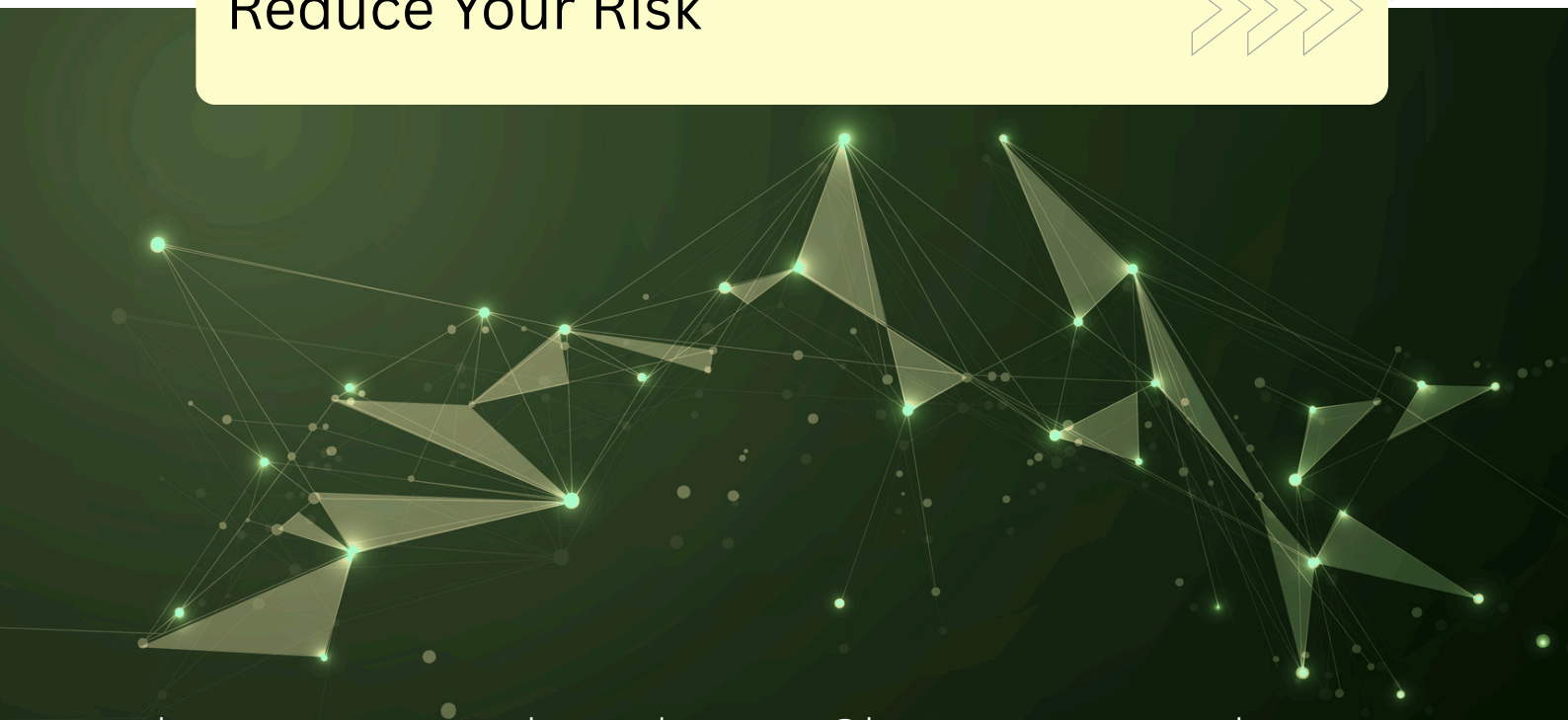
DIGITAL SECURITY CHECKLIST

Reduce Your Risk



bettercomputertech.com | contact@bettercomputertech.com

FORWARD

This e-book offers potential cost savings, as a single computer repair can often exceed $80 per hour at most service providers. Typically, a standard computer repair requires a minimum of one hour to complete. While the duration may be longer for individuals with limited experience, we advise taking your time and proceeding deliberately. It is crucial to double- and triple-check each step, as errors can lead to more significant and costly issues.

Please note: Due to the inherent risks involved in computer repair, we strongly recommend seeking assistance from a qualified professional if you lack confidence or experience. Incorrect actions can result in further damage and increased expenses. However, if you possess a degree of technical aptitude and can follow instructions carefully, this guide may be a valuable resource.

IMPORTANT NOTICE: This e-book is provided for educational purposes only. Any actions you undertake are your sole responsibility. By using this guide, you agree to hold the authors and publishers harmless from any liability for damages or injuries resulting from your attempts to follow these instructions.

PLEASE READ AND FULLY UNDERSTAND ALL INSTRUCTIONS CONTAINED WITHIN THIS E-BOOK BEFORE ATTEMPTING ANY REPAIRS TO ENSURE A COMPREHENSIVE UNDERSTANDING OF THE PROCESS.

LEGAL DISCLAIMER

The information provided herein is intended for general informational purposes only. While every effort has been made to ensure the accuracy[1] of the content, all information is provided in good faith without any representation or warranty, express or implied, regarding its accuracy, adequacy, validity, reliability, availability, or completeness.

Under no circumstances shall the authors or publishers be held liable for any loss or damage of any kind incurred as a result of the use of or reliance on any information presented within this document. Your use of this information and any reliance thereon is strictly at your own risk.

This document does not constitute professional advice. The information contained herein is for general informational and educational purposes only and should not be considered a substitute for professional guidance.

Accordingly, before taking any action based on the information provided, we strongly encourage you to consult with qualified professionals. We do not offer any form of professional advice. Any reliance on the information contained within this document is solely at your own risk.

DISCLAIMER OF LIABILITY

Exercise caution when following these instructions or any other computer maintenance procedures. Incorrect actions, such as deleting essential files or removing critical programs, can cause significant damage. Specific results are not guaranteed, and there may be instances where these steps are not applicable to your particular computer system.

By using this guide, you agree to hold A Better Tech, its affiliates, and any individuals associated with or involved in its creation harmless from any damages arising from work performed by you or any other party on your computer. Your acceptance of this document signifies your receipt and understanding of this disclaimer.

FURTHER ASSISTANCE AND RESOURCES

If the provided steps do not resolve your issue, it is possible that your computer has more complex problems requiring professional attention. We recommend seeking a reputable local computer repair shop. When selecting a service provider, ensure they are professional, courteous, and offer competitive pricing.

CONTACT INFORMATION (For Local Users)

If you are located in the Spring, TX area, you can contact **A Better Tech** for assistance:

Phone: 832-510-7222
Website: https://bettercomputertech.com
Email: contact@bettercomputertech.com

Introduction

Protecting your digital life is more important than ever. This checklist provides essential steps to safeguard your personal information, devices, and online accounts from common threats. Follow these simple guidelines to build a stronger defense against cyberattacks and ensure a safer digital experience for yourself, your family, or your small business.

Strong Passwords

☑ **Use a unique, strong password for each account.**

- A strong password should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and symbols.
- Avoid using easily guessable information like your name, birthday, or pet's name.

☑ **Use a password manager.**

- Password managers can generate and securely store complex passwords, so you don't have to remember them all.

☑ **Regularly update your passwords.**

- Change your passwords every 3-6 months, or immediately if you suspect a breach.

☑ **Regularly review account permissions.**

- Periodically check connected apps and services on your social media, Google, and Microsoft accounts.
- Remove any apps or services you no longer use or don't recognize. These could be potential security risks.

Multi-Factor Authentication (MFA or 2FA)

☑ **Enable MFA whenever possible.**

- MFA adds an extra layer of security by requiring a second verification method, such as a code sent to your phone or an authenticator app, in addition to your password.

☑ **Understand the different MFA methods.**

Software Updates

☑ **Keep software updated.**

- Enable automatic updates for your operating system (Windows, macOS, iOS, Android) and all your applications (browsers, antivirus, productivity software).

Antivirus & Anti-Malware Software

☑ **Use reputable antivirus/anti-malware software.**

- Install and keep active a trusted antivirus program on all your computers.
- Set up regular scans to detect and remove malicious software.

Firewalls

☑ **Enable firewalls.**

- Ensure your operating system's built-in firewall is enabled on all computers.
- Your home router also has a firewall that should be active.

Mobile Devices

☑ **Secure your mobile devices.**

- Use a strong passcode or biometric authentication (fingerprint, face ID) on your smartphones and tablets.
- Set up features like "Find My iPhone" or "Find My Device" (Android) to locate, lock, or remotely erase your device if it's lost or stolen.
- Be mindful of the permissions apps request on your phone. Only grant access to what's necessary.

Network Security

☑ **Secure your Wi-Fi network.**

- Change the default administrator username and password on your router.
- Change the default network name (SSID) and password on your router.
- Use a strong Wi-Fi password (WPA3 encryption is recommended if your router supports it).
- Enable a separate guest network for visitors to keep your main network isolated.
- Enable the firewall on your router.

☑ **Be wary when using public Wi-Fi.**

- Avoid conducting sensitive activities (banking, shopping, logging into critical accounts) on unsecured public Wi-Fi networks.
- Use a VPN to encrypt and protect your data from eavesdropping on public networks.

Phishing & Scams

☑ **Be wary of suspicious emails and links.**

- Be suspicious of unsolicited emails, texts, or calls asking for personal information, passwords, or demanding urgent action.
- Phishing emails often contain urgent or threatening language, grammatical errors, and requests for personal information.
- Do not click on links or open attachments from unknown senders.

☑ **Verify the sender's identity.**

- Before responding to an email, verify the sender's identity by contacting them through a separate channel (e.g., phone call).

☑ **Report phishing attempts.**

- Report phishing emails to your email provider and to the relevant authorities.

Data Backup

☑ **Back up your important data regularly.**

- Create backups of your files, photos, and other important data on a regular basis.

☑ **Use a combination of backup methods.**

- Consider using both local backups (e.g., external hard drive) and cloud backups (e.g., cloud storage services) for redundancy.

☑ **Test your backups.**

- Periodically test your backups to ensure that you can restore your data in case of a disaster.

☑ **3-2-1 rule.**

- Keep 3 copies of your data, on 2 different types of media, with 1 copy off-site (e.g., cloud).

Online Safety

☑ **Shop on secure websites.**

- Look for the padlock icon in the address bar and make sure the website's URL starts with "https://".

☑ **Use strong passwords for online shopping accounts.**

- Avoid using the same password for multiple online shopping accounts.

☑ **Be cautious of fake online shopping sites.**

- Fake shopping sites can be very convincing. Check the URL and look for errors in spelling and grammar.

More Online Safety

☑️ **Think before you click/share.**
- Exercise caution when clicking on links or downloading attachments from unknown sources.

☑️ **Limit personal information**
- Be mindful of how much personal information you share on social media and public forums.

☑️ **Review privacy settings.**
- Regularly check and adjust privacy settings on your social media accounts and other online services.

Important Disclaimer: No security measure is 100% foolproof. This checklist provides general guidance for improving digital security. It is not a guarantee against all possible threats. For advanced security needs or specific vulnerabilities, professional assistance may be required.

By implementing these digital security practices, you can better protect yourself from cyber threats. Regularly review and update your security measures to stay ahead of evolving threats. Remember, staying vigilant is key to maintaining a safe digital environment.

Thank you for downloading our e-book and for joining our community! We hope these resources empower you to confidently tackle your DIY computer maintenance and repair tasks. For more in-depth guides, tutorials, and the latest tech tips, be sure to visit our blog and subscribe to our *YouTube* channel. We regularly share new content and offer a variety of other helpful digital downloads to enhance your tech know-how. Stay tuned for more valuable resources coming your way!