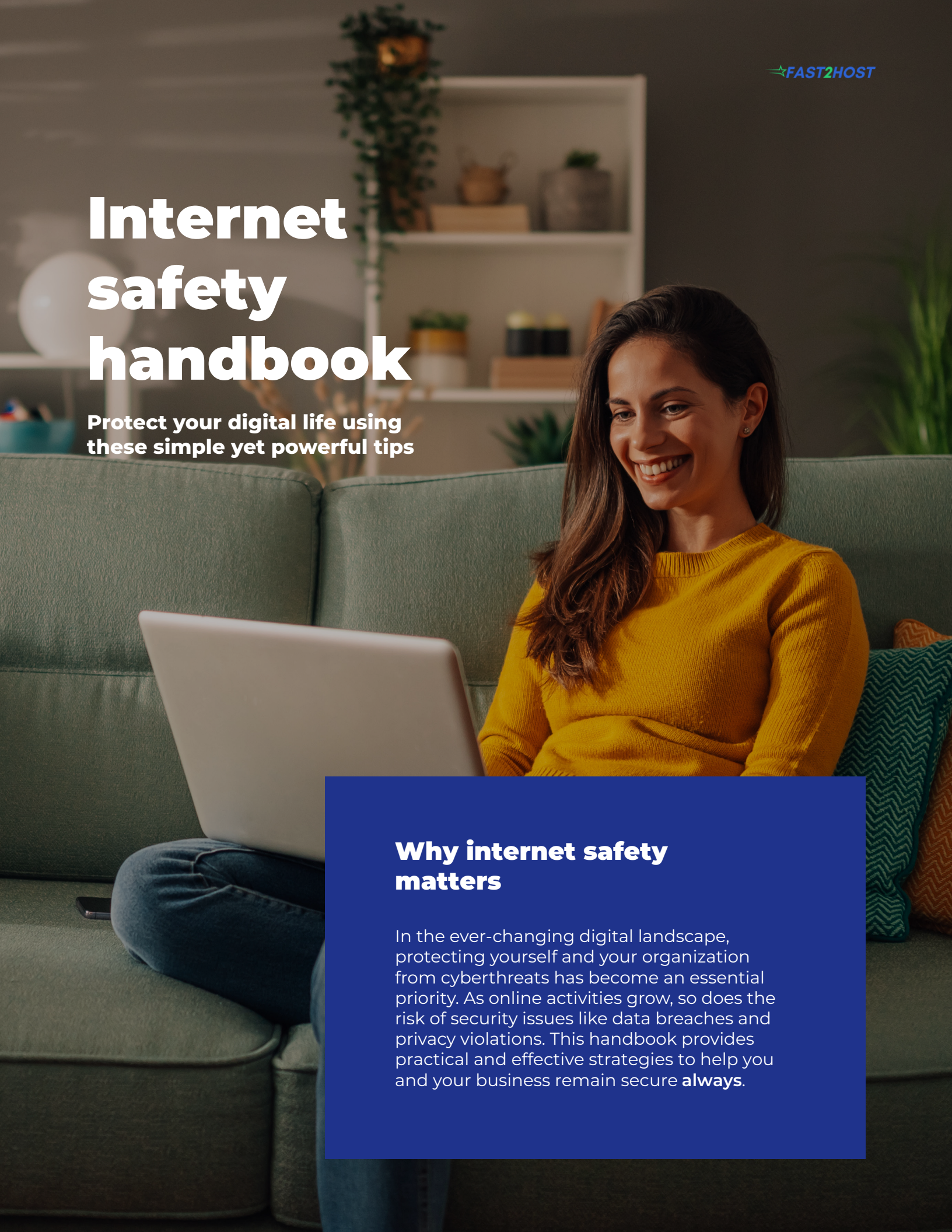


FAST2HOST

# Internet safety handbook

**Protect your digital life using these simple yet powerful tips**

## Why internet safety matters

In the ever-changing digital landscape, protecting yourself and your organization from cyberthreats has become an essential priority. As online activities grow, so does the risk of security issues like data breaches and privacy violations. This handbook provides practical and effective strategies to help you and your business remain secure **always**.

Chapter 1

## Password security

- **Use a password manager:** A password manager generates and stores strong, unique passwords for each account, reducing the risk of password reuse and making it easier to manage complex passwords.
- **Complex passwords:** Use a string of words that are entirely unrelated and not easily guessed. If this isn't possible, ensure your passwords are at least 12 characters long and include a mix of uppercase and lowercase letters, numbers and special characters.
- **Avoid personal information:** Do not use personal information such as your name, birthdate, or common words in your passwords, as these are easily guessed.
- **Enable multi-factor authentication (MFA):** Enable MFA on all accounts that support it. MFA adds an extra layer of security, requiring a second form of verification (e.g., a code sent to your smartphone).

**Fun Activity:** Use a trusted online tool to test the strength of your passwords and ensure they meet the recommended complexity standards.

Chapter 2

## Recognizing phishing attacks

- **Grammatical errors:** Phishing emails often contain poor grammar and spelling mistakes. Be wary of any communication that seems unprofessional.
- **Requests for sensitive information:** Legitimate organizations rarely ask for sensitive information like financial details via email or text. If you receive such a request, verify it through a trusted channel.
- **Unfamiliar links or sender addresses:** Hover over links to see their destination before clicking. Check the sender's email address for any discrepancies or unfamiliar domains.
- **Urgency and threats:** Phishing emails often create a sense of urgency or threaten negative consequences if you do not act quickly. Stop and take a moment to verify the legitimacy of the request.
- **Report suspicious emails:** If you suspect an email is a phishing attempt, report it to your IT or security team immediately. They can take steps to protect the organization and other employees.

**Quick Fact:** Did you know according to a report by security company Egress, 94% of organizations were victims of phishing attacks, of which 96% were negatively impacted?

Chapter 3

## Secure your devices

- **Regular software updates:** Keep your operating system, applications, and firmware up to date to protect against known vulnerabilities.
- **Reputable antivirus software:** Use antivirus software from a trusted provider and ensure it is always running and updated.
- **Avoid public Wi-Fi:** Public Wi-Fi networks are often unsecured and used by attackers to intercept your data. If you must use public Wi-Fi, use a Virtual Private Network (VPN) to encrypt your connection.
- **Physical security:** Keep your devices in a secure location and use strong physical security measures like locks or alarms.

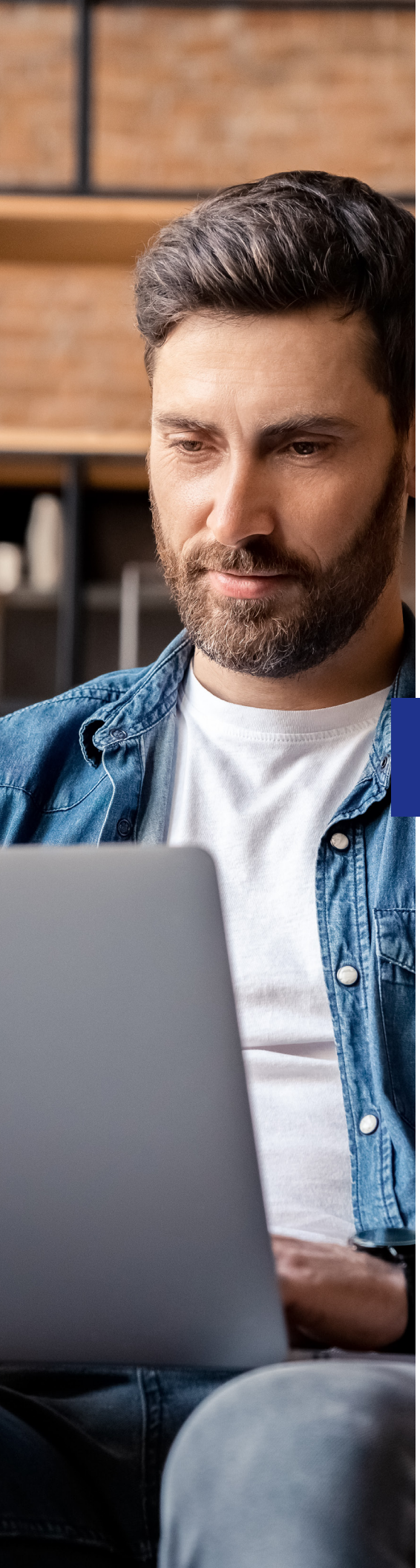
**Pro Tip:** Enable "Find My Device" on smartphones and laptops to help locate them if they are lost or stolen.

Chapter 4

## The 3-2-1 Backup Rule

- **3 copies of data:** Always keep at least three copies of your important data. This ensures redundancy and reduces the risk of data loss.
- **2 different media:** Store these copies on at least two different types of storage media, such as hard drives, SSDs and cloud storage. It helps protect against media-specific failures.
- **1 offsite copy:** Keep one copy of your data offsite in a physical location like a safe deposit box or a cloud storage service. This protects against local disasters like fires or floods.
- **Cloud solutions:** Utilize cloud-based backup services that offer real-time backups and encryption to ensure your data is always safe and accessible.
- **Test backups regularly:** Periodically test your backups to ensure they are working correctly and you can restore data when needed.

**Toolbox:** Recommend using reliable backup software or solicit the services of a reputable MSP like ourselves. Contact us, and we can help back up your data.



Chapter 5

## Safe browsing habits

- **Verify website URLs:** Always double-check the URL of a website before entering any sensitive information. Look for misspellings or unusual domain names.
- **Secure HTTPS connections:** Ensure the website you are visiting uses HTTPS, indicated by a lock symbol in the browser bar. HTTPS encrypts your data, making it harder for attackers to intercept.
- **Ad-blockers:** Use ad-blockers to reduce the risk of encountering malicious ads that can lead to malware infections.
- **Browser security settings:** Configure your browser to block pop-ups, disable third-party cookies, and enable phishing and malware protection.
- **Regularly clear cache and cookies:** Clear your browser's cache and cookies to remove any potential tracking data and reduce the risk of session hijacking.

**Pro Tip:** Unprotected browsing sessions are a common form of cyberattacks. Using secure connections and ad-blockers can significantly reduce this risk.

Chapter 6

## Educate your team

- **Regularly train employees:** Conduct regular cybersecurity training sessions to inform employees about the latest threats and best practices.
- **Phishing awareness:** Teach employees how to recognize and report phishing attempts. Use simulated phishing emails to test and improve their awareness.
- **Secure file sharing:** Educate employees on the risks of using unsecured file-sharing services and provide them with secure alternatives.
- **Password hygiene:** Train employees on the importance of strong passwords and the use of password managers.
- **Clear policies:** Develop and distribute clear internet usage and cybersecurity policies. Ensure all employees understand and follow these guidelines.
- **Blame-free reporting:** Foster a culture where employees feel safe reporting suspicious activity without fear of retribution. Encourage them to ask questions and seek help when unsure.

## The future of online safety

The digital world is ever-changing, but one thing remains constant: safety comes first. Implementing these strategies will significantly enhance cybersecurity and protect your personal and organizational data.

Share this guide with your network, and let's build a safer internet together! Contact us today:

**Fast2host** | https://www.fast2host.com
support@fast2host.com
+441480260000