

WILTECH



SIMPLE TECH GUIDES



DIGITAL SAFETY MADE SIMPLE

A beginner-friendly guide to protecting
your phone, passwords, accounts, money,
and personal information online.

SAMPLE PREVIEW • NOT THE FULL PRODUCT

Contents

1. Your Digital Life and Why It Matters
2. The Threats You Are Most Likely to Meet
3. Strong Passwords Without the Confusion
4. MFA, Passkeys, and Recovery Methods
5. Phishing, Fake Messages, and Social Engineering
6. Protecting Your Smartphone and Computer
7. Safer Online Shopping, Banking, and Payments
8. Social Media Privacy and Oversharing
9. Public Wi-Fi, Home Wi-Fi, and Smart Devices
10. Apps, Downloads, Permissions, and Malware
11. Protecting Personal and Family Information
12. Updates, Backups, and Safe Device Disposal
13. What to Do If an Account Is Hacked
14. Your 7-Day Digital Safety Reset

[Glossary, Resources, and Final Checklist](#)

CHAPTER 3

Strong Passwords Without the Confusion

Create long, unique passwords, avoid personal clues, and use a password manager safely.

The three qualities that matter most

A strong password should be long, unique, and difficult to predict. Length makes guessing harder. Uniqueness prevents a stolen password from unlocking other accounts. Unpredictability means the password is not based on information another person can find or guess.

Modern guidance places strong emphasis on length. For an important account, aim for at least 15 characters when the service allows it. A password manager can create much longer random passwords without requiring you to memorize them.

Mixing uppercase letters, lowercase letters, numbers, and special characters can increase the number of possible combinations, especially when the result is long and random. However, replacing an A with @ in a short familiar word does not make it truly unpredictable. Length and uniqueness still matter more than a clever-looking pattern.

AVOID PERSONAL DATES

Do not build passwords from birthdays, anniversaries, graduation years, addresses, phone numbers, children's names, pet names, sports teams, or other details that appear in your life or social media.

Two safe ways to create passwords

Method 1: Let a password manager generate it

This is the easiest choice for most accounts. A password manager can generate and store a long random password such as a mixture of letters, numbers, and symbols. You do not need to type or remember it each time. The manager fills it after you unlock the vault.

Use a different generated password for every account. If one website is breached, the stolen password will not work elsewhere.

Method 2: Use a long passphrase you can remember

A passphrase is a longer password made from several unrelated words. Add separators, numbers, or changes in capitalization when helpful and when the service accepts them. The words should not form a famous quote, lyric, personal sentence, or predictable phrase.

CHAPTER 5

Phishing, Fake Messages, and Social Engineering

Recognize manipulation in email, texts, calls, QR codes, ads, and direct messages.

Phishing is a story designed to move you

A phishing message is rarely just a bad link. It is a story designed to create emotion and speed. You may be told that a package cannot be delivered, an account will close, a payment failed, a family member needs help, a refund is waiting, or suspicious activity requires immediate action.

Professional grammar and a familiar logo do not prove that a message is real. Criminals can copy branding, use artificial intelligence to improve writing, imitate voices, and create realistic websites. Focus on the request and verify it independently.

The STOP method

1. Slow down. Do not let urgency choose for you.
2. Think about the request. Is it unexpected? Does it ask for money, credentials, a code, remote access, or secrecy?
3. Open the official app or type the known website address yourself. Do not use the message link.
4. Prove the request through a trusted channel. Call a saved number, use the number on a card or statement, or ask the person through a different method.

A LINK CAN LOOK RIGHT AND STILL BE WRONG

On a computer, hovering may reveal the destination, but criminals also use look-alike addresses and shortened links. The safest method is to open the official app or enter the known address yourself.

Common phishing stories

- Package delivery problem or unpaid customs fee.
- Bank fraud alert that tells you to call a number in the message.
- Password expiration or mailbox storage warning.
- Invoice, document, voicemail, or shared-file notification you were not expecting.
- Prize, refund, tax payment, job offer, investment, or cryptocurrency opportunity.
- Family emergency requesting secrecy or fast payment.
- Technology support warning asking for remote access.
- Marketplace buyer asking for a verification code.

DIGITAL SAFETY BUNDLE



ACTION WORKBOOK

Audits, checklists, a 7-day reset plan, phishing red flags, and an emergency recovery worksheet.

SAMPLE PREVIEW • NOT THE FULL PRODUCT

5. Phishing Red Flags Cheat Sheet

TERM	PLAIN-ENGLISH MEANING
Urgency	Act now, your account closes today, or a package will be returned immediately.
Fear	Your money is at risk, police are coming, taxes are overdue, or your device is infected.
Secrecy	Do not tell your bank, family, employer, or anyone else.
Unusual payment	Gift cards, cryptocurrency, wire transfer, cash courier, or money moved to a safe account.
Verification code	Someone asks you to read a code sent to your phone or email.
Remote access	A caller or pop-up asks to control your computer or phone.
Unexpected attachment	An invoice, voicemail, document, or resume you were not expecting.
Login link	A message asks you to sign in instead of opening the official app or known website.
Changed payment details	A supplier or coworker suddenly requests a new bank account.
Too good to be true	A prize, refund, investment return, job, or extreme discount with pressure to act.

STOP

Slow down. Think about the request. Open the official app or known website. Prove the request through a separate trusted channel.