

“The Digital Shield:

Protecting Yourself from Cyber

Threats”



Contents

Foreword **Error! Bookmark not defined.**

1. Introduction to Online Safety: 3

2. Creating Strong & Secure Passwords: 4

3. Recognizing & Avoiding Scams: 6

4. Safe Browsing & Avoiding Malware: 8

5. Protecting Your Personal Data: 9

6. Final Tips & Resources: 9

1. Introduction to Online Safety:

The internet has transformed how we communicate, shop, and work, but it also presents risks. Cybercriminals constantly look for ways to steal personal information, financial data, and passwords. Understanding these risks is the first step toward protecting yourself.

Common Cyber Threats

- **Phishing:** Emails or messages pretending to be from legitimate companies, tricking you into giving away personal information.
- **Hacking:** Unauthorized access to your accounts, devices, or personal data.
- **Identity Theft:** Someone using your personal details to commit fraud.
- **Scams:** Fake job offers, lottery winnings, and romance scams designed to steal money or information.

By the end of this guide, you'll be equipped with the knowledge to **identify and prevent these threats** before they happen.

2. Creating Strong & Secure Passwords:

A strong password is your first line of defence against hackers.

What Makes a Strong Password?

- At least **12 characters long**
- Includes **uppercase & lowercase letters, numbers, and symbols**
- Not related to personal details (avoid names, birthdays, or "password123")
- Unique for every account (don't reuse passwords!)



P A S S W O R D

How to Use a Password Manager

A **password manager** stores and creates strong passwords for you, so you don't have to remember them all. Some trusted ones include:

- **Bitwarden**
- **1Password**
- **LastPass**

Two-Factor Authentication (2FA)

- This adds an extra layer of security by requiring a second step (a code sent to your phone or email) before logging in.
Always enable 2FA for important accounts like:
 - Banking & finance apps
 - Email accounts
 - Social media

3. Recognizing & Avoiding Scams:

Cybercriminals are becoming smarter, and scams are harder to detect. Here's how to **spot and avoid them**.

Common Scams & How to Avoid Them:

Scam Type	How It Works	How to Avoid It
Phishing Emails	Fake emails from "banks" or "tech support" asking for personal info.	Never click suspicious links. Verify senders before responding.
Phone Scams	Callers pretending to be from Microsoft, Amazon, or HMRC.	Hang up & call the official number to verify.
Social Media Scams	Fake giveaways or messages from hacked accounts.	Avoid clicking unknown links. Double-check with the sender.

What to Do If You Get Scammed

- **Don't panic.** Change your passwords immediately.
- **Report it** to Action Fraud UK or relevant authorities.
- **Monitor your accounts** for unusual activity.



4. Safe Browsing & Avoiding Malware:

How to Identify Secure Websites

- Always check for "https:///" in the URL (secure websites).
- Look for a **padlock icon** in the address bar.
- Avoid sites with **too many pop-ups or requests for personal data**.

Best Free & Paid Security Software

Free	Paid
Avast Free Antivirus	Norton 360
Bitdefender Free	Bitdefender Total Security
Windows Defender (built-in)	McAfee Total Protection



5. Protecting Your Personal Data:

Social media and apps collect **huge amounts of data** about you. Here's how to **limit what they know**.

- **Check privacy settings** on Facebook, Instagram, and Google.
- **Limit app permissions** (e.g., why does a flashlight app need your location?)
- **Be cautious** about sharing personal details publicly.

6. Final Tips & Resources:

Daily Habits for Better Security

- ✓ Keep your software and apps **updated**.
- ✓ Use a **different password** for each account.
- ✓ Don't **overshare** on social media.
- ✓ If something sounds **too good to be true, it probably is**.

I'd love to hear how you have implemented this guide. Please feel free to write me directly at: milan.gurung@outlook.com

