

Safety Practices to Protect Yourself from Online Threats

Staying safe online is crucial to protect your personal data, finances, and digital identity. Here are essential safety practices (“parasites” can be corrected as “practices”) to follow:

1. Use Strong, Unique Passwords

- Create complex passwords using a mix of letters, numbers, and symbols.
- Avoid using the same password for multiple sites.
- Use a trusted password manager to store your credentials.

2. Enable Two-Factor Authentication (2FA)

- Add an extra layer of security with 2FA on all important accounts (email, banking, social media).

3. Beware of Phishing Scams

- Don’t click on suspicious links or download attachments from unknown sources.
- Double-check email addresses and URLs for authenticity.
- Never share personal information over email or phone unless you initiated contact.

4. Keep Software Up to Date

- Regularly update your operating system, apps, browsers, and antivirus programs to patch vulnerabilities.

5. Secure Your Devices

- Use a screen lock (PIN, password, or fingerprint) on smartphones and computers.
- Install trusted antivirus and anti-malware software.

6. Use Secure Connections

- Avoid public Wi-Fi for sensitive transactions; use a VPN when needed.
- Only enter personal or financial information on websites with HTTPS.

7. Monitor Bank and Credit Accounts

- Review statements regularly for unauthorized transactions.
- Set up instant alerts for account activity.

8. Manage Privacy Settings

- Limit what information you share on social media and adjust privacy controls.
- Be wary of apps requesting unnecessary permissions.

9. Backup Important Data

- Regularly backup your files to a secure cloud service or external device.

10. Educate Yourself & Stay Informed

- Learn about new and emerging online threats.
- Participate in cybersecurity awareness programs.

Stay alert and proactive. Safe online habits protect your identity, money, and peace of mind!