■■ Security Awareness Notes (Practical Guide)

■ Purpose

To help individuals and small teams strengthen their cybersecurity habits and reduce the risk of common threats such as phishing, password leaks, and social engineering.

■ 1. Password Security

- Use a password manager to generate and store unique passwords for every account.
- Enable Multi-Factor Authentication (MFA) wherever available — especially for email, banking, and admin accounts.
- Avoid using easily guessed passwords such as 'password123', birthdays, or pet names.
- A passphrase (e.g., four random words) is often easier to remember and more secure than a short complex password.

■■ 2. Phishing Awareness

- Check the sender’s email address — small typos can indicate fake accounts.
- Hover over links before clicking — make sure they lead to legitimate domains.
- Beware of urgency — phrases like 'act now' or 'your account will be closed' are common red flags.
- Don’t download unexpected attachments or share credentials via email.
- When unsure, verify with the sender using another communication channel.

■ 3. Device & Data Protection

- Keep your operating system and apps updated. Turn on automatic updates.
- Lock your device when leaving your desk, even for a few minutes.
- Encrypt sensitive data — use full-disk encryption on laptops and strong screen locks on phones.
- Backup important files to secure cloud storage or offline drives.

■ 4. Safe Internet Practices

- Use HTTPS websites and avoid submitting data on unencrypted pages.
- Avoid public Wi-Fi for confidential work — or use a VPN.
- Limit sharing personal information on social media (e.g., birthday, workplace, travel plans).
- Check app permissions before installing — avoid apps that request unnecessary access.

■ 5. Reporting and Response

- Report suspicious emails or system behavior to your IT/security team immediately.
- If you suspect a data leak or phishing click, change your passwords and notify your administrator.
- Preserve suspicious emails’ headers and attachments when requested — they can help investigate.

■ Quick Security Checklist

Task	Frequency	Status
Enable MFA on key accounts	Once	■
Update software and OS	Weekly	■
Review app permissions	Monthly	■
Backup critical files	Weekly	■
Review password manager entries	Quarterly	■

■ References

- CISA: Security Tips
- NCSC UK: Phishing Guidance
- StaySafeOnline.org