Nine Essential Cyber Security Habits to Adopt Today

1. Pause Before You Click!

Think twice before clicking on links or opening attachments, even if they appear to come from someone you know.

- Always navigate to websites through a known, legitimate source (Eg. HTTPS) instead of clicking on unknown links.
- If an attachment seems unexpected, confirm with the sender via a trusted method or choose not to click, to be on the safer side.

2. Verify Requests for Personal Information

Always confirm requests for private data—whether it's yours or someone else's.

- Scammers can easily impersonate trusted contacts.
- Regularly review financial statements and credit reports for unusual activity.
- Many phishing messages contain spelling and grammatical errors.
- Consider whether the request is legitimate. Is the person or organization likely to need that information?

3. Control Your Passwords

Creating strong, complex passwords and managing them wisely is essential for keeping your accounts secure.

- Use unique passwords for different accounts.
- Keep work and personal passwords separate.
- Never share passwords.
- Change password frequently.
- Opt out of saving passwords in browsers.
- Enable multi-factor authentication (MFA) for added security.

4. Secure Your Devices

Lock up your workspace and protect your devices when stepping away.

- Always lock your computer screen.
- Take your phone and portable devices with you or store them securely.
- Utilize strong authentication methods whenever possible.

5. Backup Important Files

Ensure that your critical data is backed up regularly.

- Store backups in a separate location from originals.
- Use organization-approved storage solutions.
- Regularly test backups to ensure they function properly.

6. Report Suspicious Activity

If something seems suspicious, trust your instincts—report it!

- Alert your supervisor and follow your organization's reporting protocol for suspected scams or suspicious activities.

7. Educate Yourself and Others

Stay informed about the latest cyber security threats and trends.

- Attend training sessions and share knowledge with colleagues as and when you get an opportunity.
- A well-informed team is your first line of defence against cyber threats.

8. Use Secure Networks

Always connect to secure networks, especially when accessing sensitive information.

- Avoid public Wi-Fi for financial transactions or sensitive work.
- Use a Virtual Private Network (VPN) when necessary for added protection.

9. Be Cautious with social media

Limit the amount of personal information you share online. So you can protect your privacy, enhance your safety, and create a more positive online experience.

- Review privacy settings on social media platforms.
- Be mindful of friend requests and who has access to your information; do not accept requests from a locked profile.
- Regularly audit your online presence to minimize potential risks.

Remember: Cyber Security is Everyone's Responsibility!