Staying Safe Online: for Stuck Parents

Abusers may exploit technology to monitor, harass, or control. Taking steps to protect your digital security can help maintain your privacy and safety.

1. Secure Your Devices and Accounts

- **Use Strong, Unique Passwords**: Create complex passwords for each account. Avoid using easily guessed information such as birthdays or common words. Consider using a reputable password manager to keep track of them.
- **Enable Two-Factor Authentication (2FA)**: Activate 2FA on all accounts that offer it. This provides an additional layer of security by requiring a second form of verification alongside your password.
- **Keep Software Updated**: Regularly update your devices' operating systems and applications to protect against security vulnerabilities.

2. Manage Privacy Settings

- **Adjust Social Media Privacy Settings**: Control who can see your information by reviewing and limiting the visibility of personal details and posts to trusted individuals.
- **Turn Off Location Sharing**: Disable location services on apps unless absolutely necessary, and avoid sharing your real-time location publicly.

3. Detect and Prevent Unauthorised Access

- **Check for Unfamiliar Devices**: Regularly review devices connected to your accounts and remove any you don't recognise.
- **Monitor Account Activity**: Watch for unusual activity, such as unrecognised logins or password changes, and address these issues promptly.

4. Browse the Internet Safely

- **Use Private Browsing Modes**: When researching sensitive topics, use private or incognito modes to avoid storing your browsing history.
- **Clear Browser History**: Regularly delete your browsing history, cookies, and cache, especially after accessing sensitive information.

5. Communicate Securely

- **Use Encrypted Messaging Apps**: Choose messaging platforms that offer end-to-end encryption to ensure your conversations remain private.
- **Beware of Phishing Attempts**: Avoid clicking on suspicious links or sharing personal information in response to unsolicited messages.

6. Understand Technology-Based Abuse

- **Recognise the Signs**: Be aware of behaviours such as someone demanding access to your devices, installing tracking apps without your consent, or monitoring your online activities.
- **Seek Help**: If you suspect you're experiencing tech-based abuse, contact organisations specialising in digital safety for support.

7. Access Support Resources

- **Chayn**: www.chayn.co
- **Women's Aid**: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/cover-your-tracks-online/

Remember: While these steps can enhance your online safety, it's important to create a personalised safety plan that fits your circumstances. Consider seeking advice from GlobalARRK or your local DV organisation on creating a safety plan.