Digital boundaries are just as important as physical ones

This guide provides practical steps to protect your digital presence and reduce the risk of online stalking or cyberstalking.

1 Report and block suspicious accounts

If you do not know the person/entity behind the account and they are interacting with you in an uncomfortable manner, do not hesitate to report and block them immediately. Removing their access minimizes the risk of being targeted by someone with malicious intent.

Suspicious accounts might attempt to gather personal information through messages, comments, or tags.

2 Limit public information

Avoid sharing sensitive personal information publicly (such as your home address, phone number, or routine activities) across any platforms. Before sharing photos, check that the image does not reveal identifiable locations or personal information. Background details such as house numbers, street signs, or landmarks can inadvertently share your location.

Strangers may use small clues in photos to track your location or personal details.

3 Review social media privacy settings

Set your profiles to private, and limit who can see your posts, photos, and updates – as well as who can contact you through direct messages, comment on your posts, or tag you in photos. Regularly review your privacy settings.

Only trusted individuals should have access to your online presence.

4 Be cautious when sharing your location on social media

Turn off location services on your social media platforms, and avoid sharing your real-time location online, whether through posts or automatic check-ins.

This helps prevent stalkers from tracking your whereabouts in real-time.

5 Use strong, unique passwords for every account

Generate unique passwords for each of your accounts using a password manager. Avoid reusing passwords across platforms.

Reusing passwords increases the risk of your accounts being compromised if a stalker gains access to one.

6 Be cautious when registering online:

Many websites require email sign-ups, which can increase your online visibility. Whenever possible, use a secondary email account specifically for public or less essential registrations, like e-commerce or fitness centers.

This approach limits access to your main email, keeping it safer from unknown senders or data leaks.

7 Enable Two-Factor Authentication (2FA)

Add an extra layer of security to your accounts by enabling 2FA, which requires a second form of verification (such as a code sent to your phone) before logging in.

This prevents unauthorized access even if someone has your password.

8 Lock down access to your devices with biometric security

Ensure your devices (phones, laptops) have strong lock screens, and set them to require a password or biometric verification (e.g., fingerprint, face ID).

This makes it harder for someone to access your device physically.

9 Use a VPN for online security

A Virtual Private Network (VPN) adds an extra layer of privacy by hiding your IP address, making it harder for stalkers to trace your online activity. It's especially important if you're using public Wi-Fi. Public Wi-Fi is often unsecured and a common target for hackers.

This ensures your location and browsing habits remain private.

10 Log out of your account after each use

Always log out of your account when you are done, especially on shared or public devices. Enable automatic logout features if available, as these log you out after a period of inactivity.

Staying logged into your account can make it easier for unauthorized people to access your data. Logging out adds an extra layer of protection against potential prying eyes.

11 Monitor your accounts for suspicious activity

Regularly check your email and social media for any unauthorized logins or suspicious activity.

Many platforms offer alerts if unusual login attempts are detected.

12 Regularly clean up your digital presence:

Conduct a "digital clean-up" monthly or quarterly to enhance security: reviewing and removing followers who seem suspicious, unsubscribing from unused online services, renewing passwords, deleting outdated or unused accounts, and performing an online search of your name to check what information is publicly available.

13 Avoid suspicious and phishing links

Avoid clicking on unsolicited links or downloading attachments from unknown senders, as they could be attempts to steal your data or compromise your security. Always verify the sender's email address carefully and report spam immediately to filter out future phishing attempts.

Stalkers may use phishing techniques to gain access to your personal information.

14 Use anti-stalking tools

Install security software that includes features to detect and prevent stalking, such as anti-spyware and anti-tracking tools.

Kaspersky's feature alerts you to apps that can secretly collect your personal data, and detects devices that may facilitate stalking via Bluetooth technology.

15 Be selective about what you store in the cloud

Avoid uploading highly sensitive or private information to cloud storage. Consider what data you store and whether it's absolutely necessary to keep it online.

The fewer sensitive files stored in the cloud, the less attractive your account will be to anyone trying to gain unauthorized access. Store extremely personal data offline on secure, encrypted local drives whenever possible.

Anna Larkina,
Privacy expert at Kaspersky