Online Safety Toolkit for Women

Internet Browsing

Always log out of shared devices

Delete browsing history regularly and check settings on Google Account.

Delete Cookies on websites so search history can be deleted. This should be prompted when deleting history.

Private/incognito browsing will mean there's no history of websites you have visited.

In your browser check what has access to your location, camera, microphone etc. Check what extensions are allowed as these can produce pop ups on your computer.

Connections and passwords

Never use your full name on Bluetooth connection.

Change passwords regularly. Use a mix of capitals, lower case, numbers and symbols for passwords. A combination of random non-associated words makes a stronger password.

Turn off location sharing on phones (and check children/dependent devices for settings)

Biometrics for phone or other devices – other people who have access to fingerprint feature on your device will also be able to access online banking if you have this active. For banking or sensitive apps, to turn off biometrics log in.

Messages and emails

If using an iPhone and deleting messages, you may need to delete twice. Open messages and click on edit in top left hand corner. Click on show recently deleted and delete messages from this folder too.

Always check that an email is from who you think it is by hovering over the sender's name and checking the email address is correct.

Safer Internet Day 2023 | UK Safer Internet Centre

BSWA Birmingham & Solihull Women's Aid

@bswaid **bswaid.org**

Registered charity number 1073926 Ryland House, 44-48 Bristol Street, Birmingham B5 7AA

Miscellaneous Tips

Use two factor authentication wherever possible, especially for emails, PayPal, banking. Set up these apps to send you a text code whenever anyone tries to log in to your account.

Family Link for Google offers stricter parental controls. If children want to download apps or games, the family link will send the parent a message and ask if they will allow or deny the other device (child's device) to download. You can limit screen time using this app too.

It is possible to request that Google removes personal information or contact details from online searches.

Keep neutral profile pictures even with private accounts as backgrounds can be identifiable. Better yet, don't use a picture of yourself for your account.

When sharing photos online, never share bank details, addresses and make sure photos don't accidentally show that information.

Tips from refuge.org.uk

Refuge have advice for lots of apps / devices to consider making secure as an abuser may use them to track you. For example JustEat has your address, Trainline saves your tickets in the app and much more.

Refuge also have an 'Interactive Home' tool where you can see how WiFi devices in the home may be being monitored and also how best to secure your WiFi.