GENERAL ONLINE SAFETY ADVICE

These tips address common concerns about staying safe while browsing online, especially when someone may be monitoring your activity.

General Security Tips

- Use a secure password to log into your computer. Avoid predictable ones (e.g., pet names, birthdays).
- Change your passwords regularly.
- Avoid saving passwords on shared or unsafe computers.
- If possible, use a different device entirely to browse safely.
- In Summary
- If you're in a situation where your online activity may be monitored:
- Be cautious when clearing history or cookies.
- Use Private Browsing when possible.
- Avoid using your personal device if it may be compromised.
- Use a public or trusted computer (library, friend, work) for safer browsing.
- Regularly change passwords and consider setting up a new, anonymous email account.

How Can Someone Track You Online?

- Spyware: Software can be installed (without your knowledge) on computers or phones to monitor your activity.
- Browsing history: Most browsers save a trail of visited sites, cached images, and search terms.
- Stored data: Passwords, cookies, and form entries can be used to access your accounts or identify your activity.

Deleting History or Cookies Can Raise Suspicion

Be cautious:

- Deleting cookies might remove saved login information (e.g. for online banking), which can alert someone monitoring the device.
- Clearing your browser history may also be noticeable.

Use Private Browsing (Incognito Mode)

Private or Incognito Browsing prevents most traces of your session from being saved, including:

- Browsing history
- Cookies and cached files
- Auto-complete data

PLEASE NOTE this mode does not make you invisible online.
It won't protect you from spyware or other monitoring software.
Always close the private window after use. Leaving it open can raise suspicion.

Stored Passwords

Browsers often ask to save your passwords. If this happens:
Click "No" when prompted to save a password.
Use Private Browsing to avoid saving passwords accidentally.
If needed, delete saved passwords via your browser's settings—but be aware that this might be noticed.

Toolbars & Search Histories

Search toolbars (like Google, Yahoo, or AOL) may save the words you type:
Look for options like "Clear Search History" in the toolbar settings.

Email Safety

- Threatening emails should be printed or saved as evidence.
- Sent, Draft, and Deleted folders can all contain messages you may not want someone else to see. Be sure to empty them.
- Even deleted emails must be removed from the Trash or Deleted Items folder to be fully erased.

If your current email account may be compromised:

- Create a new, anonymous account (e.g. bakedbeans123@example.com) using a provider like Gmail, Hotmail, or Yahoo.
- Access this account only from safe devices.
- Change your email passwords if you're at risk, as many accounts can be reset through email access.