Unexpected Electronic Gifts

How are they a security issue?

While receiving them in the mail may be exciting, unexpected gifts, **especially electronic devices**, can pose a significant security risk. Attackers may access personal data like **banking details, and account credentials** through them. In our advanced technological world, devices and apps connected to wireless networks and cell phones can quickly gather data through audio recordings and location tracking.

RECOMMENDATIONS:

- Regularly update devices and apps for the latest security patches.
- Educate yourself about fraud, brushing, and phishing.
- Report any unusual occurrences immediately.
- Be wary of apps that track your geolocation; they might leak your whereabouts.
- Beware! Random gifts of devices can signal counterintelligence or cyber threats.

WHAT TO DO

- Change passwords immediately if you suspect a data breach.
- Regularly monitor your bank transactions for unauthorized activities.
- Regularly backup important data in case of device loss or compromise.
- Use privacy settings on social media and online accounts to limit the information that's publicly accessible.

WHAT NOT TO DO

- Pay for any unwanted packages or for items they did not order.
- Keep personal and confidential information off non-work issued devices.
- Never use obvious passwords (common words, phrases, birthdays, etc.)
- Do not download apps from unofficial app stores.

A-SJ-007-000/DA-133 OPI: DGDS 2023/08