Safe Cyber Practices Guide in the workplace

#Be Aware.. To Be Safe

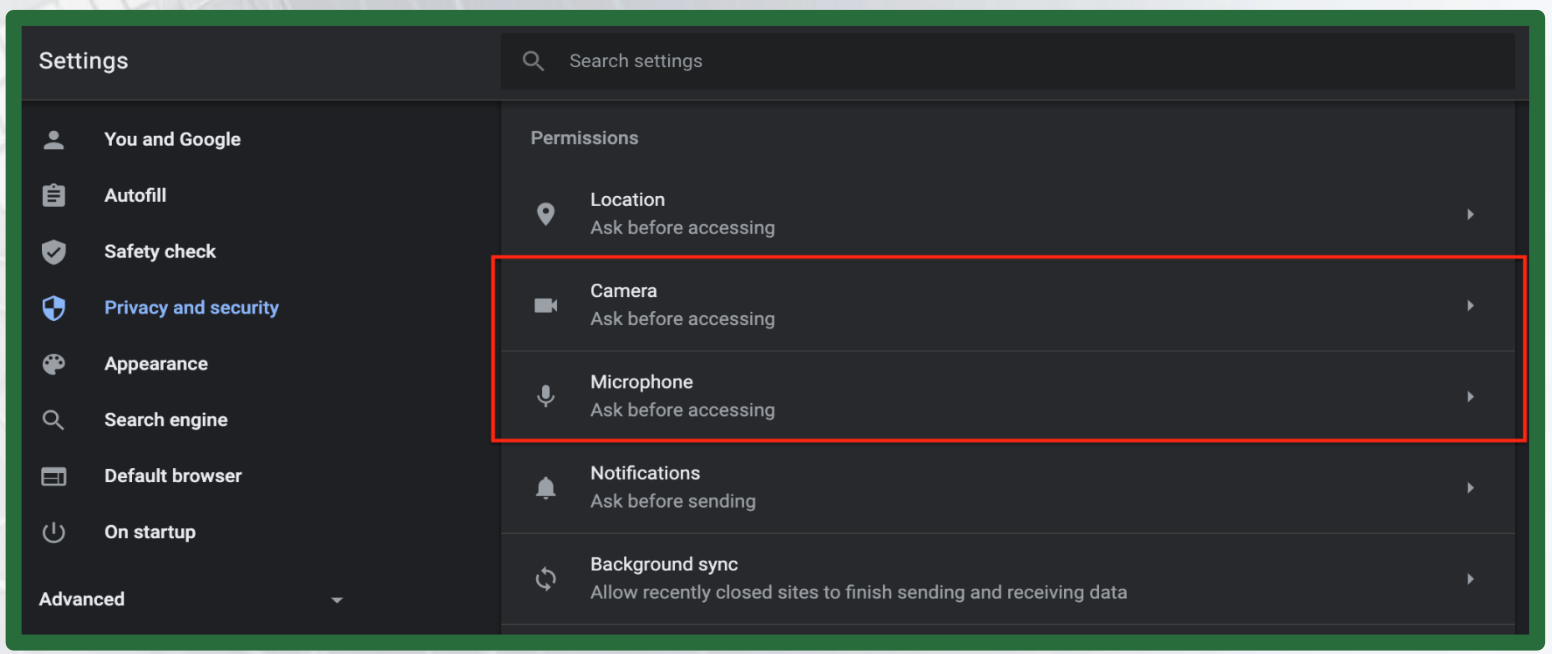
Cybersecurity@ibnsina.edu.sa

Topics

Secure Internet Browsing

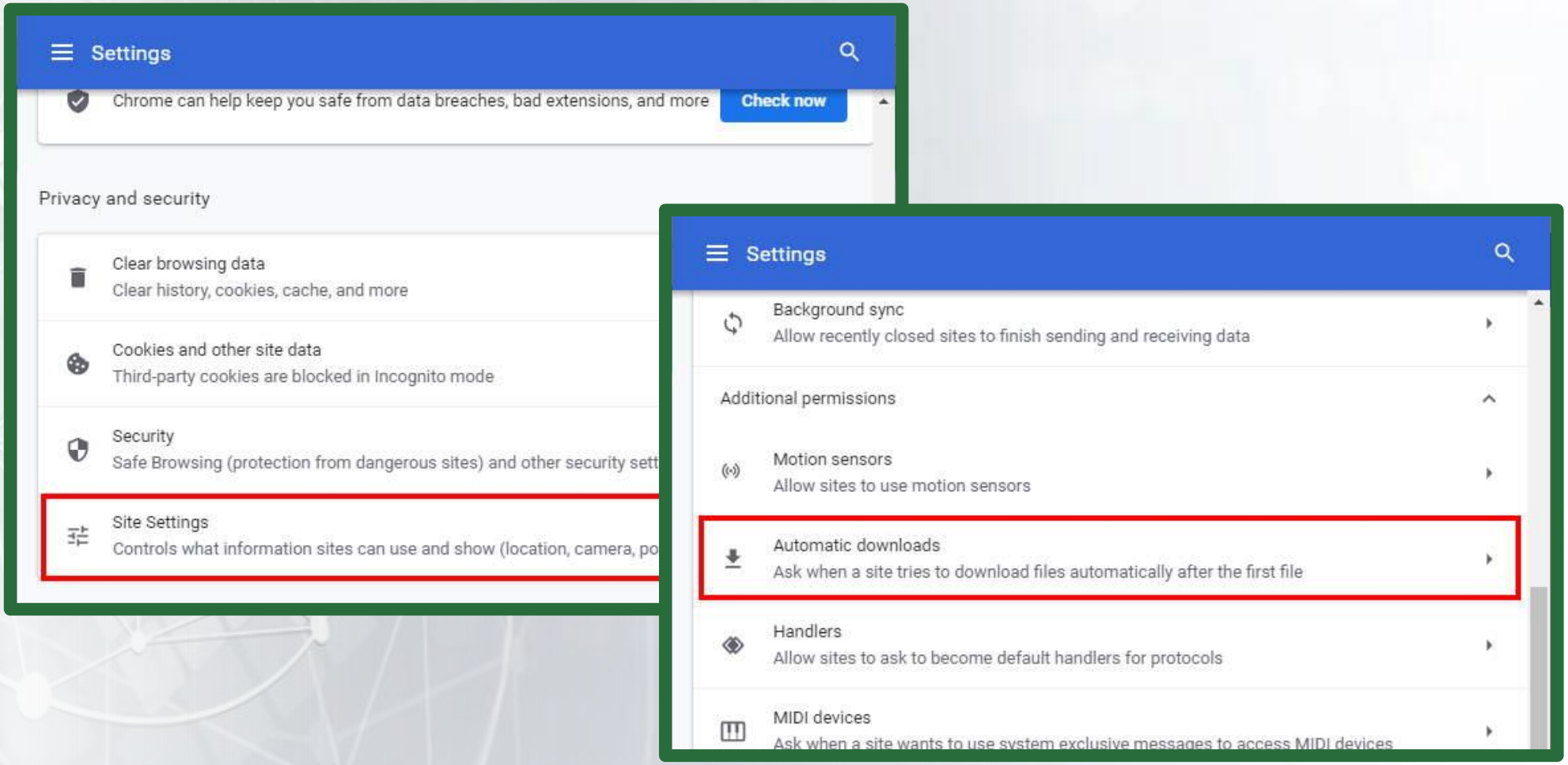
1- Avoid visiting suspicious websites and make sure that website's URL should begin with “https” rather than “http”.

2-Restrict access to geolocation, camera and microphone:



Secure Internet Browsing

3-Turn-off automatic downloads. Click on setting > then..



Secure Internet Browsing

4- Do not use the automatic login feature.

5- Periodically clear the history and cookies files from the browser.

6- Use the latest version of the Internet browser software.

7- Make sure to adjust the security and privacy settings for the Internet browser.

8- Block pop-up windows, as they may lead to malicious or hidden attacks.

Secure Handling of Email Services

especially phishing emails

What is phishing?

It is a dangerous and effective method for hacking operations. Criminals pretend to be known people and send targets messages containing a malicious link or attachment. The goal is for targets to click on the link, which may download malware or lead them to an untrusted site to steal their personal information.

Common signs of the phishing email:

- Unusual senders requesting your personal data.
- A simple change in the letter order of the address of a user you know.
- Spelling or grammatical errors.
- Unexpected email domains.
- Request an urgent response to sent or threatening content.

Secure Handling of email services

especially phishing emails

Ways to prevent phishing attacks:

- Avoid opening emails from untrusted sources.
- Check the sender before you click on any link or attachment.
- Check before responding to any messages asking for personal information.
- When you receive messages requesting to update your data, update it via only the official website, not via the attached link.
- Do not participate in promotions using your work email.
- If a suspicious message looks like it's coming from someone you know, contact that person via a different communication method, to make sure it's safe.
- Install all software and system updates on your device.

Secure Use of Social Media

- Use strong passwords for your social media accounts.
- Activate the two-factor verification feature on social media sites.
- Do not post sensitive information or employment information on social media sites.
- Do not use social media sites to exchange business documents or data.
- Avoid logging into social media sites using public devices or untrusted networks.
- Activate security questions, update them constantly, and store them in a safe place.
- Install security updates and fixes for social media apps from trusted sources as soon as they are released.

Remember, "What you post once on the Internet..
remains always on the Internet.."

Safe Handling of Mobile Devices and Storage Media

- Install security updates and fixe packages for operating systems, software, and applications only from trusted sources as soon as they are released.
- Create a complex password, and do not share it with anyone.
- Do not use external storage media on work devices.
- Do not connect any unsafe or unknown storage media to your device.
- Always make sure to check storage media of known origin before opening them.
- Delete temporary storage files “cookies” periodically.
- Make sure you have anti-virus software installed and activated on your device.