BGCC Wi-Fi Security Checklist

1. Change Default Settings

- Change the default SSID (Wi-Fi network name) to something non-identifiable.
- Change the default admin username and password for your router.

2. Use Strong Encryption

- Ensure Wi-Fi encryption is set to WPA3 (or WPA2 if WPA3 is not supported).
- Disable WEP or WPA - these are outdated and insecure.

3. Set a Strong Wi-Fi Password

- Use a complex password with at least 12 characters, including letters, numbers, and symbols.
- Do not reuse passwords from other accounts or services.

4. Secure Router Access

- Change the default IP address for the router if possible.
- Disable remote access unless absolutely necessary.
- Enable firewall features built into the router.
- Enable two-factor authentication (2FA) if supported.

5. Keep Firmware Up-to-Date

- Regularly check for and apply firmware updates from the router manufacturer.

6. Network Segmentation

- Create a separate guest network for visitors.
- Isolate IoT (smart home) devices on a separate VLAN or network.

7. Disable Unnecessary Features

- Disable WPS (Wi-Fi Protected Setup) to prevent brute-force attacks.
- Turn off UPnP (Universal Plug and Play) unless required.

8. Monitor Connected Devices

- Regularly review the list of connected devices.
- Block unknown or suspicious devices.

9. Use a VPN (Optional)

- Use a reputable VPN for enhanced privacy, especially on public or guest networks.

10. Educate Users

- Ensure everyone using the network understands safe Wi-Fi practices.
- Avoid connecting to unsecured public networks without protection.