Cybersecurity Cheat Sheet

1. Enable Two-Factor Authentication (2FA) on all online accounts

Enable 2FA wherever possible.

It adds an extra layer of security by requiring a second form of verification (e.g., a text message or authentication app) in addition to your password.

2. Stop using Passwords and use Strong Passphrases

Use passphrases instead of simple passwords.

Combine random words, numbers, and special characters.

Make them long and memorable (e.g., “PurpleUnicorn$42Rainbows!”).

Check out this website to help you with passphrases:

https://bitwarden.com/password-generator/

3. Use Password Vaults To Save Those Passwords

Use a password manager (vault) to securely store and manage your passwords.

Your favorite browser such as Chrome, Edge, Firefox, Safari, Brave and Opera allow you store your passworrds. Generate unique, complex passwords for each account and let the vault remember them.

4. Mobile Device Security

Don’t download strange apps from the Google Play and Apple App store

Configure auto-lock settings and use strong device passphrases and passkeys

Avoid leaving devices unattended in insecure locations.

Turn on “Find My Device”

5. Use Safe Wi-Fi Connections

Avoid accessing sensitive information over free public Wi-Fi.

Use your cellular data connection (mobile hotspot) when possible.

Be cautious when using public networks.

6. Data Encryption

Enable protection for your smart devices by using biometric thumbprint and facial recognition

If you’re a Windows user, use Bitlocker

If you’re a Macintosh use, use File Locker

Encrypt sensitive data (files, drives, emails).

7. Back that Thang Up.

Regularly back up your data to prevent loss.

Enable OneDrive, DropBox, Google Drive or iCloud Drive for Backups

You can also use Carbonite (www.carbonite.com) for backups

8. Social Media Caution

Limit oversharing on social media platforms.

Be aware that cybercriminals use personal information for social engineering.

9: Stop Sharing Your Mobile Number

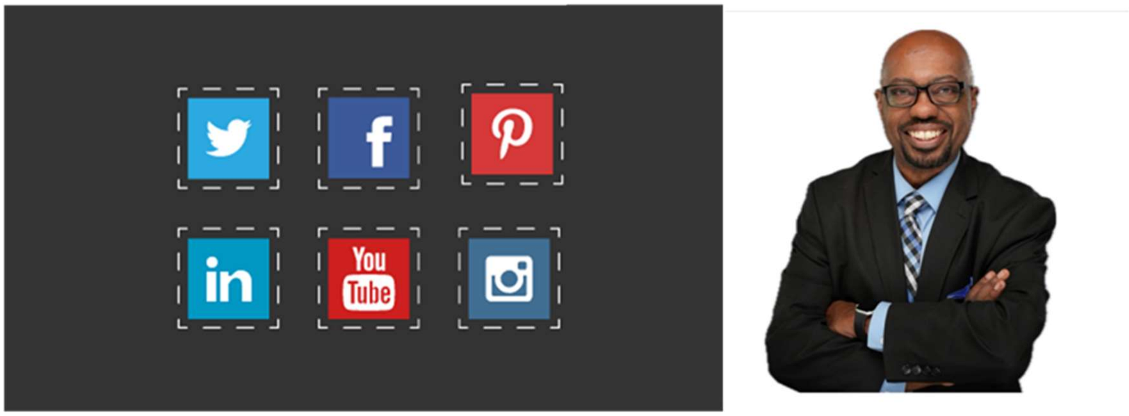
Be cautious about sharing your mobile number online.

Avoid posting it publicly or providing it to unknown sources.

Consider using Whatsapp, Google Voice, Vonage or Ring Central as your main business number.

We’re going to be **great friends**!

I love technology, I’ve read all the manuals and I’m serious about making technology fun, safe, exciting and useful for you!



Follow Me On Social Media @burtonkelso and at burton@burtonkelso.com