# SAFE INTERNET HYGIENE

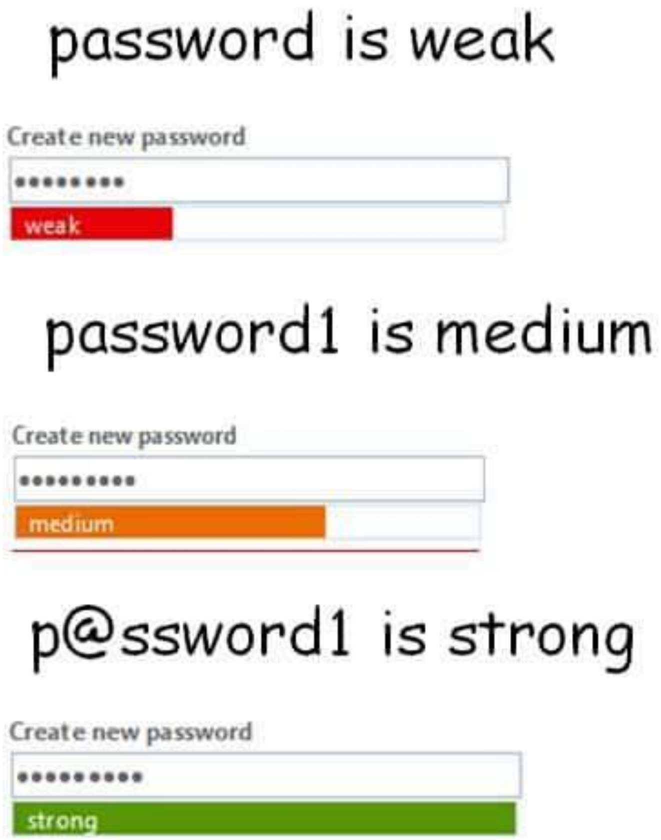
BY: CRYPTO SHERPA

# INTRODUCTION

- Welcome to the presentation on Safe Internet Hygiene
- The Internet has become an integral part of our lives, and it's essential to practice safe habits to protect ourselves and our personal information.

# STRONG PASSWORDS

- Use strong, unique passwords for every online account.
- Combine upper- and lower-case letters, numbers, and special characters.
- Avoid using easily guessable information like birthdates or names.
- Consider using a password manager to securely store and manage passwords.



password is weak

Create new password

••••••••

weak

password1 is medium

Create new password

•••••••••

medium

p@ssword1 is strong

Create new password

•••••••••

strong

# TWO-FACTOR AUTHENTICATION (2FA)

- Enable Two-Factor Authentication whenever possible.
- 2FA adds an extra layer of security by requiring a second form of verification (e.g., a code sent to your phone) along with your password.) along with your password

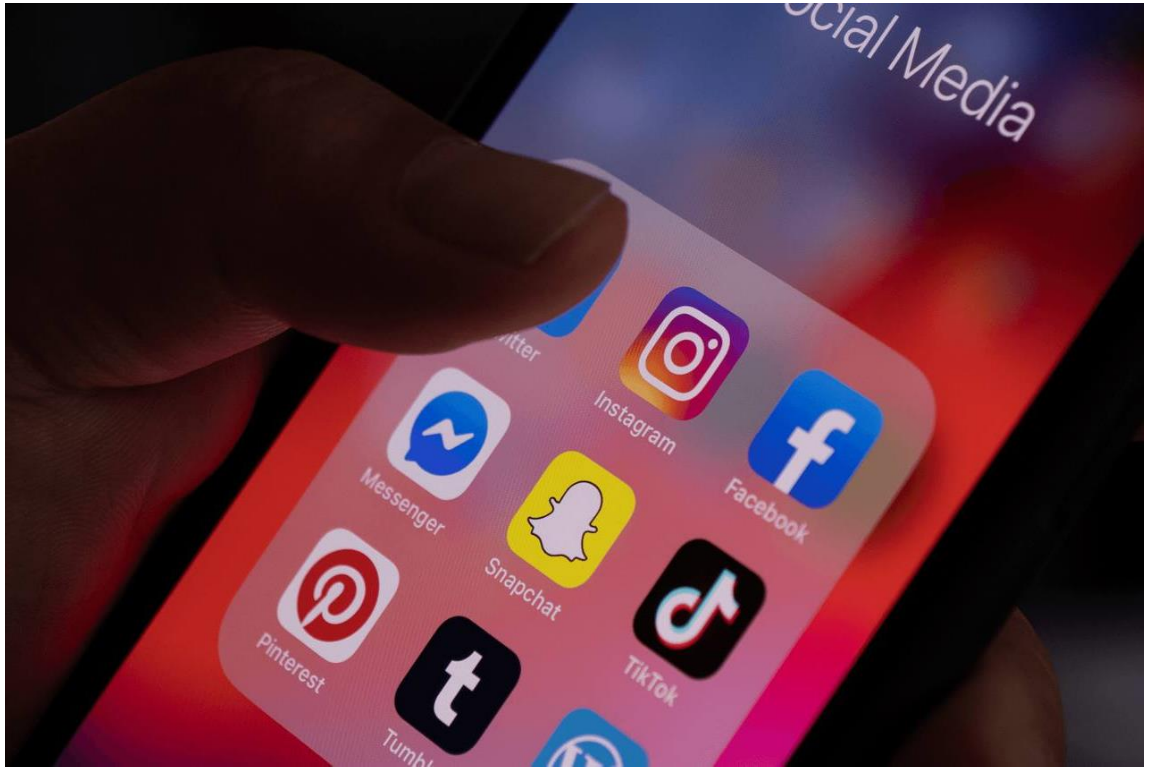
# PHISHING AWARENESS

- Be cautious of suspicious emails, messages, or links from unknown sources.
- Verify the sender's email address and check for grammatical errors.
- Never share personal information or login credentials through email or unfamiliar websites.

# SAFE BROWSING

- Use secure websites (look for https:// and a padlock icon in the address bar).
- Be cautious when clicking on links, especially from social media or unknown sources.
- Regularly update your browser to ensure the latest security features are enabled.

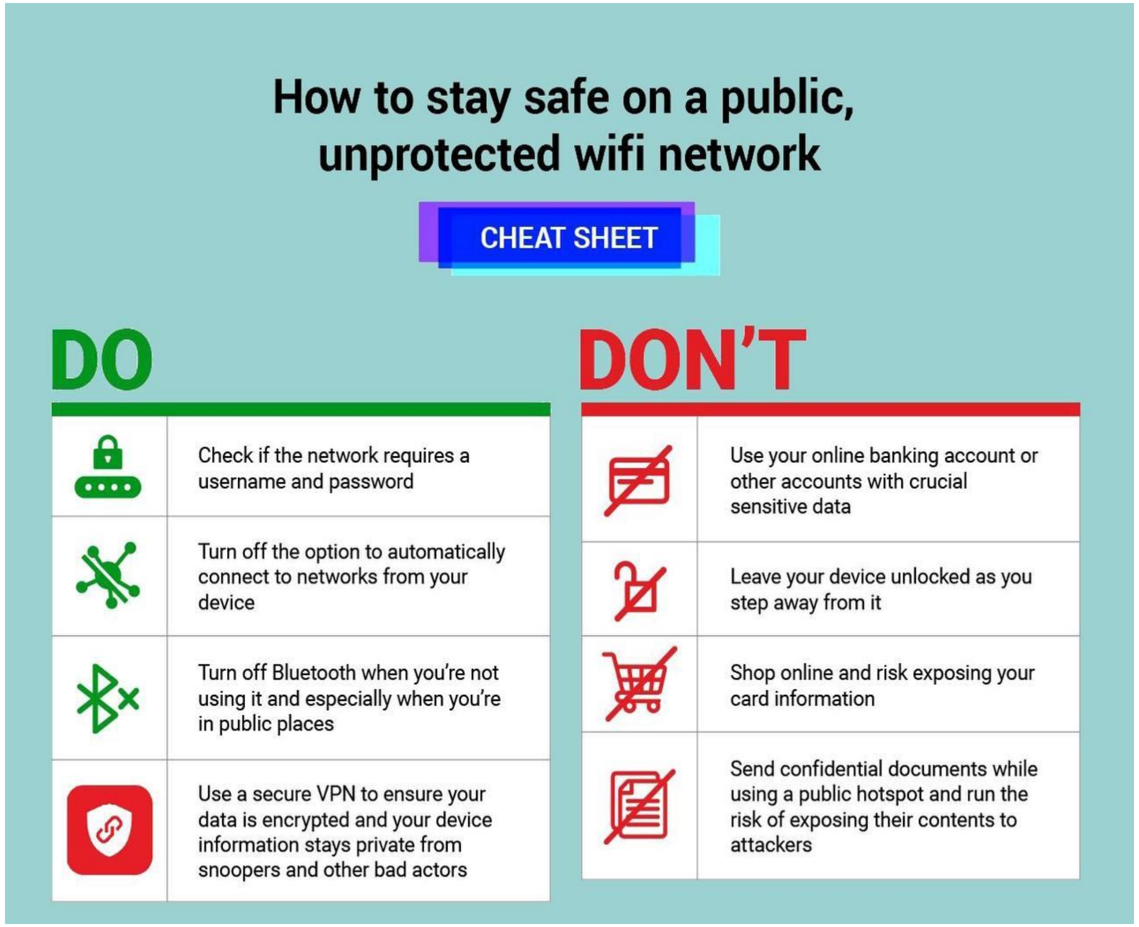
# SOCIAL MEDIA PRIVACY



- Review and adjust your privacy settings on social media platforms.
- Limit the amount of personal information visible to the public visible to the public
- Be cautious about accepting friend requests or messages from strangers.

# SECURE WI-FI USAGE

- Use password-protected Wi-Fi networks, preferably with WPA2 or WPA3 encryption.
- Avoid connecting to public Wi-Fi networks without using a Virtual Private Network (VPN).
- Turn off automatic Wi-Fi connections to unknown networks.



How to stay safe on a public, unprotected wifi network

CHEAT SHEET

| DO | DON'T |
|---|---|
| Check if the network requires a username and password | Use your online banking account or other accounts with crucial sensitive data |
| Turn off the option to automatically connect to networks from your device | Leave your device unlocked as you step away from it |
| Turn off Bluetooth when you're not using it and especially when you're in public places | Shop online and risk exposing your card information |
| Use a secure VPN to ensure your data is encrypted and your device information stays private from snoopers and other bad actors | Send confidential documents while using a public hotspot and run the risk of exposing their contents to attackers |

# REGULAR SOFTWARE UPDATE

Keep your operating system, antivirus, and applications up to date.

Updates often include security patches that protect against known vulnerabilities.

# DATA BACKUP

- Regularly back up your important files and data to a secure location.
- Consider using external hard drives, cloud storage, or both for redundancy.

# ONLINE SHOPPING SAFETY

- Shop from reputable websites with secure payment gateways (look for the padlock icon).
- Avoid making purchases on public computers or unsecured Wi-Fi networks.
- Check your financial statements regularly for any unauthorized transactions.

# PARENTAL CONTROLS

- Parents should set up parental contr on devices used by children.
- Monitor their online activities and educate them about safe internet practices.

# CONCLUSION

By practicing safe internet hygiene, you can protect yourself from cyber threats and ensure a safer online experience.

Be vigilant, stay informed, and share this knowledge with family and friends for a more secure digital world.

# THANK YOU