# Hackathon 1 - Stay Safe Online

## Hack Street Boys

## Possible categories / pages to cover

### First phase - Collection of all categories and information

1. Overview of online Safety, importance of staying safe online
2. Password security - Best practices for creating strong passwords, password managers, multi-factor authentication
3. Phishing and social engineering - How to recognise phishing/spam emails and messages, email security tips, common social engineering scam tactics, steps to take if you suspect a phishing/scam attempt, privacy settings on social media, safe social media practices
4. Data privacy - Understanding privacy settings on social media and other platforms. Importance of data encryption, GDPR and other data protection regulations, protecting personal information, sharing information online, understanding social media footprints (online presence and reputation), deleting old or inactive accounts
5. Secure browsing/communications - Using HTTPS and understanding the significance of secure websites, safe browsing habits, importance of keeping browsers and plugins updated, encrypted messaging apps, safe video conferencing practices, protecting your online communications, safe use of public WI-FI, using VPN's, safe practices on public networks
6. Device security - Best practices for securing mobile devices, laptops and desktops, the role of anti-virus and anti-malware software, importance of regular software updates and patches, recognising fraudulent applications, configuring devices securely.
7. Internet security for children - Safe browsing for kids, parental controls, educating children about online dangers, tools and strategies to help with that,
8. Online shopping and banking - Identifying secure e-commerce sites, safe online shopping tips, secure online banking practices, recognising fraudulent websites, recognising and avoiding common scams, using secure payment methods
9. Cyberbullying and harassment - Identifying cyberbullying, how to respond to harassment threats, resources for victims
10. Data breaches and identity theft - What to do if your data is breached, preventing identity theft, monitoring your credit and online accounts
11. Online safety tools and resources - Recommended software and tools, online safety organisations, helpful articles and guides
12. News and updates - Latest cyber threats, new security technologies, updates on privacy laws and regulations

13. Email - Secure email practices, protecting sensitive information in email
14. Legal and ethical aspects - Understanding legal implications of online activities, reporting and dealing with illegal online activities.
15. Data backup and recovery - Importance of regular backup, methods and tools for data backup, strategies for data recovery in case of loss or breach.
16. More information - External links
17. Credits (where content comes from etc. Maybe in the footer?)

## Second phase - Creation of viable categories for the hackathon

### Priority pages

1. Overview page - overview of online Safety, importance of staying safe online
2. Password security - Best practices for creating strong passwords, password managers, multi-factor authentication
3. Email & Social Media - How to recognise phishing/spam emails and messages, email security tips, common social engineering scam tactics, steps to take if you suspect a phishing/scam attempt, privacy settings on social media, safe social media practices, Understanding privacy settings on social media and other platforms. protecting personal information, sharing information online, understanding social media footprints (online presence and reputation)
4. Device Security - Best practices for securing mobile devices, laptops and desktops, the role of anti-virus and anti-malware software, importance of regular software updates and patches, recognising fraudulent applications, configuring devices securely.
5. Data breaches and identity theft - What to do if your data is breached, preventing identity theft, monitoring your credit and online accounts
6. More information - External links
7. Credits (where content comes from etc. Maybe in the footer?)

### Secondary pages (in order of importance)

1. Secure browsing/communications - Using HTTPS and understanding the significance of secure websites, safe browsing habits, encrypted messaging apps, safe video conferencing practices, protecting your online communications, safe use of public WI-FI, using VPN’s, safe practices on public networks
2. Internet security for children - Safe browsing for kids, parental controls, educating children about online dangers, tools and strategies to help with that,
3. Cyberbullying and harassment - Identifying cyberbullying, how to respond to harassment threats, resources for victims
4. Online shopping and banking - Identifying secure e-commerce sites, safe online shopping tips, secure online banking practices, recognising fraudulent websites, recognising and avoiding common scams, using secure payment methods

Third level pages (in order of importance)

1. Legal and ethical aspects - Understanding legal implications of online activities, reporting and dealing with illegal online activities.
2. Data backup and recovery - Importance of regular backup, methods and tools for data backup, strategies for data recovery in case of loss or breach.
3. Online safety tools and resources - Recommended software and tools, online safety organisations, helpful articles and guides
4. News and updates - Latest cyber threats, new security technologies, updates on privacy laws and regulations