"Navigating the Digital World: Unpacking Online Risks & Building Digital Resilience"

Hello Cambodia!

I am Ahmad Umair

I am from Malaysia and I'm here to contribute, connect, and inspire on the vast canvas of the Internet.

Here is my email: umairsuhaidi@gmail.com

TOPICS TO BE DISCUSSED TODAY

Make a big impact with our professional slides and charts

Topic 1: Protect Me From Myself

Discussion regarding privacy risks and simple steps to reduce digital footprint

Topic 2: The Dark Side of Connectedness (Cyberbully)

In this session, we will talk about the troubling cases of cyberbullying that have occurred worldwide. We'll have a poll where you can participate, and we'll also discuss the important work of organizations that are working to address cyberbullying.

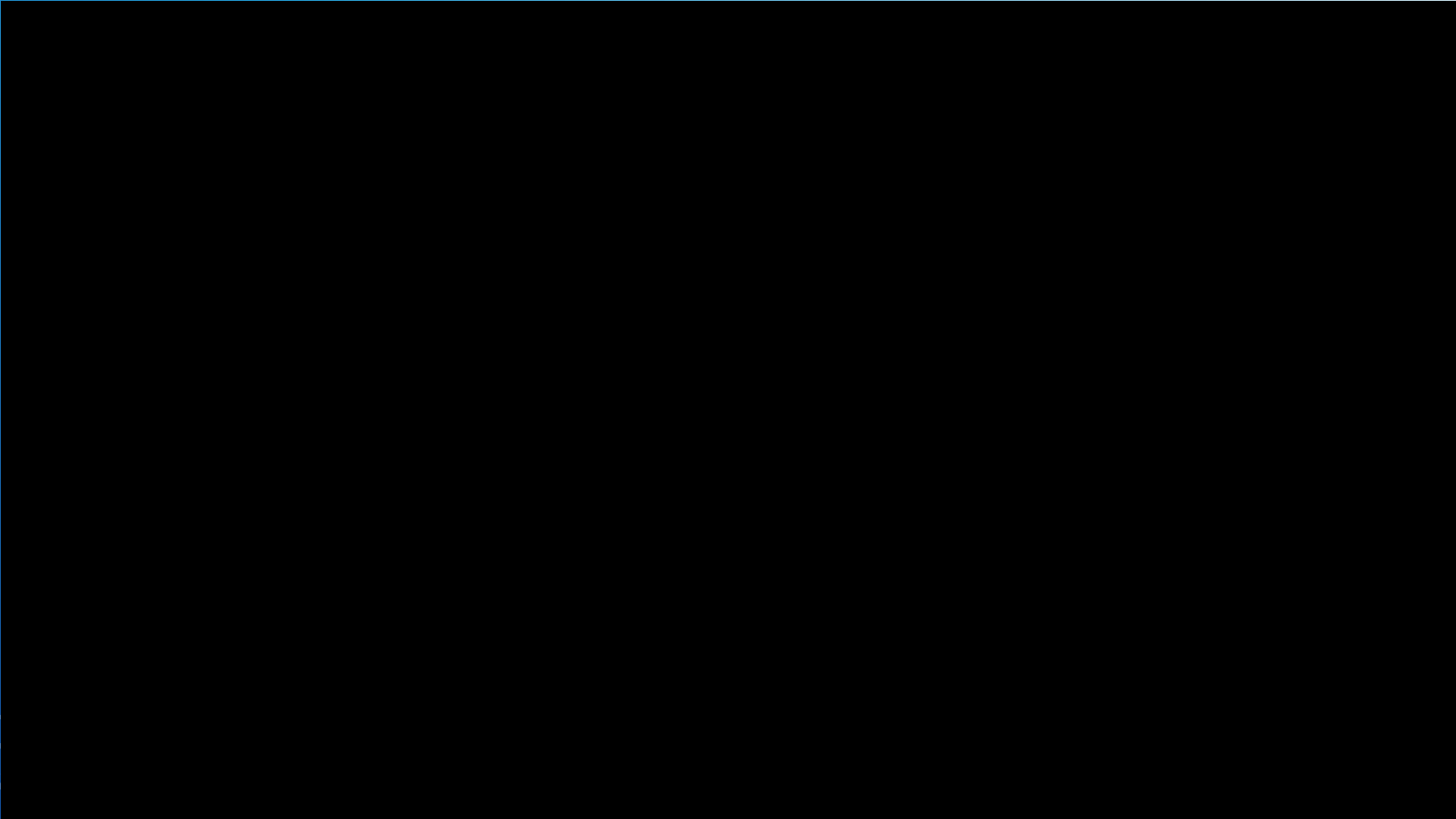## Topic 3: EXPLORING THE MYTHS AND TRUTHS OF THE INTERNET THE INTERNET

We're going to play an interesting and interactive game together to expose somemisunderstandings regarding the internet

TOPIC 1:

PROTECT ME FROM MYSELF

"

What do you understand from the video? Kindly share your thoughts in the chatbox!

From the video, we can conclude that:

- The amount of our digital footprints determine the level of our **privacy risk**

- Simple steps need to be taken for the sake of **reducing our digital footprints**

Understanding Terminology

Privacy Risk

Refers to the <u>potential threats</u> or dangers to an individual's personal information and privacy in the digital realm.

Digital Footprints

The <u>traces left behind by our online activities</u>, such as browsing history and social media interactions, which can reveal personal information.

PRIVACY RISKS CONSEQUENCE

Privacy risks can manifest in different ways, including:

REPUTATIONAL HARM

Privacy risks can **result in reputational harm** if personal information or embarrassing content is exposed to the public. This can lead to social stigma, discrimination, or **damage to personal and professional relationships**.

LOSS OF CONTROL

When personal information falls into the wrong hands, it can be accessed and **used for malicious purposes**, such as identity theft, financial fraud, or **impersonation**. Unauthorized access can occur through hacking, phishing, or other cyber-attack

Profiling and Targeted Advertising

Privacy risks can happen when your personal data is collected and used to create detailed profiles. These profiles can be used to show you specific ads, control your actions, or sway your choices.

HOW TO REDUCE DIGITAL FOOTPRINTS?

Here are some simple steps to reduce digital footprints:

Review and Adjust Privacy Settings

Check your privacy settings often on social media, online services, and devices. Keep personal info private and share posts and data only with trusted friends.

Be Cautious with Personal Information

Think before sharing personal info online. Don't post sensitive details like address, phone number, or finances publicly. Use fake names or alternate emails for non-essential services.

Minimize Data Sharing:

Be selective about the personal information you provide when signing up for websites, apps, or services. Avoid sharing unnecessary details and only provide information that is essential for the service or transaction.

Regularly Review App Permissions

Regularly check app permissions on your devices. Remove unnecessary permissions that access sensitive data or features not essential for the app's function.

What are the most effective privacy best practices?

"

In the digital age, it's important to protect your privacy. By being careful about what you share online and minimizing privacy risks, you can keep your personal information safe and stay in control of your online presence.

TOPIC 2:

The Dark Side of Connectedness (Cyberbully)

Disturbing Cyberbullying Cases Ever Documented

Three weeks before turning 14, American teen **Megan Taylor Meier** committed suicide by hanging herself. Her parents demanded an investigation, and it was determined that MySpace's social networking site was the source of her cyberbullying. This case was an early warning sign of the ill-effects of social media. (2006)

Phoebe Prince was a 15-year-old student who **tragically committed suicide** in 2010. She was relentlessly bullied by her peers, both in person and online, after starting at a new Massachusetts high school. The case gained significant media attention and sparked discussions about the devastating consequences of cyberbullying and the need for better anti-bullying measures.

Amanda Todd was a Canadian teenager who died by suicide in 2012 at the age of 15. She experienced severe cyberbullying, harassment, and blackmail. Her tragic story, shared in a YouTube video, brought attention to the harmful impacts of cyberbullying and the need for better support for young people facing such challenges.

14

Let's Answer a Poll!

Scan Here

OR

Search mentimeter.com
and insert this code:
5368 5309

Prominent Organization Addressing Cyberbully Issue Around the Globe

The Cybersmile Foundation
Global Oranization.

A global nonprofit organization dedicated to combating cyberbullying, offering support services, and promoting digital wellbeing

Bullying-Free New Zealand
New Zealand

A national organization focused on preventing bullying, including cyberbullying, through education, awareness campaigns, and support for schools and communities.sea

Protect & Save the Children
Malaysia

A Malaysian organization that addresses child protection issues, including cyberbullying, through awareness campaigns, advocacy, and support services for children and families.

Child Helpline Cambodia
Cambodia

Provides a helpline and support services for children, including addressing issues of cyberbullying and online safety. While not solely focused on cyberbullying, they play a significant role in supporting children facing online challenges.

16

"

In conclusion, cyberbullying serves as a stark reminder of the need for online responsibility. Each of us has the power to make a positive impact by treating others with kindness, empathy, and respect in the digital realm. Let us embrace the responsibility to create a safer and more compassionate online environment for all.

TOPIC 3:

EXPLORING THE MYTHS AND TRUTHS OF THE INTERNET THE INTERNET

Let's Play a Game!

Explanation Time!

Question 1: Is it possible to determine the authenticity of an email by checking the sender's display name?

Answer: (**Myth**) The display name in an email can be easily manipulated, so it is not a reliable indicator of authenticity. Always verify the email address itself to confirm its legitimacy.

Explanation Time!

Question 2: Can you protect your privacy online by adjusting your social media privacy settings?

Answer: (Truth) Adjusting your privacy settings can help improve your online privacy to an extent, but it doesn't guarantee complete protection. It's important to be cautious about the information you share and be aware of potential privacy risks

Explanation Time!

Question 3: It is safe to click on pop-up ads that claim you've won a prize or lottery.

Answer: (**Myth**) licking on such pop-up ads can lead to scams, malware, or phishing attempts. It's best to avoid clicking on them and close the pop-up windows.

Explanation Time!

Question 4: Does using a strong and unique password for each online account fully guarantee your security?

Answer: (**Myth**) While using strong and unique passwords is essential, it's not the sole factor in ensuring security. Additional measures like enabling two-factor authentication and being cautious of phishing attempts are also crucial.

Explanation Time!

Question 5: Can you identify a secure website by looking for a padlock symbol in the browser's address bar?

Answer: (**Partial Truth**) The padlock symbol indicates that the website uses HTTPS, which encrypts data transmission. However, it doesn't guarantee the website is completely trustworthy or free from other security vulnerabilities.

Explanation Time!

Question 6: Do antivirus programs provide 100% protection against all types of malware?

Answer: (**Myth**) While antivirus programs are important for detecting and preventing malware, they are not foolproof. New and evolving malware can sometimes bypass antivirus software, so it's essential to practice safe browsing habits.

Explanation Time!

Question 7: It is safe to install applications from third-party app stores outside of official sources?

Answer: (**Myth**) Third-party app stores can pose a higher risk as they may host malicious or modified apps. It is generally safer to stick to official app stores like Google Play Store or Apple App Store, as they have stricter security measures in place.

Want to make big impact to the Internet community? Join the upcoming Asia Pacific Internet Governance Academy (APIGA)!.

End of Presentation. Any Question?

Thank You for Having Me Cambodia!