Episode 5

"Media Literacy 101: Online media (bots, deep fake, shallow fake)

Opening music

HOST: Welcome back to "Media Literacy 101," the radio series that aims to educate and empower listeners to navigate the media landscape in a critical and informed way.

HOST: In today's episode, we will focus on digital literacy and online safety.

Soundbite 1: Understanding the Internet and How it Works

HOST: The internet is a global network of computers that allows people to share information and communicate with each other. It is a powerful tool that has changed the way we live and work. However, it is important to understand how the internet works and the potential risks associated with it.

Soundbite 2: Techniques used to Spread Disinformation

HOST: Disinformation is often spread through social media, where it can be amplified by bots and other automated accounts. It can also be spread through email, text message, forums, chatrooms, photos, videos and other forms of online communication.

Computer programmes known as AI or Artificial Intelligence with the ability to replace original videos, audio or photos, known as **deep fakes**, are becoming a cause for concern in the spread of disinformation and malinformation. You only have to check out the Instagram deepfake profiles of Tom Cruise and Keanu Reeves to see how convincing these are. These programmes can replicate actual people doing and saying things that they haven't actually done or said. If you are witnessing a politician doing and saying something on a video it is difficult to doubt its authenticity. This is where good old intuition and knowledge of a character becomes extremely important. We need to ask ourselves, is this something that aligns with what I know of this person?

Shallow Fakes are equally as disturbing but created by someone with basic video editing tools. An existing piece of media content can be completely altered and manipulated to present a different story or message. The goal of both deepfakes and shallowfakes are to twist reality and distort the facts.

Internet Bots are software applications that have been designed and programmed to complete repetitive tasks automatically and more quickly than humans and work 24/7. There are different types of bots, for example, Alexa and Siri are Chatbots that can simulate conversations. Social Media platforms have Social Bots that influence online discussions. If you're shopping online, Shopbots will help you find the best price for the product you're looking for. Spiders, also known as

Crawlers, find content for search engines like Google or Firefox. These are all known as good bots and can be used to replace humans in areas like customer service, business and entertainment. In fact, chatbots are now being utilised in the care of older adults to fight social isolation and assist in daily activities.

Bad bots are malicious bots used in cybercrimes and include ***Spambots*** which drive users to websites through pop up promotions and ***Hackers*** that can attack websites and gather personal and sensitive information.

Soundbite 3. How to identify malicious bots

There are a number of ways to know if your system has been infected.

- Internet connection runs slower than usual.
- The computer crashes without cause
- It might take longer than usual to shut down or reboot
- There are add ons in your browser that you didn't install.
- Pop up windows appear even when you are not using the internet
- You get warnings popping up to tell you to click on a link or your computer will be infected
- Your friends get emails or messages from you that you didn't send

Soundbite 4: Tips for Creating Strong Passwords and Protecting Your Online Privacy

HOST: Protecting your online privacy is important, especially as more and more of our personal information is shared online. We'll be looking in more detail in our next episode how to protect yourself online but here are some tips for creating strong passwords and protecting your online privacy:

- Use a mix of letters, numbers, and special characters in your passwords
- Avoid using easily guessable information such as your name or birthdate
- Be wary of public Wi-Fi networks
- Use privacy settings on social media accounts

Soundbite 5: How to Spot and Avoid Online Scams and Fraud

HOST: Online scams and fraud can take many forms, from phishing emails to fake websites. Here are some tips for spotting and avoiding online scams and fraud:

* Be skeptical of unsolicited emails and text messages

* Be wary of offers that seem too good to be true

* Do not provide personal information unless you are certain of the legitimacy of the request

* Check for spelling and grammar errors on websites or emails

* Use two-factor authentication when available

Soundbite 6: Guest Speaker

HOST: To explain more about what we've discussed today I'd like to welcome …….

HOST: Our next episode will focus further on ways to protect yourself from disinformation and manipulation on social media.

HOST: Be sure to tune in next week for the sixth episode of "Media Literacy 101." In the meantime, don't forget to check out our website for more information and resources on media literacy.

Closing music

HOST: Thank you for tuning in to "Media Literacy 101." Until next time, stay informed, stay curious, and stay media literate.

Outro music