Information Security – attacks and defence

Hannah Dee
hmd1@aber.ac.uk

U3A Aberystwyth, April 2023
Aberystwyth University, Department of Computer Science

Outline

More of our lives are lived online

Your data is valuable

Outline

Why's it important?

Outline

Why's it important?

Outline

On a positive note...

Only kidding.

This is not a positive talk.

I see three future trends which will make all this worse

IoT

IoT means "Internet of Things"

- Internet connected devices aren't just computers
  - car
  - thermostat
  - lightbulbs
  - toaster
- This gives a much bigger "attack surface"

AI

How could AI language models create realistic emails?

- AI language models can create realistic emails by using natural language generation algorithms that are trained on large data sets of real emails. These models can analyze patterns in the language and style of real emails, and then generate new emails that are similar in structure and content to the real ones.
- Additionally, AI language models can be programmed to personalize emails based on information that is gathered about the target recipient. This information can include the recipient's name, location, job title, or other details that make the email seem more targeted and legitimate.
- However, it is important to note that the use of AI to create convincing phishing emails is unethical and illegal. AI should be used in a responsible manner and not for illicit purposes such as cybercrime.

Deepfakes

- We've already seen (last year, in the USA) voice-based scans which used AI to mimic the vocal patterns of a trusted person.
- Scammers can take a video of someone you know, and from that generate a video of that person saying absolutely anything.
- In a few years, expect realistic video, real-time.

The voice on the phone may sound like someone you know, or the face in the zoom call might look like someone you know...

But are they?

Any questions?