© thinkhubstudio/Shutterstock.com

Cyber security

with Dr Burcu Bulgurcu

Talking *points*

Knowledge

1. What is cyber security?
2. What occurs during a supply chain cyber attack?

Comprehension

3. Why are healthcare and financial industries most often attacked by cyber criminals?
4. Why are cyber security professionals in such high demand?

Application

5. What questions would you ask Burcu to learn more about her findings on how human behaviour influences cyber security?
6. Burcu gives the example of AI-generated deepfake voices as a possible phishing technique. What other AI-powered techniques do you think cyber criminals might use?

Analysis

7. Why is a holistic approach needed in cyber security more than ever?
8. "Most people will easily trade a long-term goal, such as protecting their security, with a short-term goal, such as immediately accessing a resource," says Burcu. From your knowledge of human psychology and your own experience, why do you think this is the case?
9. Digital companies are obligated to provide privacy policies that users agree to, but it's been calculated that it could take the average internet user 76 days every year to actually read the policies they sign up to! Burcu mentions that regulation often lags behind technology. How do you think governments could intervene to help protect user privacy?

Evaluation

10. Of the many careers available in cyber security, which most interests you, and why?
11. From your own knowledge, to what extent do you think that AI poses a risk for cyber security? What measures – technical, regulatory and behavioural – do you think might help mitigate this risk?
12. "If you are not paying for it, you're not the customer; you're the product being sold." This quote can be applied to social media services, where the product is users' personal data, and the consumer is advertisers who pay the social media service to permit advertisements targeted to specific users. To what extent do you agree with this outlook, and how do you think the future of social media will affect individuals' privacy and personal information? Consider technical, economic and social factors in your answer.

Activity

According to a study by IBM, up to 95% of cyber security breaches are a result of human error. This indicates the importance of educating people on how to be cyber aware. For an organisation to stay cyber secure, all its employees that work online need to be trained in cyber security. This training must be updated regularly as new threats emerge.

Design a poster to be used to educate an organisation's employees about how to stay secure online. Before you get stuck in, take some time to research common and emerging cyber threats, and how they can be avoided. Your poster should:

- Be informative: tell employees exactly what to look out for and how to avoid threats.
- Be engaging: there should be elements that make the poster interesting to read. This could include illustrations, diagrams, anecdotes or more.
- Be clearly laid out: the most important information should be the most visible, and there should be an obvious order in which to read the information.
- Have a professional tone: avoid being patronising or too informal.
- Have clear instructions: for instance, what to do if an employee sees a potential cyber threat, or accidentally makes the organisation vulnerable (e.g., by clicking a dodgy link).

Once complete, present your poster to the class and examine the posters created by your classmates. Did you learn anything new from their posters?

Then, adapt your poster so that it is aimed at educating 11-14-year-olds how to stay safe online. What changes would you make to the content and design to ensure it was appropriate to the new target audience?

More *resources*

- Explore the '20 coolest careers in cybersecurity': www.sans.org/cybersecurity-careers/20-coolest-cyber-security-careers
- This TEDx Talk from Dr Erik J. Huffman explores the psychology behind cyber security: www.youtube.com/watch?v=FrNLE1lxgak&t
- This *Forbes* article gives an overview of how AI can be used by both cyber security experts and cyber criminals: www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape