

CYBERSECURITY AND SOCIAL PSYCHOLOGY WITH DR JASON HONG AND DR LAURA DABBISH

TALKING POINTS

KNOWLEDGE

1. What is social proof?
2. What are social norms?

COMPREHENSION

3. Why is cybersecurity important?
4. Why is social psychology an important consideration within cybersecurity?
5. Why do people tend to follow social norms?

APPLICATION

6. How would you design a study to investigate how successful the 'Hacked Time' game is at changing users' security behaviour? How would you analyse how to improve the game further?
7. What extra risks to cybersecurity do you think are arising with the development of the Internet of Things?

ANALYSIS

8. Jason and Laura's Facebook research showed that while more socially-influenced people were likely to investigate extra security settings, they were not any more likely to adopt them after investigation. Why do you think this might be? What further research does this warrant?
9. What are some positive and negative social norms in the digital space you can think of? Have you seen any of these change or develop in recent years?

EVALUATION

10. Consider your own motivations for using or not using cybersecurity measures. What do you think would persuade you to change your habits? Do you think the same applies to people in other social groups – for instance, older people or people in a different country?
11. There are growing levels of public mistrust in social media companies. Do you think this influences levels of cybersecurity or the effectiveness of company-led security awareness campaigns? How?

MORE RESOURCES

- You can learn more about Jason and Laura's research at: www.socialcybersecurity.org
- Jason recommends this video of Robert Cialdini talking about 'The 6 principles of Influence': www.youtube.com/watch?v=eCNeOga965U
- The Human Computer-Interaction Institute where Jason and Laura work host seminars throughout the year that can be viewed online: www.hcii.cmu.edu/seminar-series
- This article from *The Psychologist* shows how hackers are using social psychology to compromise people's cybersecurity and the social motivations behind hackers themselves: thepsychologist.bps.org.uk/volume-29/september/social-psychology-cybersecurity
- This video from TEDx gives a rundown of the development of social norms: www.youtube.com/watch?v=oqkzp9C2Vyl

ACTIVITIES YOU CAN DO AT HOME OR IN THE CLASSROOM

Choose a social media platform that you are familiar with, such as Instagram or TikTok. Consider:

- What are your own levels of cybersecurity on this platform?
- What do you think are the levels of cybersecurity of those you interact with on the platform, such as friends and influencers?
- Have you seen any cybersecurity campaigns on the app?
- Have you seen any instances of the negative effects of lower cybersecurity, such as people getting hacked or having their identity stolen?
- What positive and negative 'trends' have you seen on the platform?

Now, imagine you are designing a campaign for the social media platform to use to persuade users to increase their levels of cybersecurity. Draw on the lessons learned from Jason and Laura's work with Facebook. Use the internet to research:

- Existing levels of cybersecurity on your chosen platform
- Successes and failures of past cybersecurity campaigns
- Scientific research into social proof and social norms in the digital space.

When designing the campaign, consider:

- Do you have a particular 'target audience' in mind within the platform users?
- How will you incorporate social psychology into your campaign?
- How will you track what aspects of the campaign are most or least successful?
- How can you avoid unwanted outcomes (e.g. people stopping using the platform)?
- How can you make the campaign visually engaging?

When you have finished, present your campaign to your peers, who take on the role of the social media company you are pitching to. What questions and comments do they have? Reverse the roles and assess the campaigns your peers have put together.