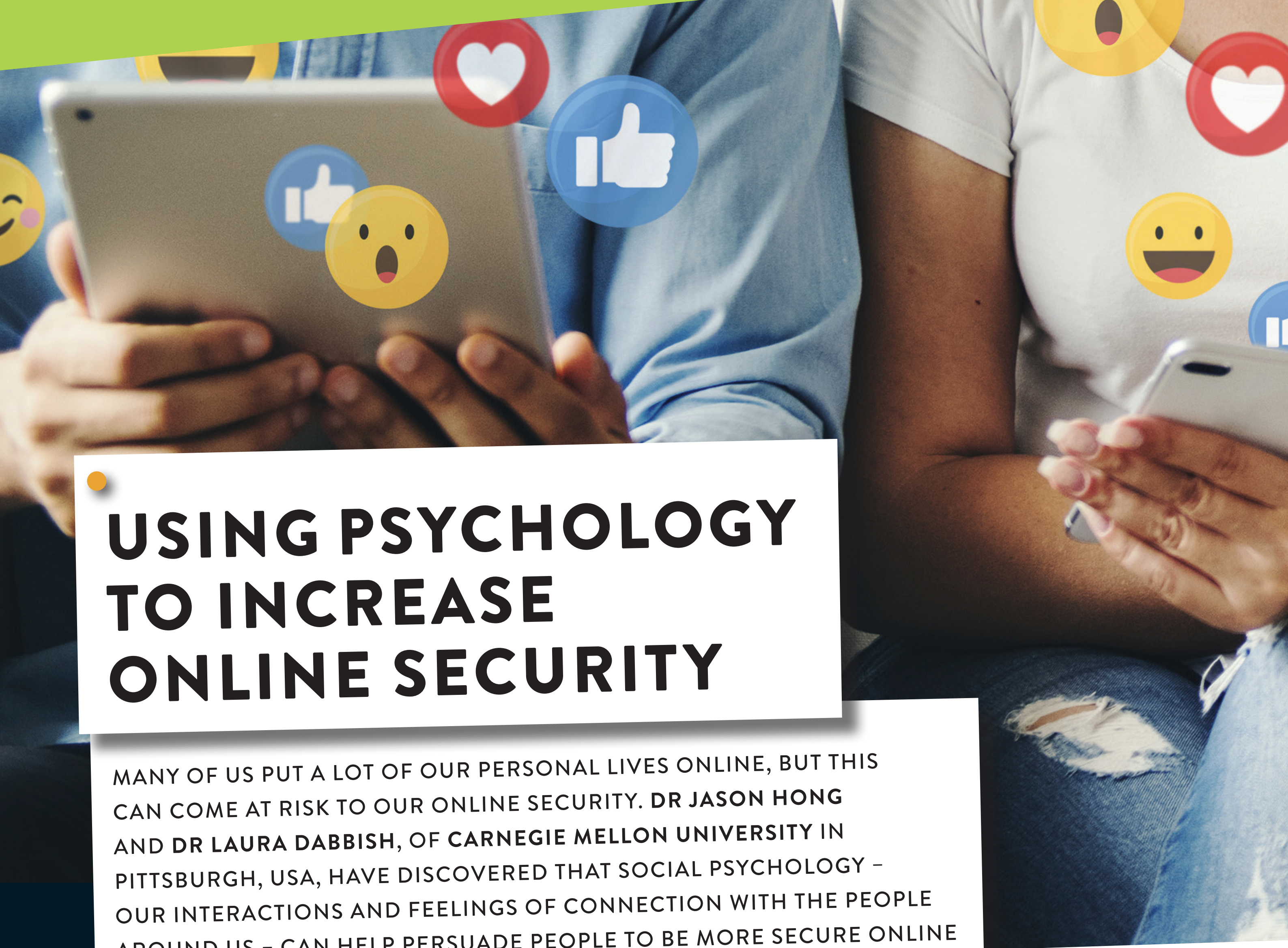

USING PSYCHOLOGY TO INCREASE ONLINE SECURITY

MANY OF US PUT A LOT OF OUR PERSONAL LIVES ONLINE, BUT THIS CAN COME AT RISK TO OUR ONLINE SECURITY. **DR JASON HONG** AND **DR LAURA DABBISH**, OF **CARNEGIE MELLON UNIVERSITY** IN PITTSBURGH, USA, HAVE DISCOVERED THAT SOCIAL PSYCHOLOGY – OUR INTERACTIONS AND FEELINGS OF CONNECTION WITH THE PEOPLE AROUND US – CAN HELP PERSUADE PEOPLE TO BE MORE SECURE ONLINE

GLOSSARY

CYBERSECURITY – protection against criminal or malicious use of electronic data

PHISHING – a form of cyber scamming using a fraudulent message to trick someone into revealing personal information

SOCIAL NORMS – 'typical' behaviours of a particular social group, which can be used as reference points for members of the group to guide their individual behaviour

SOCIAL PROOF – a psychological phenomenon where people tend to copy the actions of others because of a desire to fit in with the group or because they assume others know something they do not

SOCIAL PSYCHOLOGY – the branch of psychology that covers the origins and influences of social interactions

Cybersecurity has come a long way in recent decades, but threats to our digital resources – such as viruses, scams and identity frauds – have also developed rapidly. Though there are lots of steps that can be taken to increase cybersecurity, many people choose not to take them. Understanding why this is, and how to change this behaviour, is essential for helping people avoid online dangers.

Dr Jason Hong and Dr Laura Dabbish are both experts in cybersecurity at Carnegie Mellon University in Pittsburgh. Rather than focusing on just providing ways to increase cybersecurity, they aim to find lessons from how people interact with the digital world and with each other. "Our research into the human factors of cybersecurity focuses on people as social actors whose security behaviours are influenced by their relationships, communities and life situations," says Jason.

WHY SOCIAL PSYCHOLOGY IS IMPORTANT

For many years, there has been a preconception among computer scientists that if security tools exist, people will use them. Jason recounts his 'lightbulb moment' when he realised the real picture is more complex. "I overheard a conversation where one person mentioned a mutual friend who had slipped on some ice and broken their laptop," he says. "The other person said they were going to back up their own data immediately, and they did!" This was a clear example of where social influence led to a behaviour change in the digital space.

Laura explains more about why social psychology is so important. "Humans are social creatures," she says. "We look for cues on how to behave from those around us, especially those we feel close to." This applies to a huge amount of our behaviour: what we buy, how we vote and how we treat others, for example. How we manage our online security and privacy is no exception. "We look at others' social media to see what's appropriate to share, we discuss with our friends and family when we hear about data breaches to figure out how to respond," says Laura. "We share anecdotes about our own online experiences and listen to those of others."

SOCIAL PROOFS AND SOCIAL NORMS

The concept of 'social proof' is well-documented in social psychology. "If you've ever alighted from a bus or train and don't know which way to go, following everyone else is generally a pretty good strategy," says Jason.

The same concept applies in a less practical but equally important sense, through our desire to fit in through following social norms. "Social norms are mutually understood acceptable behaviours within a social group," says Laura. "They may not ever be discussed, but still drive our behaviour. For instance, cutting a queue would be a clear violation of a social norm."

Social norms can be good and bad behaviours. For instance, if you see lots of people littering or buying the latest fast fashion, you might be inclined to replicate that behaviour. "In terms of cybersecurity, if everyone in a social group is sharing lots of personal information online, there is social pressure to do the same," says Laura. "This can put people at risk of issues like identity theft or sharing photos or posts they later regret." People who take extra security precautions may violate this social norm and be labelled as paranoid or overly cautious. Jason and Laura are interested in leveraging social proof to make security precautions more accepted and adopted.

RESEARCH WITH FACEBOOK

Jason and Laura and their PhD student Sauvik Das worked with Facebook, the social media company, to investigate ways to help its users be more secure online, beginning with a large study with 50,000 people. "Facebook was about to run an awareness campaign by posting messages on people's feeds saying, 'Facebook offers extra security settings to help you protect yourself' or similar," says Jason. "We modified the messages to say things like, '108 of your friends use extra security settings'."

The Facebook study showed the importance of adapting messaging to use social proof as an effective persuasion tactic. "We found that simply showing people how many of their friends used security features drove 37% more viewers to explore the promoted security features compared to simply raising awareness through a non-social announcement," says Laura. Their research showed a clear role for social aspects within awareness campaigns, though some knowledge gaps remain to be investigated.

FROM SURVEYS TO GAMES AND BEYOND

Laura and Jason have run surveys and interviews to investigate people's attitudes to security and how they manage security and privacy in different relationships. "We found that a majority of changes to people's approaches to cybersecurity were triggered by social interactions," says Jason. "This included being warned about insecure behaviour by a friend or family, being shown an interesting new security technique by a colleague or friend, or hearing about someone's negative experience, such as being hacked." The team followed up with a larger survey that found social triggers were the most common prompts for recent adoption of new security behaviours.

Learning from their insights, Laura and Jason, along with PhD student Tianying Chen, led the development of a game called 'Hacked Time', which involves the player going back in time to help a friend correct insecure behaviour and avoid getting hacked. "We found this game was effective at increasing self-efficacy for security techniques and for increasing cybersecurity awareness," says Laura. "We are interested in learning more about how incorporating social influences into game design can motivate safer cybersecurity behaviour."

DR JASON HONG

DR LAURA DABBISH

Human Computer Interaction Institute, School of Computer Science, Carnegie Mellon University, Pittsburgh, USA

FIELD OF RESEARCH

Social Cybersecurity

RESEARCH PROJECT

Taking lessons from social psychology to encourage people to exhibit safer and more secure behaviour in digital spaces

FUNDER

National Science Foundation (NSF)

This work was supported by the National Science Foundation under grant numbers 1704087 and 1347186. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Jason and Laura plan on taking their research further, to use social psychology in more sophisticated ways to persuade people to be more secure online. "Google gave a presentation a few years ago that showed that less than 10% of people use two-factor authentication, a powerful security technique," says Jason. "As risks to people's security grow and evolve, we want to find out how to persuade people to better protect themselves."

ABOUT CYBERSECURITY

WHAT DO JASON AND LAURA FIND REWARDING ABOUT RESEARCH IN THEIR FIELD?

"In many areas of science, there is often a large gap between one's research and seeing a positive impact on people," says Jason. "Computer science is different, partly because we set our own rules rather than using the rules of nature, and partly because it's a younger field. It's often surprising how much influence a small team of researchers can have on industry and public policy."

"I love the interdisciplinary nature of the work," says Laura. "Our department combines insights from computer scientists, psychologists and designers, and this helps us take a much broader approach to the role of technology in people's lives. The collaboration this involves is extremely rewarding and I enjoy learning from my colleagues, while contributing my own perspective."

WHAT TYPES OF COLLABORATION DOES THEIR RESEARCH INVOLVE?

"We have assembled teams of developers, artists, designers and social scientists, which come together with a common purpose to move a research prototype towards eventually reaching the public," says Laura. "For instance, for developing 'Hacked Time' we drew on the expertise of a game design faculty, who pulled together software developers, artists and narrative designers."

WHAT ISSUES WILL FACE THE NEXT GENERATION OF CYBERSECURITY RESEARCHERS?

"The biggest problem faced by cybersecurity is that old problems aren't going away, while new problems are always developing," says Jason. "Weak passwords were a problem forty years ago and are still a problem today, for instance. Now, we have new challenges, such as security for the emerging Internet of Things – where billions of small computers sense and control parts of the physical world, including everything from traffic lights to central heating. Another example is cryptocurrency, which has some positive uses, but also has major problems in terms of theft and use of ransomware."

WHAT SKILLS ARE USEFUL FOR A CAREER IN CYBERSECURITY?

"It's useful to have a solid technical base," says Jason. "This doesn't just apply for programmers, but for anyone interacting with cyber systems. At the moment, there are many people working on the legalities or policy surrounding cybersecurity that barely understand how computers work. It's important to understand the terminology and how these systems work, the trade-offs involved, and what is possible or not. I would also encourage insight into what it means to be human, which is best achieved through an interest in the humanities and arts. Cybersecurity is, ultimately, a human problem, given it involves understanding why people may or may not adopt security measures."

WHAT SHOULD SOMEONE CONSIDERING A CAREER IN CYBERSECURITY KNOW?

"A common misconception people have about cybersecurity is that it's all technical work focused on the computer," says Jason. "In reality, it's far more varied. There are lawyers working on issues of compliance, policymakers working on nationwide goals for cybersecurity, economists investigating trade-offs of different policies, and psychologists working on how to motivate people to be more secure."

EXPLORE A CAREER IN CYBERSECURITY

- Jason and Laura's university runs a summer research experience for US undergraduates, where students contribute to cutting-edge research into human-computer interactions: **www.hcii.cmu.edu/summer-research-program**

- Cybersecurity careers are growing in the UK, too. This webpage explains more about how to get into the field, emphasising the importance of both technical and non-technical expertise: **www.prospects.ac.uk/jobs-and-work-experience/job-sectors/information-technology/cyber-security-training**

PATHWAY FROM SCHOOL TO STUDYING CYBERSECURITY

- As Jason and Laura emphasise, cybersecurity involves people from a diverse array of educational backgrounds. Degrees in subjects like computer science may provide the most direct pathway, but degrees in other subjects such as psychology or law could also lead to a career in cybersecurity.

- Jason recommends technical subjects to ensure a sound understanding of computer science. This includes subjects like computer science, mathematics and physics. He also emphasises the importance of understanding human interactions with technology – this could be achieved through subjects such as psychology, history or art.

JASON AND LAURA'S TOP TIP

Experiment with possible careers through personal projects and self-directed learning. There are so many great online resources available, and don't be afraid to reach out to experts or people you admire in the field. Seek out opportunities for early research experiences if that interests you.

HOW DID JASON BECOME AN EXPERT IN CYBERSECURITY?

As a youngster, I was very lucky to have parents who let me do pretty much whatever I wanted! I was very into comic books, science and building LEGO models. I have a rather active imagination as a result.

I fell into research by accident. In my second year at college, a professor asked me if I wanted to help out with some research that summer, and, since I didn't have any other plans, I signed up. It was a really fun experience, imagining and building new things that had never been done before. I was very lucky to be admitted to the computer science PhD programme at University of California at Berkeley, where I loved thinking about big ideas and their potential. I felt that research was a way I could use my skills to make a positive difference for humanity.

I am able to connect ideas from different fields in new ways to solve problems. I've drawn on ideas from machine learning, social psychology, gaming, visual design and more. I'm also good at recovering from setbacks – though I've had many successes in my life, I've had far more failures. The important thing is to figure out how to improve and keep pushing forward.

I have two young children who help me switch off from my work. We've been building a lot of LEGO and even practising piano together. During the pandemic, I started playing video games with them too, which I think are great, but only in moderation.

I helped found Wombat Security Technologies, which used our research to protect people from phishing scams. When it was sold in 2018, we used some of the proceeds to found a scholarship and two junior faculty chairs. I've always felt it is important to give the people who come after you better opportunities than you had.

HOW DID LAURA BECOME AN EXPERT IN CYBERSECURITY?

I was introduced to computers at a young age through computer games. My father was an electrical engineer and sparked my interest in computation and technology. My mother taught me to appreciate the humanities through art and music.

I attended a state-funded specialist maths and science high school, which gave me my first opportunity to participate in research. For one day a week, I got to work with researchers to find new ways to evaluate certain chemical properties of cosmetic products without having to test them on animals or people. I learned that research was something I enjoyed and that it could involve not just studying something, but also innovating and creating new tools and techniques.

I'm curious about the world, about human nature and how things work. This curiosity helps drive me to better understand the human experience with technology. Empathy is also useful – my work involves bridging disciplines, so it's important to understand the varying perspectives on the same problem.

I find daily walks restorative and a way to decompress from work. Research shows that being in nature, even for short periods of time, improves well-being. I also enjoy running in all seasons.

Mentoring is one of the most enjoyable aspects of my work, and I'm always proud to see my students go off to productive and fulfilling careers. I've mentored undergraduate students in research projects, and they've later gone on to do PhDs, move into industry, or start their own companies.