HOW TO BEAT THE CYBERCRIMINALS AND STAY SAFE ONLINE

AS WE BECOME INCREASINGLY RELIANT ON OUR ELECTRONIC DEVICES, IT IS BECOMING MORE IMPORTANT THAN EVER TO BE CYBER SECURITY AWARE. **PROFESSOR SHUJUN LI** AND **DR JASON NURSE** OF THE **KENT INTERDISCIPLINARY RESEARCH CENTRE IN CYBER SECURITY (KIRCCS), UNIVERSITY OF KENT,** TALK ABOUT SOME OF THE CHALLENGES IN CYBER SECURITY AND WHAT WE CAN ALL DO TO OVERCOME THEM

According to a report by Statista, Facebook had 2.45 billion monthly active users as of the third quarter of 2019. That is a tremendous amount of information being shared on a regular basis, and many of us share posts without giving much thought to the risks attached to doing so. The risk of identity fraud is ever-increasing, because the more people publicly post online (on social media channels or forums, etc.), the more they open themselves to risks.

Sharing too much information online can enable cybercriminals to collect personal information and impersonate you across other websites or services. This is known as identity fraud. In this way, the offenders use information to hack into your online accounts, or even sign up for credit cards in your name. It is therefore essential that we all take steps to protect our personal information online.

The University of Kent is home to the Kent Interdisciplinary Research Centre in Cyber Security (KirCCS), which aims to harness "expertise across the University of Kent to address current and future cyber security challenges". Cyber security researchers Professor Shujun Li and Dr Jason Nurse are part of the team at KirCCS and are passionate about improving cyber security awareness and education.

WHAT ARE SOME OF THE CURRENT CHALLENGES KIRCCS IS TRYING TO ADDRESS?

KirCCS deals with a whole range of research topics. Some are highly technical (for example, security testing and verification), others can be described as socio-technical, i.e., studying user behaviour, trust in online social networks or privacy management.

Shujun is the Socio-technical Theme Lead at KirCCS. One challenge, he says, is understanding how to engage everyone – end users like you, system designers, developers and managers, among other people – in the whole cyber ecosystem so that we all play our part. And measuring the effectiveness of cyber security awareness and educational activities is a key part of this challenge. "There is a general lack of reliable metrics to evaluate the performance of cyber security awareness campaigns," says Shujun, "More research in this space is therefore needed."

Another challenge is how to incentivise people and organisations to care about cyber security and take necessary actions. These actions do not only require technical solutions but also new policies and regulations, such as enforcing high security standards and rewarding vendors who provide secure products and services.

WHICH RISKS POSE THE GREATEST THREAT?

Online sexual abuse of children, including child pornography, has been one of the most highlighted crimes in recent years. Cyber harassment (or cyber bullying) is another one. While such crimes are undertaken over the internet, the harm they cause to victims is very real, and in many cases lead to lifelong mental health problems or even suicide. Clearly, safety

PROFESSOR SHUJUN LI

Director of Kent Interdisciplinary Research Centre in Cyber Security (KirCCS) and Professor of Cyber Security at the School of Computing, University of Kent.

DR JASON NURSE

Director of Public Engagement at KirCCS and Lecturer in Cyber Security at the School of Computing, University of Kent.

FIELD OF RESEARCH

Cyber Security

RESEARCH PROJECT

The strategic objective of KirCCS is to promote wide-ranging multidisciplinary research, and to teach and develop skills in cyber security to its students and the wider community, through degree programmes, workshops, visits, outreach days, lectures and training.

THERE ARE A RANGE OF THINGS YOUNG PEOPLE CAN – AND SHOULD – DO TO KEEP THEMSELVES SAFE ONLINE:

- Set up strong passwords on all devices and services you use. These include smartphones, laptops, desktop computers, as well as online social media accounts such as those on TikTok, Snapchat and Instagram.
- Ensure you have good privacy settings. Think carefully about who can see your posts on social media or online forums.
- Remember to install the latest updates on your systems and devices – updates help keep your devices (and therefore you) secure from cyber threats. One useful method of ensuring your devices are always up to date is to turn on automating updating options.
- Be constantly vigilant about the threat of online sexual abuse or cyber harassment. If you are ever suspicious about someone you are talking to, raise the alarm and seek advice from adults you trust.

measures need to evolve constantly to protect people at risk of online sexual abuse and cyber harassment.

WHY DO YOUNG PEOPLE NEED TO BE AWARE OF THESE RISKS? DON'T UK ORGANISATIONS AND THE GOVERNMENT HAVE YOUNG PEOPLE'S SAFETY AT HEART?

For online sexual abuse of children, children and young people are targeted by criminals who know how to exploit those who are vulnerable. For cyberbullying, anyone can be a victim, but children and young people are particularly at risk. As the children's charity NSPCC says, "Any child can be bullied for any reason. If a child is seen as different in some way or seen as an easy target, they can be more at risk."

This means that everyone needs to play their part in keeping the society secure. The government and organisations have systems, platforms and services in place to protect young people, but they also need everyone's help to make things work more effectively – this means you, your parents, carers, school staff and anyone else who works with young people. We are all part of the solution. And if you're really serious about helping people keep safe online, you could become a cyber security expert like Shujun and Jason!

ABOUT CYBER SECURITY

Cyber security is hard to define because there are so many variables. Just think of all the technologies, devices, systems, data, programs and processes that are involved in cyber security. Now think about the human input and the involvement of cyber bullies, terrorists and paedophiles mentioned in the article. And what about individuals such as you? According to Techradar, 90% of security incidents involved "human errors". If you imagine all of these variables together, how would you define cyber security? You might have a good idea of what cyber security is but others may define it differently to you.

HOW AWARE IS THE UK PUBLIC OF CYBER SECURITY?

"Overall, cyber security awareness in the UK is good, but it can always be improved," says Jason. "The challenge is that cybercriminals are constantly creating new scams, tricks and cyber-attacks." So, what does this mean? It means that everyone has to be on their guard, regularly update their devices, products and software, and keep an eye out for new guidelines on how to keep safe online.

There have been many campaigns in the UK designed to improve awareness, which have had a positive impact on UK society as a whole. However, as Shujun mentioned, it is difficult to know how effective these awareness campaigns are; for example, are young people more or less cyber security aware than adults? We cannot know for certain, but institutions like KirCCS are helping to spread the message of the importance of cyber security to young people. Young people, in general, are more knowledgeable about computers and pay more attention to new technologies than their parents.

WHAT ARE SOME OF THE MAIN CYBER SECURITY RISKS TO YOUNG PEOPLE IN THE UK?

"One significant risk is that of the oversharing of personal information online; the fact is that cybercriminals often monitor what people are saying on social media to gather information for their attacks," says Jason. These attacks may come in the form of targeted scams, phishing emails, identity fraud or cyber harassment.

Shujun adds that another significant risk is young people's exposure to criminals who are experienced in targeting children and young people. "These criminals might be paedophiles trying to exploit children or terrorists trying to recruit young people to their radical ways of thinking."

WHY SHOULD YOU CONSIDER A CAREER IN CYBER SECURITY?

It is an area that is exciting and there is a constant need for more people with a variety of skills. Every day at work is different and there are new challenges all the time. Perhaps most importantly, anybody who works in cyber security has the opportunity to protect people and invent new technologies. You are not just addressing computing concerns – you are potentially saving lives! Cyber security challenges come in many forms, as Shujun and Jason explain:

Artificial Intelligence (AI) and Cyber Security: The recent rise of deep learning and other AI technologies has led to new challenges around how to secure AI algorithms and protect users' privacy against unethical, irresponsible, insecure and privacy-intrusive AI algorithms.

Human Factors of Cyber Security: Humans are a core part of modern systems and it is increasingly important that we understand how to engage users with security. This means that we need to better understand how humans perceive cyber security in systems, the challenges they face in making "good" security decisions, and the various ways that cyber criminals may attempt to compromise how individuals think about security for their own benefit. This domain requires focus on psychology, human computer interaction, and sociology amongst other topics.

Cyber Security Governance: At an international level, there are huge governance gaps and inconsistencies caused by missing and conflicting laws and regulations covering cyber security, data protection, privacy, cybercrime and digital forensics. The potential of cyber conflict and cyber war between some states, the sharp rise of nationalism and right-wing movements in several key states, and cyber activities of terrorist groups have been making the cyber security governance landscape even more complicated.

Blockchains and Cryptocurrencies: As one of the most disrupting and controversial areas in cyber security, blockchains and cryptocurrencies have a unique characteristic of being intrinsically interdisciplinary, involving sciences, engineering, social sciences and humanities. The use of virtual cryptocurrencies as a way of incentivising human participation and the built-in anonymity has been making a huge (positive and negative) impact in many areas.

Quantum Cyber Security: Quantum computers are closer to becoming a reality and in 20 years' time we will need completely different cyber security theories and tools to keep us secure.

OPPORTUNITIES IN CYBER SECURITY

- Although studying a cyber security-related degree at university will enhance your skills and knowledge, you do not need to have a degree to work in cyber security. It really depends on which role you are interested in performing within the field of cyber security. The Learn How To Become website has loads of information about careers in cyber security.
- KirCCS holds public engagement events throughout the year, including workshops and summer schools: https://cyber.kent.ac.uk/events.html. It is worth checking whether the university or college near you holds similar events.
- The demand for skilled cyber security professionals combined with a scarcity in talent supply has resulted in high wages and excellent benefits for qualified applicants. Depending on the role, employees can expect anywhere between £60,000 (IT security consultant) and £100,000 (chief information security officer).

ASK PROF SHUJUN LI AND DR JASON NURSE

WHAT DID YOU IMAGINE YOURSELF DOING WHEN YOU WERE YOUNGER?

JN: I always imagined I would work with technology in some way, but I never really considered the thought of working in cyber security (or computer security, as it was called back then!).

SL: I enjoyed reading scientific magazines that were aimed at young people when I was a kid, although I liked reading about history, too. I have always had an interest in science fiction and, while I was interested in science and technology from an early age, I had never given much thought to anything related to cyber security. My real interest in the field started when I was around 24.

HAVE YOU ALWAYS BEEN INTERESTED IN COMPUTERS?

JN: Yes – I have always been fascinated by how computers and technology work. I think the desire to understand more – particularly to the point where I could start creating things such as applications, is what inspired me to get into computing.

SL: Not really. My early exposure to science and engineering was more in physics, chemistry, mathematics, biology and geography (in China this subject included geology and cosmology as well). I never really encountered computer science or electronic engineering before I started my undergraduate study in 1993, since when I began working with computers and it quickly grabbed my attention and fascination.

WHICH SUBJECTS DID YOU TAKE AT SCHOOL/COLLEGE?

JN: The subjects I studied included mathematics, IT, business, accounting, chemistry, biology and history.

SL: In middle school in China, my main subjects included mathematics, physics, chemistry, biology, geography, Chinese, English, history, politics, PE, music and arts.

DO YOU PLAY COMPUTER GAMES AT HOME? WHAT ELSE DO YOU DO TO RELAX?

JN: Yes, I tend to play the occasional computer and video games. I especially like car racing games! I also like to do puzzles and play chess.

SL: Yes, of course. Playing games is part of modern life. I used to be a big fan of Chinese role-playing games when I was studying at university.

SHUJUN AND JASON'S TOP TIPS

1 – Take every opportunity you get to learn about technology – the way it works and how it is used.

2 – There are many ways to get into computing and cyber security. There is no pre-defined path that you absolutely have to take. These topics have traditionally been very technical but there is an increasingly important social side (e.g., psychology and sociology), which focuses on the interactions between humans and computers. Ultimately, this should open the subject to people with broader interests than simply computing.

3 – In the field of cyber security, you can choose to be an "eagle" (who is good at looking at things from a broad perspective) or a "frog" (who is good at looking at things at a deeper level). Which one is most suitable for you depends on many factors, but you should be able to pick up some clues as you study at school. In general, it is important to try to be an "eagle" when you are younger and eventually switching to becoming a "frog" as your interests become more specific. However, keep in mind that it is also possible to be a mix of both!

Researchers often do talks to help the public understand their research. In this photo, Shujun speaks about his research on cognitive modelling for studying human behaviours in cyber security.

Jason discusses cyber security with local businesses.