Cyber safety and security - ‘Show Me the Money’

A report by John Armstrong, Vice President U3A Network Queensland

A symposium held during Seniors Month discussed the rapid increase in cyber attacks on individuals and organisations in recent times. Sponsored by nbn™, the Seniors Online Safety & Cyber Security Symposium brought together seniors network groups and community group leaders to discuss how to empower our seniors in online safety and cyber security.

Cyber safety relates to what people are doing online, their behaviour and actions, while cyber security relates to protecting devices and networks from intrusion.

‘Cyber = Money’ was the key message of the panel members at the symposium, and that the present has never been more important for networked groups to develop relevant programs to inform and educate seniors about safe online connections.

Keynote speaker, Samantha Isaacs of ASCCA said that seniors are being targeted increasingly. “It’s not just a lack of confidence in using computers amongst some seniors, it’s the access seniors have to cash such as in retirement funds, so the motivation is there to concentrate on seniors as a prime target for increasingly sophisticated scams,” Ms Isaacs said.

“I work in the cyber security field and I don’t always know what to look out for, as the operators are becoming more skilled and more devious in establishing a convincing argument to respond to their requests for your money. It’s important to have the confidence to recognise when you are being scammed and to adopt a healthy suspicion of such online approaches.

“A contributing issue is that these days we are almost forced to do things online, as more and more government and other organisations require applications and other forms to be completed online. This in effect produces more susceptible groups of people who may not be confident in their online practices, even have a reluctance to go online at all.”

Dr Ewan Ward, Director of the Joint Cyber Security Centre Queensland, said that the cyber threat environment is only getting worse, with a 300 per cent increase in call volume on their 1300CYBER1 hotline in the past 12 months.

“The cyber criminals are becoming more adept at getting at your money through tactics such as Ransomware on computers and networks and other scams,” he said.

“They don’t care who you are, they just want you to pay.”

Included on the Centre’s website at cyber.gov.au is ‘How to Use the Internet Securely: A Guide for Seniors' where there is a wealth of information about cyber and how to be online securely.

IDCARE's Head of Identity Security Operations, Moises Sanabria, provided an insight into the psychology and sophisticated tactics that have made scammers so successful in Australia. “Our data collected over several years shows that seniors are not necessarily more susceptible to being scammed; nevertheless, seniors are a high value target for scammers. The top three factors are: that this cohort have the highest percentage of telephone land lines, which is a point of entry for scammers and it’s not even humans on the end of the line, it’s a BOT (short for robot) that places the calls; also, many seniors have outdated devices with old or ineffective security patches, and criminals are expert at exploiting this vulnerability; they also respect authorities and big brand companies, so that if an email comes from a bank or a telco, with appropriate branding and knowledge of the individual’s details, then it may be considered as real.

"But the biggest problem in falling for a scam is plausibility, it's the plausible approach employed, and Australia has been bombarded with 55 million scam calls in the past year. They use local numbers, purchased as a bundle, to give confidence that it's a local call. And the main reason to target Australians is that we have the most resilient economy and one of the highest earnings per capita. Seniors are a particular target because they want to create a better nest-egg for their children, and the money that is leaving Australia to scammers is in the billions of dollars per year.

"Scammers also have incredible ability to tap into the flight-or-fight response that individuals have, and you can impair the rational part of your brain in this pressure situation. Criminals are incredibly adept at making people excited or scared, and when they get you into this state of confusion they can convince you to hand over money. People who speak to us afterwards say, 'I felt like I was in a trance, or hypnotised', and if someone says 'hang up, that's a scam' that's when they snap out of it.

"People who say 'I'll never be scammed' devalue the ability of the scammers who do this over and over again to perfect the tactics and psychology of the situation - and technology helps them do this by creating this point of entry that enables them to control the emotion of the contact.

"Spoofing (disguising a communication from an unknown source as being from a known, trusted source) is another successful tactic of sophisticated scammers: saying they can prove via displaying a trusted phone number or email address that they are legitimate, so unfortunately technology is one step ahead for scammers in lowering natural suspicion and emotional defences."

"Flubot is another technology on Android devices that sends a text message, ostensibly from a trusted source such as a bank or government department, asking the receiver to click a link to retrieve a document, and in the process gaining access to the device."

In countering cyber security threats, government agencies need the help of seniors organisations. Dr Ward said that cyber security agencies need organisations to communicate to their members the dangers and pitfalls of poor online practices and to be aware constantly of the cyber threat that is constant.

"You are the trusted conduits to people in your organisation so it's really important that you communicate the threat as widely as possible and provide the linkages to agencies such as ours about cyber activities."

Typical security practices related to devices would include: using a password manager, and long passwords with letters, numbers and symbols are less likely to be compromised; using multi-factor authentication whereby a user has to provide at least two forms of identification; and turning on automatic updates for computer software that ensures the software has the latest security prevention elements.

The significant increase in telephone calls and text messages from scammers creates a person-to-person interaction, which boosts the success rate of these scammers, and this requires similar personal support to counter this threat. There has been a 30 per cent increase in these approaches in the past year.

The old adage that 'if it seems too good to be true, or too bad to be true' - an unexpected parcel delivery, a huge discount deal, a cash refund, turning off your phone or internet, or the like - then in all probability it is a scam. All reputable organisations will not ask for money or credit card details over the phone, and if they do it needs to be regarded with great suspicion.

The panel agreed that the objective in countering the scammers was to empower people to go online, with the awareness and the knowledge of the tactics used by scammers.