ThinkUKnow e-Newsletter - June 2016

Tech talk
With the end of financial year approaching, we've decided to focus this month's 'tech talk' on email scams.
We've teamed up with our program partners at Microsoft to provide you with information on how to avoid becoming a victim, and ways to start the conversation with young people on how to protect their personal and financial information.
This time of year sees many of us scrambling to collect group certificates, receipts, and seeking professional help in gaining the most out of our returns.
Unfortunately, this time of year also creates an opportunity for scammers to take advantage. They pretend to be 'tax experts', 'accountants' and sometimes even pose as the Australian Taxation Office (ATO).
Scammers may also attempt to contact you directly via email which may look legitimate, however there are some tell-tale signs to look out for that can keep your computer and private information safe.

What is phishing?
Phishing emails are designed to steal money by installing malicious software on your computer to collect personal information from within your computer and websites you have visited. Scammers sometimes use social engineering to convince you to install malicious software or hand over your personal information under false pretences.

What does a typical phishing email message look like?

1. Spelling and bad grammar. Scammers are not always known for their writing skills.

Time2Talk

Although not all our young ones are working and lodging tax returns, this time of year provides a great opportunity to discuss the implications of opening emails from unknown senders or clicking on suspicious links. Here are some ways to start the conversation:

1. Would you offer your personal information to a stranger?

2. Consider the list of people and organisations you feel comfortable sharing personal information with. Such as your name, address, birth date and bank details. Are these good choices?

3. What should you do if you receive an email from someone you don't know?

4. What filtering software can you use to limit unwanted contact?
And remember, if something seems too good to be true, it probably is!

A common scam around this time of year is one claiming to have uncovered money owing to you from previous tax periods. To obtain the "refund" you might be asked to provide details such as name, email address, date of birth and banking details. If you receive this type of email, our advice is do not open it or click on any links and

Professional companies and organisations usually have editors that will not allow a mass email to go out with basic grammar and spelling errors. If you notice mistakes in an email purporting to be from a usually reputable organisation, it is likely a scam.

2. Beware of links in emails. Avoid clicking links in email messages. Try hovering your mouse (but don't click!) on the link to see if the address that appears matches the link typed in the message. A seemingly innocent link can be a scam.

3. Spoofing popular websites or companies. Scammers use graphics in emails that appear to be connected to legitimate websites but actually take you to scam sites or legitimate-looking pop-up windows. Never click on links associated with these sites.

delete the email immediately.

If in doubt about the authenticity of any communication you receive from the ATO check with them directly by calling 1800 008 540.

What should I do if I suspect I am the victim of a scam?

• If you believe you are a victim and have lost money as a result of phishing activities, contact your financial institution immediately.
• Scams or phishing emails can be reported to the Australian Cybercrime Online Reporting Network https://www.acorn.gov.au/

For more information visit:
• https://www.scamwatch.gov.au/
• www.acorn.gov.au
• https://www.ato.gov.au/general/online-services/in-detail/online-security/how-to-verify-or-report-a-scam/