byfields
business advisers

SCAMMERS DO NOT HIBERNATE

Mike Cornforth | IT Manager

Nearing EOFY, businesses, farmers and individuals are scurrying around to close off as many jobs as possible. With this, it's easy to take your eye off the ball when it comes to IT security, and the scammers know this.

At the time of writing this piece, one of our newest and youngest staff members in the Perth office came to me after coming across an email which we are commonly receiving. Notwithstanding our strong spam filters, this one made it through. It was addressed from one of our regional Directors and read...

> **I'm supposed to give you a call on this, but I'm currently occupied at the moment and can't make or receive any calls. I need you to get something done right now, I need some Google Play gift cards to be sent to a recipient. Do you have an idea of the nearest store you can get them from? Let me know if this can be done, so I'll get back to you with details.**

Fortunately, the suspicious nature was noticed in the domain name the email was sent from, the subject line, and the suspicious request details. This example shows we as accountants are not immune to some phishing.

According to an ACCC report, Australians lost $851mn in scams (2020), mainly surrounding investment, romance, and payment redirection spoofs. Companies exposed were Telstra, NBN, Banks, ATO, and even the Police, with the over 55 age demographic the greatest hit.

Some tips to help you protect yourselves from scammers, but also representing good IT hygiene, include:

- Treat EVERY email with a degree of suspicion. Is the email asking you to pay into a "new" bank account? This is a dead give-away!!
- DO NOT click embedded links that look suspicious.
- DO NOT open unknown attachments to emails.
- Built in windows firewall is sufficient in most cases, but also antivirus software will give some extra protection. Consider Bitdefender, Kapersky, Symantec, or McAffee.
- Adhere to using passphrases not just passwords. E.g., Mywifel0vessh0ppingonebay! versus Mwls0e!
- Use two factor authentication or multi factor where recommended.
- Consider Dashlane and LastPass as software solutions to manage your passwords.
- When configuring your Wi-Fi router make sure you change the username and password.
- Consider using a Virtual Private Network when travelling such as NordVPN, or Surfshark.
- Keep hardware and software up to date.
- Backup your data regularly. This will change dependent on data used.

Security of your IT systems is a multilayered approach, using much of the above, but also including making sure the person behind the keyboard is alert! Stay safe this Winter.