# Be scam aware

Online scams are becoming increasingly sophisticated, so businesses need to actively protect themselves and maintain a high level of skepticism and awareness. To help you we thought we would share some of the latest scams, so you can be on the alert.

To keep up to date we recommend registering at scamwatch.gov.au.

## False Invoices

They look like real invoices, and started life as real invoices, but hackers can intercept the software and/or emails of suppliers and access customer and invoice details. The key is that they request a change of bank details.

To protect yourself, always confirm any changes to bank details over the phone, never by email, as you may simply be communicating with the hackers.

## Ransomware

Cryptolockers and the latest CryptoWall 4.0 break into your servers, typically through remote access and lock your files, literally holding you to ransom. To date they have extorted more than $3m from their victims

To protect yourself, ensure you keep your security software up to date, constantly back up, avoid emails with attachments from unknown senders and seek advice from professionals as to what security you need. Ace can assist if you are concerned your IT security is not sufficient.

Ace Internet Services Pty Ltd
Acenet.com.au
1300 360 979

## Swift payments

Swift, the international company, used by large banks to transfer money around the globe was hit by numerous attacks earlier in the year. The hackers, or rogue internal staff used the Swift system to send out messages requesting bank transfers. While this scheme typically affects banks, always be aware.

To protect yourself, banks have been asked to update their security systems, and you should do the same, and be particularly careful if you do receive a swift payment request.

## Fake wire transfers

An oldie but a goody, this simple but effective scheme has seen a resurgence. Fraudsters simply ask for money to be wired to them using nearly, but not quite the right domain name, company.com.au becomes cmpany.com.au, and if you're not looking for it it's easy to miss.

To protect yourself, always check domain names, if they are miss spelt, or not quite right, always go back to the company through another means and double check.

## Remote access scams

If you receive a call out of the blue, claiming to be from Telstra, the NBN or other IT companies, and advising you that you need to urgently upgrade your software, beware. They request to remote into your computer, and demand you buy software to fix the 'problem' they identify.

To protect yourself, never allow someone to remote into your computer if you don't know who they are, and it is unsolicited. Never provide bank details over the phone if you haven't made the call or you don't know the person.  Only purchase software from a trusted source.