

IT'S A SCAM!! AND THE SCAMS ARE GETTING MORE SOPHISTICATED!

Written by Victor Hamit

In an unusual couple of weeks we have been approached by a number of clients about potential scams to which they have been subjected.

Coincidentally, the Australian Taxation Office ("ATO"), on 10 April 2019, issued a daily update for Tax Professionals warning of:-

"A recent spate of robocall scams are spoofing genuine ATO phone numbers to display on caller IDs. We [ATO] will never call you threatening immediate payment or arrest for a tax debt."

For more information on how to spot a scam or what to do if you receive one, go to the ATO website [here](#).

Email spoofing is the creation of email messages with a forged email sender address. The intention being to mislead the recipient into believing the email address is legitimately from a known or trusted source.

Another example of spoofing recently was an email "sent" from the client's own email address to himself. The email claimed that the client's website, contacts and email had been hacked. The hacker claimed it had taken control of the client's computer and computer camera. The hacker claimed that it had incriminating video and other evidence that the client had watched internet porn and unless the client paid the equivalent of \$US1,000 in bitcoin to a nominated account within 48 hours, the "incriminating material" would be distributed to all contacts in the client's email and Facebook accounts.

The client was suspicious because he did not watch internet porn on his computer (nor any other device!), nor did he have a Facebook account. The client immediately contacted his IT manager and was told it was a prolific scam and to both ignore it and contact his website and email service provider to adjust his Sender Policy Framework (“SPF”) and Domain Keys Identified Emails (“DKIM”) settings. Whilst this action cannot guarantee full protection, it will improve the website and email defences.

There are community blogs which identify common scams. But also check the following sample sites:-

- Australian Securities and Investments Scheme (“ASIC”): [Scams targeting ASIC customers](#);
- Australian Competition and Consumer Commission (“ACCC”): [Protecting yourself from scams](#);
- ATO: [Scammers fake ATO phone numbers](#); and
- IP Australia: [Unofficial Trademark Invoices](#).

By way of example, the ATO reported for the single month of January 2019:-

- 23,237 phone scam reports were officially made;
- \$497,216 was reported as being paid to scammers. Payments via Google Play, iTunes and Bitcoin amounted to 83% of the total amounts paid.

In addition, Telstra’s 2019 Security Report claims that 51% of respondents who have been victims of Ransomware have paid to unlock files. The report claims 77% of Australian businesses that paid the ransom were successful in retrieving their data.

For those subject to the Notifiable Data Breach regime under the Privacy Act 1988 (Cwth), the Office of the Australian Information Commissioner (“OAIC”) issues quarterly reports. In the quarterly report of October to December 2018, the major areas of notification were caused by human error or malicious or criminal attacks or a combination of both. The top 4 sectors that reported notifiable data breaches were identical to those in the previous quarter which in order were:-

1. Health service providers;
2. Finance;
3. Legal, Accounting and Management Services; and
4. Education.

This short Article provides an insight into the proliferation and increasing sophistication of scams, but also the scale of money involved. It is trite, yet important to emphasise not only ongoing updating of technological defences but ongoing training and preparation for your human resources.

Date Published: 26 April 2019

Victor Hamit

Wentworth Lawyers Pty Ltd

Level 40
140 William Street
MELBOURNE VIC 3000

Tel: +61 3 9607 8380
Mobile +61 408 590 706

Email: vhamit@wentworthlawyers.com.au

Website: www.wentworthlawyers.com.au

Disclaimer:

These materials are provided as a general guide on the subject only, not as specific advice on any particular matter or to any particular person. Please seek specific advice on your own particular circumstances as situations and facts vary.

Liability limited by a scheme approved under the Professional Standards Legislation