BULLETIN
All Members

Reference No: AM 15-17 **Date issued:** 06/07/2017

Ransomware Attacks

Dear Members

Due to recent ransomware attacks, which have affected some Australian businesses, VACC are warning members to remain vigilant against scammers trying to compromise your computer security. This potentially could damage your business.

Scammers will try and trick you into downloading a virus which infects your computer system and prevents you from accessing your personal data. Once infected, payment demands will be enforced upon you with no guarantees they will unlock your computer system.

The recent Petya ransomware is being distributed via email, embedded with a malicious attachment or link.
The ACCC have released some actions you should take to protect yourself, which include:

- Update your computer's operating system with the latest security patches – visit the Stay Smart Online < span style="font-style: normal;">website to find out how.
- Don't open emails or attachments from people you don't know.
- Make sure your computer's firewall is on and your anti-virus and anti-spyware software is up-to-date.
- Change passwords and backup your data regularly – store your backups offsite and offline.
- Ignore phone calls claiming they are from your internet service provider requesting remote access to your system.

Keep up-to-date with the latest scams targeting small businesses by following @Scamwatch_gov on Twitter or visiting the SCAMwatch website.

John Khoury
Industry Policy Adviser
Industrial Relations, Policy and Engagement
VACC
Level 7 | 464 St Kilda Road | Melbourne Vic 3004
P: 03 9829 1153 | **M:** 0412 510 108 | **W:** vacc.com.au