# What should I watch out for and how can I protect my business against scams and scammers?

Scammers want you to click the link, open the attachment and give away valuable information to gain access to your system. It is often the first click or opening that exposes a business to a security breach. Types of attacks include:

- Phishing: the email from a supposed bank or a supplier asking you to click this link or open that attachment or reply with your account details.
- SMiShing: using text message technology to trick a user into downloading malware such as a virus or Trojan horse, onto your phone. If the device is set up to synch with your office system, they can gain access to it and all your information.
- Scareware: convincing you your computer has been hacked or infected with malware and getting you to fix it by clicking on the enclosed link that then infects your computer.
- Ransomware: downloads that lock your computer or network where payment is required to unlock it.
- Vishing or 'voice phishing': phone calls where scammers masquerade as genuine business contacts. Some can display a fake caller ID. Automated recordings may direct you to call a given number or enter account details. Vishers may intercept your follow up call to confirm the call was genuine. A common trick is for the scammer not to hang up so they are able to stay on the line on your phone and impersonate a genuine contact.

To avoid falling for scams ensure your team are briefed and know what to watch out for. Check the email address or URL is correct. Often scammers use a slight variation of the genuine one. Never give out credit card or bank numbers and other business or personal identifying information. Have a secure backup solution. Consider investing in a mobile security application that includes SMS (text) filtering as well as anti-theft, antivirus and web protection. Call the supplier in question (whoever the scammer has masqueraded as) and check that the approach is legitimate. When calling to confirm, do so from a different phone. If you are still in doubt contact your IT provider.