Computer Security Tips

January 2017

Scam-proof your business

Scams and scammers become more sophisticated every day. No surprises there. They rely on keeping a jump ahead of people. As businesses step up their investment in new technology and media platforms, scammers find new ways to worm their way in.

FYI… Social engineering

Many scams fall under the umbrella term 'social engineering'. These techniques aim to gain people's trust and con them into letting their guard down to leave themselves (or potentially your business) open to fraud. You might have the most high tech security system in the world but it's useless if a human is conned into propping the door open. Social engineering approaches want you to act without thinking, to click the link, open the attachment, to be helpful and friendly and open the door. Social engineering manipulates people into giving away valuable information or unwittingly giving a scammer system access. It is often the first opening that exposes a business to a security breach. These techniques have emerged as security risks. Brief your team to minimise the risk of cyber-attack or fraud.

Types of popular social engineering attacks include:

Phishing: the email from the bank or a supplier asking us to click this link or open that attachment or reply with our account details.	Baiting: who doesn't like free stuff? Baiting plays on this by leaving around USB flash drives infected with malware. A user reaches for a handy flash drive and then unwittingly infects their computer and potentially the network.
SMiShing: short for 'SMS phishing', it uses text message technology to fool you. It can trick a user into downloading malware such as a virus or Trojan horse, onto his or her mobile phone or other device. If the device is set up to synch with your office system, you can see the problem. SMiShers can use text messages to obtain financial data from users for identity theft or fraud.	Vishing: short for 'voice phishing'. This scammer fools the victim into thinking that he or she is assisting a genuine business contact. Some can display a fake number or caller ID on your phone. 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.
Scareware: this involves convincing the user that their computer has been hacked or infected with malware or they have inadvertently made an illegal download. Predictably the problem can be fixed by clicking on the enclosed link. And then of course, the user's computer really has been infected with malware.	Ransomware: a user inadvertently downloads malware which locks up the computer or the whole network. The firm literally is held to ransom as it must pay the extortionist to be able to access its data, or else all files will be deleted, permanently encrypted or otherwise impossible to access.

Blocking scammers

Because there are so many variations on scams, brainstorm examples with your team. Role play scenarios so that you maintain good security for your business but don't accidentally enrage genuine customers and business contacts by being obstructive:

- Be alert to any requests for credit card or bank numbers, but be equally suspicious of requests for other business information such as contact details for the business' directors, for personal identifying information such as birthdates or other clues to passwords paving the way for hackers
- Have a secure backup solution
- Think about whether to invest in a comprehensive mobile security application that includes SMS (text) filtering as well as anti-theft, antivirus and web protection
- Brief the team that, if a call seems suspect, they should take the caller's details, and confirm with a manager, your IT provider or the supplier in question (whoever the scammer has masqueraded as) that the approach is legitimate. When calling to confirm, do so from a different phone

O'Connor Richmond Ltd
P O Box 172, Gore
Phone 03 2089240