Phishing and whaling – Don't get hooked!

With cyber-attacks on organisations on the increase one of the most common attack techniques we are seeing at present continues to be phishing and whaling attacks. So what are these? And more importantly; what can you do to stay safe?

Another week and another article in the news media of an organisation fooled in transferring money to a fraudster. The article contained the following description of the common modus operandi: "*Emails which appeared to be from a company or organisation's CEO or managing director were sent to the CFO, senior accountant or similar urgently requesting a funds transfer."*

It is evident that no entity is immune with NFP and Charitable organisations equal targets to companies. As the same article detailed: "*A volunteer at one of the Pony Club's regional branches was tricked into transferring more than $4000 into a stranger's bank account after being targeted by scammers posing as the organisation's president."* Fraudsters appear to be very equal opportunity in their approach – as long as there is a reasonable chance of success anyone is fair game as a target.

Sadly, this is an increasingly frequent occurrence. Yet even with increased media about such cases there are obviously enough successful attacks for the fraudsters to remain very motivated to keep trying it.

So what are phishing and whaling?

Phishing is an attempt to obtain sensitive information such as usernames, passwords, credit card details or money transfers usually by masquerading as a trustworthy entity or person. Like the word fishing, it is a technique that uses bait to catch the victim.

Phishing emails often contain links to websites that are infected with malware. The websites may look identical to the real ones they are impersonating and as such often convince unsuspecting users to enter details into them.

Spear phishing are phishing attempts directed at specific individuals or organisations. In these cases, the attackers often gather information about their targets to increase their probability of success. With the advent of social media, as well as other information on the internet there is often a wealth of information that can be easily obtained to assist attackers learn about, and even convincingly impersonate, those they are seeking to defraud.

Whaling, as the name indicates, is going after the big targets. These are phishing attacks specifically directed at senior executives or the governing body members in an organisation. Due to their roles, senior executives/governing body members generally have access to greater levels of information within an organisation. They also generally have the highest levels of delegated authorities and access to the greatest amounts of funds within an organisation. Hence it makes sense they are commonly being targeted.

Unfortunately, sometimes these senior execs and governing body members are also characterised by being very busy people and not always highly technologically literate. This can sometimes mean that there may be more likelihood of them not following organisation protocol and process - a recipe for security breakdowns.

So how can your organisation stay safe?

There is no guaranteed checklist but the following are some key protection measures:

1. Awareness training – Ensure everyone in your team is made aware of the risks. The more people are aware of the dangers, the less likelihood of being fooled by such attacks.
2. Payment authorisation control basics – ensure your controls such as payment authorisation delegated authorities and controls are followed and ensure these are taken appropriately seriously. A dual authorisation requirement doesn't mean that the second authoriser is just a rubber stamping exercise. The point of dual authorisation is two critical sets of eyes over the transaction.
3. Compare to budget and expectations. Is this an expense that the organisation would normally expect? Have these goods or services been requested and received?
4. Remain sceptical – if it looks odd, query it. And crucially don't just rely on email communication. Query with a phone call or other form of communication.
5. Implement/update IT controls to ensure firewalls are as robust as possible and also consider setting IT parameter controls which will reject processing payments over a certain amount.
6. Consider cyber risk when reviewing your insurance cover. This is important to ensure you are clear what you are covered for and whether this is adequate. One small positive of the increase in cyber-attack activity is an increase in the range and type of insurance cover available.

We also refer you to the helpful advice provided by IT security specialists from Kaon SecurITy
Introduction to Cyber Security – The Nuggets

Refer also to previous articles from RSM:

Fraud | Financial Whaling Scam

Phishing scam alert | IRD warning

It's not all about the technology…

Your authors recently attended an educational presentation for directors about cyber threats sharing the wisdom of a panel of experts. One of the most interesting takeaway comments from this came from perhaps the most technological expert panel presenter. Perhaps counter intuitively this self-confessed "technology geek" made the following two key observations:

1. **Cyber threats are not about the technology** – usually it is the human part of the process that is the weak link. Access to an organisation's systems is often gained by fooling people within the organisation to do things they shouldn't such as clicking on a link or opening a document. Impersonating others is also a key technique and now this is so much easier with the considerable amount of personal information that can be gained from social media.

2. **Don't just delegate protection from cyber threats to your technology people to lead** – they are an important part of the team but the risk protection for any organisation needs to be led from the governing body or CEO.

Summary

While cyber security may sound high tech and scary; many of the best protection techniques are good old fashioned basics of human control. Stay sceptical and stay safe.

About the Authors

Craig Fisher FCA is an Audit Partner and Chairman of RSM. Craig is a specialist regarding not-for-profit and charitable entity issues.

Contact Craig on:
D: +64 (9) 367 1654
E: craig.fisher@rsmnz.co.nz
W: www.rsmnz.co.nz

Brendon Foy CA is an Audit Manager at RSM and passionate about keeping his clients safe.

Contact Brendon on:

D: +64 (9) 367 1657
E: brendon.foy@rsmnz.co.nz
W: www.rsmnz.co.nz