IT for CEOs & CFOs is published by House of Words Ltd.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

Phishing Tackled – Phishing Your Own Employees Could Prevent a Disaster

Matt Rhodes

Matt Rhodes
Commercial Services Manager
Quiss Technology Plc

Biography

Matt Rhodes joined Quiss (http://www.quiss.co.uk) in January 2012 as Commercial Services Manager. His role is primarily to expand the hosted solutions division of the business and to liaise with software vendors to help them develop their Software as a Service (SaaS) offering. Matt's other responsibilities include new business development of the Support and Maintenance solutions that Quiss offer, alongside the resale of all IT hardware and software.

Having come from a technical background, Matt has a great understanding of the technologies that businesses should be adopting. He is also constantly keeping track of the market place to ensure he is ahead of the times with the latest advances in technology ensuring our customers have the best options available to them at all times.

Keywords Cyber security, Phishing, Email, Hacking, Risk, Breach, Training, Cyber-criminals, Ransomware
Paper type Opinion

Abstract

The recent mass WannaCry ransomware attacks brought chaos to a large number of organizations across the world and attracted huge publicity to the threat posed by cyber-criminals. News that its spread was caused without anyone responding to a phishing email may only add to the sense of complacency that surrounds the growing cyber-security threat. As the author of this article explains, cyber-criminals are now targeting employees with phishing emails to gain access to secure systems, recognizing that busy workers, often distracted, bored or ignorant of the dangers are the most likely route into a secure network.

Is your organization cyber safe?

More than 90% of hacking attacks follow a phishing or spear-phishing email and increasingly it is employees being targeted – they are the weak link in your security. Unfortunately, a lot of organizations and the people that work for them believe it will never happen to them. After all, your employees have had the induction training, warning them about cyber-criminals and you send them regular updates reminding them what to look out for when using email.

But people become complacent and criminals change their methods of attack – both of which could lead to a catastrophic security breach that damages your organization beyond repair or recovery.

Every organization could do more to protect their organization against cyber-crime and it starts with ensuring everyone understands security is the responsibility of every employee – from boardroom to workshop. Safety requires a shift in culture throughout an organization and some points to consider in making an organization more resilient to an attack, include:

- Does cyber security awareness training cover the latest attack methods? Do employees know what to look out for?
- Does every employee, whatever their role, always have the correct information available to them, to ensure they make the right decision? Ask questions and question answers!
- How resilient is the organization to cyber-attacks? Could an attack be identified and stopped at source, before any damage is done?
- Could the organization respond quickly and recover from an attack? Would a successful attack cause long-term impact and what would be the impact of data being stolen and released?
- Are the organization’s suppliers and customers taking cyber security seriously? A successful attack on any of these might increase the chance of a successful attack on the organization.
- Senior managers must engage with every department head in the organization – IT, security, corporate communications, HR, etc., to plan a clear response to an attack, with everyone aware of what they are required to do.
- Senior managers must assess whether vital information is backed up appropriately to allow the organization to recover quickly following an attack, with minimal disruption.

If you find there are those within your organization not taking cyber-security seriously, they are a risk to the future of your organization. You must act and phishing your own employees is a good way to find out how people will react to an attack they are not expecting.

The lure of phishing

Security training is usually part of the induction process, but even with regular refresher sessions, people can become complacent and criminals change their methods of attack, with phishing emails becoming ever more sophisticated.

Phishing is an effective approach for cyber-criminals to access networks, steal sensitive information or hold it to ransom. To ensure the criminals have the details they need to undertake an attack, they will usually scour personal social media channels or the target organization’s website. Here they will find the information needed to create emails that closely imitate communications from trusted sources like colleagues, clients and suppliers.

The techniques have been obvious and for some, the emails have been laughable in their attempts to entice recipients to respond, but it's the less obvious ones that pose the real threat and now form a growing proportion of phishing activity.

Phishing emails now regularly contain requests for the recipient to confirm account details, delivery instructions or orders, by clicking harmless-looking links that connect to relevant websites.

Unfortunately, these fake websites which mirror the originals will be used to steal log-in details, account passwords etc., and like all fakes, they are getting better.

Phishing in numbers

The risk of being caught is low and the criminals' chances of success are high, with statistics in their favour. About 10% of people targeted will fall for a phishing attack and 23% will open the message, with 11% clicking on attachments. In addition:

- 250% increase in the total number of phishing sites from October 2015 to March 2016;
- 91% of hacking attacks begin with a phishing or spear-phishing email;
- 55% increase of spear-phishing campaigns targeting employees.

It is important to explain phishing to employees and show them what to expect. Regular training will undoubtedly help cut the risk of an individual getting caught by a phishing attack, but complacency can creep in and the criminals only need to be lucky once.

Phish to catch a thief

To help bolster security, there are specialist service providers that will conduct simulated phishing attacks on an organization's workforce. Working closely with the organization's management team, believable emails are created that appear to come from contacts familiar to the employees, like customers, colleagues, clients etc.

The attacks replicate the methods used by real criminals and can target specific groups within an organization at different times and with fake, toxic attachments. The recipients will be unaware they are being tested, although over time word will spread and sharpen the defences further.

The response of each employee to the 'fake' phishing email is recorded, along with their actions; whether they opened the email, clicked links, downloaded attachments, etc.

If an individual responds inappropriately to the email, a message will inform them they have been caught by a phishing test and remind them to be more vigilant. The messages are not designed to cause distress to employees, but engage them in the security process.

However, until an employee experiences a 'real' phishing attack, you do not know how they will react. When they are shown the possible consequences of their actions, employees understand the role each one play in keeping their organization – and quite possibly their job safe.

The initial failure rate is often close to 33%, but after subsequent reminders and ongoing training, the failure rate should fall to approximately 5%, although it is unlikely any organization will ever achieve a failure rate 0% as we are dealing with humans some under pressure, some not feeling well, some working from home and some just plain forgetful.

Comprehensive reports identify areas for improvement and highlight which individuals need more help, allowing organizations to concentrate training budgets where they will be most effective.

IT for CEOs & CFOs is published by House of Words Ltd.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

What now?

Reducing the risk of an employee responding to a well-disguised phishing email, relies not on more technology, but on testing defences and changing the security culture.

Organizations should seek out IT service providers who they can engage to target their employees with 'fake' phishing attacks to discover the weak links and then help resolve them, before any real criminals show up.

Reference

Details about Quiss Technology's Phishing Tackled service can be found at http://www.quiss.co.uk/it-services/cyber-security-3/phishing-tackled/