Gone phishin'

General Features | Professional standards



01 August 2017

Responding to the wrong email could spell disaster. *Matt Rhodes* looks at ways to prevent this occurring in your company

Key Points

What is the issue?

Despite the immense publicity about the dangers of phishing attacks via email, 1 in 10 individuals will fall victim and unwittingly allow criminals access to secure networks.

What does it mean to me?

SMEs will often be the targets because criminals believe their chances of defeating security and gaining access are higher. And once in, they can attack larger, potentially more valuable organisations that have a relationship with the SME, using compromised email accounts to phish contacts, suppliers and customers.

What can I take away?

How to stay safe online; what to look out for and how to differentiate between authentic emails and a phishing attack.

The recent WannaCry ransomware attacks brought chaos to a large number of organisations across the world and again raised the profile of the increasingly sophisticated activities of cyber-criminals.

News that the virus was spread by attacking vulnerable public systems, which once compromised were used to infect other systems, rather than following a typical phishing attack may only lead to complacency as organisations again focus on physical security.

But cyber-criminals know to target employees with phishing emails to gain access to secure systems. They understand human nature and recognise that busy workers are often distracted, bored or ignorant of the dangers lurking within emails and

represent the weakest link in the security chain.

Despite the immense publicity about the dangers of phishing attacks via email, 1 in 10 individuals will fall victim and unwittingly allow criminals access to secure networks.

SMEs will often be the targets because criminals believe their chances of defeating security and gaining access are higher. And once in, they can attack larger, potentially more valuable organisations that have a relationship with the SME, using compromised email accounts to phish contacts, suppliers and customers.

Anatomy of a spear phishing attack

The cyber criminals will create a false, yet apparently credible email address that closely resembles that of a colleague, customer, supplier, etc.

They will typically use an address where a misspelling is not immediately obvious, like joe.bloggs@fordmotorconnpany.co.uk, which when seen small in the Outlook preview panel could look a lot like joe.bloggs@fordmotorcompany.co.uk at a quick glance.

Because the phishing email is personalised and appears to come from a recognised contact, many will beat email security and arrive in the target inbox.

Not expecting a targeted phishing attack, the recipient recognises the email address and the sender, because the best (or worst) criminals will use social engineering to discover information vital to the attack, like the name of the manager at a regional office, the head of accounts or a colleague on maternity leave.

The recipient then opens the email and responds as expected, by downloading the attachment (which is toxic), clicking the included link, or following instructions to re-set passwords, enter pin numbers or allow ‘IT engineers’ onto the system to correct a fault.

Often the toxic attachment will contain malware or ransomware that infects the device and spreads across the entire system to grant criminals access to an organisation’s data. If the criminals can’t steal data to sell, or divert funds from accounts, then they may decide to encrypt data on the system and hold the organisation to ransom as recently happened with WannaCry.

This is all possible from opening just one wrong email and unfortunately, the criminals are getting more sophisticated and their attacks more likely to breach the weakest point in any system, the people that use it. And they only have to get lucky once.

What to look out for in emails

Every email, regardless of who it appears to be from should be assessed the same way, by everyone in the organisation (or indeed to personal email addresses):

- **The sender**: Look very carefully at the sender. Ask yourself if you know this person. Is this their usual email address? Is the email address similar to one I recognise?
- **Subject**: You should always give your emails meaningful subject lines and you should expect to receive the same. Again ask yourself if the subject looks unusual or unexpected – be careful if there are obvious spelling mistakes, or excessive punctuation. Irrelevant, extraordinary or poorly written subject lines often identify an email as fraudulent or spam – get into the habit of checking.
- **Content**: In the body of the email, fraudulent emails will typically ask for actions to be completed. This might be to; visit a website, send some seemingly innocuous data or simply reply to the email. Be particularly wary of emails that request personal information, particularly banking information, or claim to be from your IT team or managed service provider. Criminals will often use emotional language and scare tactics, delivered with a sense of urgency to ensure the recipient responds to unlock a suspended account for example. Be wary if there is no personal greeting; the organisations that matter to you know your name and will often include partial account numbers, card numbers or phone numbers to reassure you.
- **Links**: Be wary of links in emails, which can easily be disguised and may take you to malicious websites that impersonate a genuine site.
- **Attachments**: If documents are attached to the email, ask yourself if you recognise the attached format? (Excel, Word, PDF, jpg). Does the email mention the attachment and what to do with it? Am I expecting an attachment? Attachments can transmit viruses, so open them only when necessary and do so with caution, particularly compressed files.

It is difficult to list the most common approaches used by cyber-criminals as they change all the time and thinking you know what to expect, can lead to complacency and a potential catastrophe.

The lure of phishing

For most organisations security training is usually part of the induction process and will typically include awareness of phishing attacks and what to look out for. But even with regular refresher sessions, people often become complacent and can easily be fooled by the increasingly sophisticated nature of modern phishing attacks. The problem is also exacerbated by criminals constantly changing their methods of attack and sharing best practice on the dark web. A recent attack even delivered custom web pages reflecting the email accounts being targeted, so people being phished via their Gmail account were presented with a realistic Gmail login page, so personal details could be stolen.

Phishing or spear phishing as it is often known when the attack is particularly well-focussed, remains 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 engage in social engineering. This practice requires the criminals to scour personal social media channels or the target organisation’s website, where they will find the information needed to create emails that closely imitate communications from trusted sources like friends, colleagues, clients and suppliers.

In the past, the techniques have been obvious and clumsy; easily seen for what they were. But despite the previous often laughable attempts to entice recipients to respond, the rewards have attracted more sophisticated criminals that pose a real threat and it is their activity that now forms 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 sounding websites. The links will look similar to the real thing, but often use what looks like a subdomain or will be a misspelt name similar to the real one.

Unfortunately, the websites are fake and closely resemble the originals. These will be used to steal log-in details, account passwords etc, and like all fakes, they are getting better and more difficult to tell apart from the real thing.

Phishing in numbers

The risk of being caught is low and the criminals' chances of success are high. The statistics are also on their side, with around 10% of those targeted, falling victim to a phishing attack, as 23% will open the message and 11% will click on the attachments.

- 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
- 34.9% of all spear-phishing was directed at organisations in the financial industry

It is important to explain phishing to employees and show them what expect. Regular training will undoubtedly help cut the risk of an individual getting caught by a phishing attack, but how does an organisation know how its employees will react to a real phishing attack?

Will they do the right thing and inform the IT department or senior managers? Will they own up to the fact they have clicked a link they now know they shouldn't have? Education is the key and just like at school, it's important to test that knowledge.

Phish to catch a thief

To help bolster security, there are specialist service providers that will now conduct simulated phishing attacks on an organisation's workforce to identify employees that might respond to a genuine attack.

Working closely with the organisation'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 organisation at different times and some will include links or fake, toxic attachments. The recipients will be unaware they are being tested, although over time word of the tests will spread throughout the organisation, which can only help raise awareness and improve security.

How each employee responds to the ‘fake’ phishing email is recorded, along with their actions; whether they opened the email, clicked links, downloaded attachments, etc.

When an individual interacts with the email, other than to forward to the IT team or a manager to alert them to the attack, a message will inform them they have been caught by a phishing test. The message which reminds them to be more vigilant, is not designed to cause distress to employees, but engage them in the security process and help direct the necessary education.

Comprehensive reports identify areas for improvement and highlight trends that reveal which individuals consistently fall for scams and need more help, allowing organisations to concentrate training budgets where they will be most effective.

The initial failure rate is likely to be around 33%, but after subsequent reminders and ongoing training, the failure rate typically falls to approximately 5%, which is still worryingly high, given the potential consequences. However, it is unlikely any organisation will ever achieve a failure rate of 0% as we are dealing with humans.

What now?

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

Organisations should seek out those IT service providers who not only offer the service to target employees with ‘fake’ phishing attacks to discover those likely to be taken in, but offer training services to help support the organisation in its efforts to improve security and resilience.

Staying safe online

The most important step in staying safe in the always-on, digital world is to believe you could be the subject of an attack. It pays to follow the news, stay alert for new trends and learn about different scams and the approaches they use.

Always think before clicking links or replying to emails, even those that appear to come from people or organisations you know; criminals are always out phishing.

Beware of fake websites that appear similar to genuine sites, with similar addresses – check the URL carefully. Bad grammar, spelling mistakes and poor images are a good indicator of a fake site and if the site wants personal or secure information like passwords or email addresses be very wary of complying.

Ensure you shop only at websites with ‘https’ and the padlock icon showing in the address bar, to the left or right of the URL. It makes sense to use a credit card instead of a debit card, as credit card companies are more likely to reimburse you for fraudulent transactions.

It seems obvious, but think long and hard about your passwords. Make them tough to guess, regularly change them and use different ones for each account, use song lyrics or words from a poem, change letters to numbers or symbols when allowed.

The risk of being hacked makes it essential you back up all of your data on your computer, smartphone and tablet so you can recover it easily in the event of loss, theft or a ransom demand. It also pays to reconcile your financial statements for questionable activity, paying close attention to small regular amounts.

Be careful using Wi-Fi in cafes, pubs, hotels, etc., and ensure it is the genuine network – ask staff for the details and passwords; never undertake financial transactions over open networks.

The best defence online is your common sense. Always keep your wits about you, be careful and remember the old adage, if it sounds too good to be true, then it’s likely to be a scam.

Message from the CIOT/ATT Professional Standards team

With HMRC tax refunds being a popular target for phishing PCRT offers some guidance at paragraph 3.37:

‘A member should keep his access credentials safe from unauthorised use and consider periodic change of passwords. Other useful information can be found at

- http://www.getsafeonline.co.uk/ and at
- http://www.hmrc.gov.uk/security/advice.htm for HMRC’s online security advice.
- https://www.gov.uk/government/news/gone-phishing-75000-fake-tax-refund-emails-reported for further details.
- http://www.hmrc.gov.uk/security/examples.htm for examples of phishing emails online

A member is recommended to forward suspicious emails to HMRC at phishing@hmrc.gsi.gov.uk and then delete them. It is also important to avoid clicking on websites or links in suspicious emails, or opening attachments.’

A cyber security course is available on our websites at http://www.tax.org.uk/professional-standards/general-guidance/cyber-security and at https://www.att.org.uk/other-guidance.

The government also offers guidance at http://www.cyberaware.gov.uk/