Article

Apr 2021

Taking the Bait

A few simple techniques to help protect yourself from being 'phished'

Dan Morrison
Senior Technology Consultant

Email dan.morrison@waterstons.com

What is phishing?

These days, with the announcement of a new exploit or vulnerability to steal our personal data or compromise our computers almost every other week, it's easy to forget about the other threats out there. Not all dangers of working online are technical in nature, and a lot of the time it's easier (and faster) for an attacker to simply ask for someone's password than it is to try and make use of the latest security flaw. This is achieved through a concept known as "Social Engineering", wherein the individual(s), with malicious intent, will pose as a trusted contact or organisation to trick their victim into providing information they would never give to a stranger.

Within the sphere of Social Engineering, the number one most popular technique is the use of "phishing emails" (yes that is the correct spelling). Phishing involves the distribution (spamming) of emails to a wide range of addresses. The email message itself will be crafted to appear as if it comes from a trusted company (e.g Apple or Microsoft), eliciting you to open a malware-containing attachment or follow a link through to a malicious or fake website. One particularly prevalent example last year involved an attempt to steal the credentials of billions of Gmail users with a realistic-looking fake Gmail page. A PhishMe report in late 2016 estimated phishing to be responsible for initiating 91% of cyberattacks and a subsequent report in 2017 showed the number of phishing attacks grew by 65% over the course of the year. The phishing trend isn't disappearing any time soon.

I myself received such an email recently from PayPal suggesting I need to sign into my account to resolve a payment dispute, or else my account would be suspended. The email was good enough to bypass my junk email filters and looked like the real thing, which would have been very convincing were it not for the fact I hadn't used PayPal for a couple of months. Closer investigation then revealed the sender's email address wasn't a real PayPal address (it was actually from an @nopaypal.com address) and the links in the email took you to a non-PayPal site. These factors would be easy enough to overlook if you were in a rush, distressed by the content or were actually expecting an email from PayPal.

Unlike "spear-phishing", where fraudulent emails are crafted specifically for individuals (e.g. Finance Directors, CEOs etc) standard phishing emails are not targeted, they are sent out to millions of people every day. They are not expecting to trick everyone, but if even 1% of people fall for it, that's thousands of compromised passwords, personal details or even bank accounts. This is a lot of reward for not a lot of effort on the phishers' end.

The attacks are getting smarter

These kinds of attacks are always evolving. It's one thing to get a fake generic email from a corporation, but what if the mail comes from someone you know? More recently we have seen an influx of phishing mail designed to steal Office 365 credentials, where the emails came from legitimate senders. The attack worked as follows:

- Someone already has their email login details stolen. The phisher uses these details to log into the victim's mailbox and send an email to all their external contacts. The email asks the recipient to review some documents and provides a link they need to click on to access these documents.
- The recipient clicks the link and is presented with a fake Office 365 login page. They use their Office 365 credentials to log in, and the phisher now has access to their mailbox too. The phisher then repeats the process with the recipient's external contacts and the cycle begins again.
- Eventually the phisher will have amassed a treasure-trove of credentials, which they can either sell or use to steal further information from the compromised mailboxes. Often both.

What made the above particularly concerning is that the phisher was actually monitoring the compromised mailboxes and could view any mail before the intended recipient. That way, if a recipient queried the phishing email from their trusted contact, the phisher would intercept the query and reply, assuring them that everything was okay. The recipient, trusting the reply, then proceeds to sign in, giving their credentials to a stranger without even realising.

So far, the purpose of the attack seems designed to harvest credentials, and the observed actions have been limited to propagating the email. However the attack could easily develop into something far more serious. Imagine if the CEO's mailbox was compromised. Not only are they likely to have some high-profile contacts to spread the phishing email but the phisher can effectively impersonate the CEO. This could have serious consequences for an organisation and its reputation.

What can you do?

Even though these kinds of attacks are evolving all the time, there are simple techniques you can use to identify fraudulent mail and avoid becoming a victim of these phishing campaigns. As a bonus, you don't even need to be a technical person!

- Don't use the links in the email. Instead, open a web browser, go to the website yourself and sign in there, rather than where the email sends you. You'll be able to tell pretty quickly at that point whether the "urgent payment dispute" you've been emailed about is actually real, but you won't have sent your credentials somewhere you don't want.
- Use 2-Factor Authentication (2FA), where possible. 2FA introduces an additional sign-in step such as receiving a code on your mobile that you have to enter alongside your username and password. Even if your username/password are stolen, they are useless without your mobile, and you'll see that someone is trying to use them!
- Trust your instincts. Are you expecting the email or does the language or tone feel different to a normal email from that person? Phishers will often use pre-prepared, generic responses that won't have that usual jovial tone that Joe Bloggs normally has when he's emailing you. If something feels off then it's better to play it safe than open yourself up to compromise. You could even call the sender. In the recent phishing example above, the phisher was impersonating the sender and responding as them. If you're unsure about an email from a trusted contact and they are asking you for private information, call them. It's worth the 30 seconds it will take to confirm whether the request is real, or if something suspicious is going on.

Staff training is key

Whilst there are any number of spam-filtering tools and technologies in the market, the best way to prevent attacks is to educate your people about the potential threats, as they are the first line of defence.

We've helped companies develop holistic cyber strategies to improve their security online. This includes awareness training for staff and customised phishing attacks to see how susceptible the workforce are. Needless to say the results were often surprising to an organisation. However, this information enables training to be provided where it's needed and nurtures a more pragmatic and cost-effective approach to security education.

Nobody should be paranoid about the email they receive, but they deserve to be safe in a world increasingly reliant on email and instant communication. If phishing is responsible for starting 91% of all cyber-attacks then by knowing how to spot and avoid it, you have just tremendously improved your organisations', and indeed your own, security online.