Spear Phishing Emails – Hackers Are Getting Smarter

We have previously sent several communications out advising what spear phishing emails are and how to spot them. Spear phishing emails are where the scammers have researched the MD and Accounts contacts at a company and emailed requesting a same day transfer. Usually the REPLY TO email address is an obvious fake one and this is one of the checks we have advised you check. Today this has evolved…

We have been sent an example where hackers have purchased a domain that is very similar to their intended victims domain and emailed from that, see below :-

From: Paul Smith [mailto:paul.smith@fabrikarn.com]
Sent: 22 June 2017 12:07
To: Andrew Dean <andrew.Dean@fabrikam.com>
Subject: Re: Payment

Hi Andrew,
Did you receive my last email?
Kind Regards,
Paul

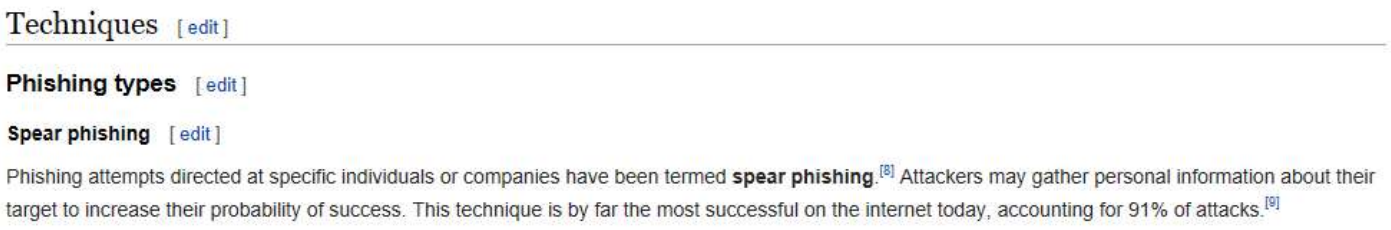
On Thu, 22 Jun, 2017 at 11:05 AM, me <paul.smith@fabrikarn.com> wrote:

To: andrew.Dean@fabrikam.com
Hi Andrew,
Are you available to set up and authorise a same day payment?
Kind Regards,
Paul

Only the eagle eyed among you will have noticed the "victim" domain is FABRIKAM and the "hacker" domain is FABRIKARN – when decapitalised these domains appear very similar **fabrikam / fabrikarn**

We have a policy within Pro-Networks that all payments requests are sent via email and authorised with a verbally communicated password – I would suggest all companies consider something similar as clearly the hackers are getting more and more sophisticated.

Customers tend to worry that their data has been compromised when they are targeted by such an attack but with the information available in the public domain today it is not too difficult to locate MD / FD details for most businesses. Please see an extract from WikiPedia below regarding Spear Phishing :-



Techniques [edit]

Phishing types [edit]

Spear phishing [edit]

Phishing attempts directed at specific individuals or companies have been termed **spear phishing**.[8] Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the internet today, accounting for 91% of attacks.[9]

I hope this helps and please share this with your colleagues and customers to warn them of this evolving threat.

As ever if you have any queries please do not hesitate to let me know!

Carl Jarvis
Pro-Networks