Organisational Resilience

Phishing attacks: Defending your organisation

In today's increasingly digital world cybercrime has become a powerful tool for criminals looking to steal data and extort money. The most successful and dangerous of all the cyber attacks is phishing. In this paper we will explore how phishing has evolved into sophisticated and often targeted attacks and understand what organisations need to be doing to protect their systems and data.

What is phishing?

Phishing is a type of social engineering attack often used to steal user data, including logon credentials and credit card numbers. It occurs when an attacker attempts to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, sabotage systems or steal intellectual property and money. Phishing can be conducted via text message or social media but the term 'phishing' is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly and hide amongst the huge number of benign emails that busy users receive.

A National Response

In April this year, the National Cyber Security Centre (NCSC) launched its Suspicious Email Reporting Service (SERS)[1] into which the public can report any suspicious email. The service was launched when the world was fighting two pandemics, one with the infection of COVID-19 and the other one with cyber-criminals targeting people with COVID-19 related phishing attacks. In the 3 months since the launch, the NCSC has analysed over 1 million reports resulting in the removal of over 4,000 scams and 11,000 dangerous URLs. This service shows how important the fight against phishing has become at corporate level as well as individual level.

Data – your most valuable asset

The Economist Magazine in May 2017 published an article "The world's most valuable resource is no longer oil, but data"[2] . With the amount of information we are producing every day in both corporate and personal space

along with increasing societal dependency in technology and connected systems, information is indeed the most expensive resource in the world. For this reason, criminals are after your data as personal information like bank details, card details, medical information or corporate information can fetch good value in dark web and then it can be used with malicious intent for financial benefit and identity theft.

Anatomy of an attack

Email has always been the primary tool used by cyber-criminals to target users. The Verizon 2020 Data Breach Investigations Report[3] identifies that 96% of public breaches starts with a phishing email. Cyber-criminals love phishing. Some are specialist in collecting data using simple phishing emails or text which is then sold on the dark web. Some cyber-criminals are good at reconnaissance, where they study your digital presence and then create well-crafted targeted phishing emails, also known as spear phishing, for a specific individual who has access to something valuable; for example finance staff who have rights to transfer funds.

As a matter of fact, every email account is important and a potential target. You may not trust an email from an unknown account but if it comes from one of your colleagues you are less likely to question its validity and any request within it. Compromised email accounts are mostly used for emailing others in the organisation with phishing emails. So, next time you think that your account is not of any value to anyone, think again, as it can be used to target someone who has access to more valuable information than you. Analysis by Cybsafe[4] of data breaches reported to the Information Commissioners Office in 2019 shows that phishing accounts for 45% of those breaches. IBM Security Reports that an average financial cost of data breach is $3.92 Million globally[5].

Trust is the most important thing in phishing attack. If a cyber-criminal can make you trust the email, then its game over for you. Normally, they use the sense of urgency or authority or manipulate human behaviours like emotions and fears. Criminals will use current news, such as the COVID-19 Pandemic, or big events like elections or specific times of the year such as Christmas to make phishing relevant to end users.

Phishing emails are also used to drop malware into computer systems. The malicious programme will then try to move through the system looking to find vulnerabilities in the network and act on them to create a loss of availability of data, such as a ransomware event.

Developing a mitigation strategy

To ensure a coherent response to the phishing risk organisations should develop a mitigation strategy considering both pre and post breach control. This must be a proportionate approach encompassing people, process and technical control. Key aspects to consider are:

- Focus on making end users your strongest link:
    - Create an environment that encourages users to report phishing attempts making reporting simple and within a blame free environment.
    - Embed cyber awareness into organisation culture and make users aware of how to spot phishing. Remember its awareness not training and not an hour-long yearly training to satisfy the compliance department.
    - Educate users on what is normal and what to expect within the business.
    - Make it easy for users to spot external emails. Tag external e-mails as EXTERNAL or something similar.
    - Use phishing simulation to educate end users about phishing as well as organisational policies where relevant.
    - Encourage users to manage their digital footprint and social presence so that they don't become an easy target.

- Make it difficult for attackers to reach the target by using web filters, email filters and applying anti-spoofing controls. Encourage the supply chain to enable Anti-Spoofing controls.
- Apply protective controls to minimize the impact of any successful attacks like Anti-malware, device and network hardening, application whitelisting, effective patch management and good password policy including Multi Factor Authentication (MFA) where possible.
- Prevent internet and email access to all network admin accounts and remove or suspend accounts that are no longer being used, such as when a member of staff leaves or moves to a new role.
- Apply detect controls, such as a security logging system, to spot any compromise to minimise the effect of the harm.
- Develop a Cyber Incident Response Plan and Phishing Playbook and exercise at regular intervals. Exercising a plan and learning from the exercise is much more important than having a plan.

Summary

Phishing is one of the biggest cyber threats we are facing, and everyone has a role to play in the fight against phishing, it's not just a corporate responsibility. Identify phishing and report them using the right channel to ensure that others who might not be lucky or smart to spot them become a victim of the same phish.

And for organisations a simple phish can end up with a massive data breach and a regulatory fine under GDPR or similar regulation, so ensure that there are adequate controls in place to mitigate this risk.

Zurich Cyber Risk Engineering service can help clients with developing their phishing mitigation strategy, increase awareness among key stakeholders and end users as well as develop and exercise response plans for phishing.

References

[1]https://www.ncsc.gov.uk/information/report-suspicious-emails

[2]https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[3]https://enterprise.verizon.com/en-gb/resources/reports/dbir/

[4]https://www.cybsafe.com/press-releases/phishing-dominates-uk-cyber-threat-landscape-shows-analysis-of-latest-ico-figures/

[5]https://www.ibm.com/security/data-breach