Are you the next Phishing Victim?

pwc

Organisations today are faced with increasing threats coming from the cyberspace, ones which could significantly damage their operation and reputation. As all industries shift towards IT-oriented infrastructures, the same is being undertaken by malicious users and organisations as they are aware that the weakest links in Security are users.

> Employees behind the keyboard can be unwitting participants to data breaches: **85%** of breaches in 2020 involved the human element.
>
> Verizon - 2021 Data Breach Investigation Report

Email phishing is a form of social engineering where malicious emails are designed to deceive recipients into providing sensitive information, or clicking links or file attachments that install malware (e.g. ransomware). Phishing attacks can target mass amounts of users or be part of a specific targeted campaign (spear-phishing). In each of the cases the atack can result in compromising sensitive data, loss of productivity and loss of client trust. Another variant of phishing called **Business Email Compromise (BEC)** has become more prevalent among threat actors in recent times. BEC attacks are designed to impersonate senior executives and deceive employees, customers or key suppliers into wiring payment for goods or services to bank accounts controlled by an attacker.

Countermeasures

Although security awareness training for employees helps users to recognise malicious emails, phishing scams evolve and are becoming highly sophisticated so it is difficult to gauge whether the organisation will suffer a successful phishing attack.

The PwC Phishing Simulation Campaign consists of an effective and practical exercise to assess how likely it is for one or more employees to fall for a phishing email and how far they will go: clicking a link; opening an attachment; divulging information; etc.

Types of phishing simulation campaigns

PwC service offerings

PwC can help your organisation by testing the human factor and identifying areas within your business that are more susceptible to a successful phish. This service offering comes into three standard tiers, starting from a basic campaign to a highly sophisticated one. Customisations to fit specific requirements may be done accordingly.

Tier 1

A basic campaign with minimal customisation designed to impersonate key people or departments in your organisation attempting to extract sensitive data from unsuspecting users.

Tier 2

A customised campaign disguised as legitimate business-specific communication that asks users for confidential information or delivers “malicious” attachments.

Tier 3

An advanced campaign that incorporates sophisticated attack scenarios, heavily customised payloads, and an impact assessment of a successful phish.

General customisations to the campaign usually include:

- Email scope: made to be relevant to organisation-specific risks
- Email frequency: sent at different times without obvious patterns
- Email subject and message: using organisation-specific language and references
- Logos and formatting: made to match the organisation’s standards and theme
- Landing page: made to look similar to the organisation’s services
- Awareness page: an informative page that phished users are redirected to, providing direct security awareness training
- Attachments: non-harmful payloads that simulate real malware, disguised as legitimate documents or executables

PwC will deliver your findings in a detailed report that captures all users' interaction with the campaign, including clicks, downloads, file openings, etc. This will provide you with insight into the various aspects of your business, highlighting potentially weak areas that require further security awareness investment.

Defending Against Phishing Attacks

1. Workforce awareness

Training personnel in identifying phishing email scams is critical as identification of such attempted attacks is the key step to preventing them. If certain criteria are met, such as the presence of invalid email headers and hyperlinks, there is clear evidence of fraudulent intentions which can easily be prevented with enough training.

2. Repeated phishing campaigns

Once awareness training is delivered, another phishing simulation campaign can be run to assess how effective the training was in raising user awareness and effectively detecting and avoiding phishing attacks. Ideally, phishing simulation exercises form part of the annual security assessment. The results from such exercises should be reflected in the overall cybersecurity strategy and policy of the organisation.

3. Stronger border defenses

implementing solutions which would halt threats from penetrating the perimeter of the organisation. In addition, introduce monitoring solutions to assist the detection process of such threats. In addition, reducing the attack surface to the minimum required, reducing the number of possible entry points for attacks.

4. Endpoint Protection

In the case where a user does click on a malicious email hyperlink or attached file, the organisation's endpoint security acts as the last line of defense, preventing the execution of the malicious payload.

Contact us

Michel Ganado
+ 356 2564 7012
michel.ganado@pwc.com

Kirsten Cremona
+356 2568 4629
kirsten.cremona@pwc.com

Follow us on: