wanstor

Microsoft 365 Attack Simulation Training

Managed Service Description

wanstor

Executive Summary

Cyber-attacks are a serious threat to UK businesses. According to the UK Government, 39% of UK companies have experienced some kind of cyber-attack within the last 12 months and nine out of ten of these attacks were caused by human error.

These errors include clicking on malicious links, entering credentials into fake websites, or falling for phishing scams. Cyber-criminals use various methods and channels, such as email, SMS, phone calls, etc., to trick your employees into compromising their security.

To prevent and respond to these attacks, employees need to be provided training on how to identify and avoid potential risks as well as provide simulated attacks to ensure users are applying the training. Microsoft 365 offers a comprehensive solution for cyber-security education and simulation.

Microsoft's cyber-security solution provides users with information on the most common and dangerous types of cyber-attacks, such as phishing, ransomware, malware, etc., and global training on how to deal with them and what actions to perform should an attack be successful.

It also allows administrators to send simulated malicious emails to users and monitor their reactions. Based on the results, users can be assigned global or targeted training to improve their skills and awareness.

Wanstor offers a managed service for Microsoft 365 phishing simulation and training that ensures organisations receive the full benefits of the product.

Wanstor will manage the configuration, setup, and regular delivery of training and simulated email campaigns, as well as the analysis and reporting of the outcomes.

wanstor

Attack Types

Cyber-attackers use various methods to target employees or organisations, such as email, voice calls and SMS. Some of these attacks are more sophisticated and use a mix of methods to trick users into believing they are authentic.

For example, an attacker might send a phishing email that looks like it comes from a trusted source and then call the user to confirm the email.

Types of phishing attacks consist of:

- **Email Phishing:** 'Phishing' is when criminals use fraudulent emails to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, gain access to organisations networks or steal data.
- **Whaling:** A whaling attack is more sophisticated than a regular phishing attack. Attackers conduct meticulous research to craft a message such as impersonating an executive at a company hoping to steal money.
- **Voice Phishing (Vishing):** Voice phishing, or vishing, is the use of telephony to conduct phishing attacks.
- **SMS phishing (Smishing):** Smishing is an attack that uses text messaging or short message service (SMS).
- **Pharming:** Pharming is a cyberattack intended to redirect a website's traffic to another.

wanstor

Managed Service Tasks

Wanstor will provide a managed service to configure and maintain the training and phishing simulation tests that Microsoft provide through the appropriate M365 licence.

This service includes a quarterly schedule of companywide training on the different attack surfaces, followed up by attack simulations every second month aimed at discovering gaps in users' knowledge.

Targeted training will then be aimed at specific groups of users to increase knowledge areas as required.

Training

+ **Companywide Training:** Wanstor will assign quarterly global training packages to the company incorporating training for all users, reaching subject areas including email, email security, PCI DSS (Data Security Standard), Social Engineering and data security.

  The training will also cover the necessary actions that employees must take if they suspect they have been targeted in a phishing campaign or if the user has been compromised or suspects they have been compromised by a malicious attack.

+ **Targeted Training:** Targeted training will be assigned to those who have been compromised based on the outcome of the simulated attacks. With specific deadlines and notification reminders as per the set training requirements

+ **Frequent Management Reporting:** Clear and concise monthly reporting to allow for visibility of training. This includes information on employees who have completed their training, those who have not yet finished, and those who have been assigned specific targeted training

wanstor

Attack Simulation

- **Varied Techniques:** Different target scenarios to determine vulnerabilities from credential harvesting, opening attachments and links. This will ensure that users are aware of diverse types of attacks and vulnerabilities and how to spot them.
- **Customisable Campaigns:** Increase the sophistication of the campaigns to include branding, custom formatting, logos as well as common public entities such as credit card, social media, and online retailers. This ensures a wide breadth of vectors are explored.
- **Frequent Managed Reporting:** Clear and concise reporting to allow for visibility of what and who the campaign targeted the training completed for everyone as well as those who require additional training.

Managed Attack Simulation Campaigns

Wanstor will configure and manage the campaigns provided by the M365 platform across an agreed scope of attack vectors aimed at global training, specific departments training or groups of individuals. There are 5 stages within the service. These are:

- **Pre-Requisites:** (only required at the initial setup)
- **Scoping:** define the target users and mail content
- **Configuration:** to configure the simulated email
- **Execution:** to deploy the simulated email to users at a specified time
- **Reporting:** management reporting on the results of the simulation
- **Training:** configuring targeted training dependent on the simulation results

Wanstor will deliver campaigns every two months. Each campaign involves a two-month cycle:

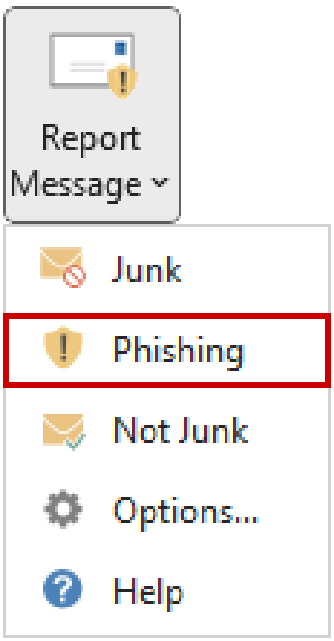
- In the first month, one day is dedicated to configuration and tailoring the campaign.
- The following month is used to curate the results and present them back to the customer.

Pre-Requisites

As part of the onboarding process, there are certain prerequisites to effectively utilise the training materials and conduct attack simulations.

Firstly, the customer will need specific Microsoft 365 licences (refer to Appendix 1 for details).

Secondly, it is advisable to install the reporting plugin in Outlook and supply instructions on reporting phishing emails, as this data is essential for tracking and analysis.



Without these components, the full effectiveness of the training may not be realised.

If these steps have not already been implemented, Wanstor will include them in the prerequisites for project delivery.

Another recommended prerequisite is to configure the tagging of emails sent from outside the organisation with either a tag or a banner.

This will inform recipients that the email originated from outside of the organisation.

This practice is particularly valuable in cases where potential attackers attempt to impersonate internal senders, as shown below:

[EXTERNAL EMAIL CAUTION] This email originated from outside of your organisation. Do not click links or open attachments unless you recognise the sender or know the content is safe.

Scoping

During the scoping stage, Wanstor work with you to determine the breadth and methods used in the campaign simulation.

Wanstor will determine the targets of the simulation which can be singular set of groups, departments or to all licensed users.

Wanstor will select differing methods of simulation ensuring that over the course of the service different simulated attack vectors are employed.

The techniques we will employ are:

- **Credential Harvest:** Users are directed to a website via a link within the email. The link then leads to website themed to represent a well-known website and asks the recipient to submit their credentials.
- **Malware Attachment:** An email is sent to the recipient with a malicious attachment which will then run arbitrary code which in a real scenario would help the attacker install additional code onto the target systems.
- **Link in Attachment:** A mixture of both credential harvest and malware attachment, the recipient is delivered an email with a link contained within an attachment directing the recipient to a web page themed to represent a well-known website and are asked to submit their credentials.
- **Link to Malware:** Much like the malware attachment but instead of attaching the malicious attachment the recipient is sent a link to malware often hosted on a well-known file sharing service such as Dropbox.
- **Drive-by URL:** The recipient is sent an email with a link which takes them to a website either a legitimate site which has been compromised or a website themed to be a clone of a well-known site. This website will then deploy code to the recipient's device.
- **OAuth Consent Grant:** The recipient is sent a link to an Azure hosted application created by the attacker which them prompts them to grant consent to their data.
- **How-to Guide:** The recipient is sent a guide on how to report phishing with the desired outcome that they successfully report the email as phishing. This technique would require the Outlook plugin to be installed.

Once the technique has been selected the next area to determine would be the branding templates. We can use the existing templates provided by Microsoft which have a predicted compromise rate attached to them.

Alternatively, we can create custom templates specific to the customer. Additional time will be required to create custom templates.

Following the assignment of templates and techniques, the training assignments are generated as the outcome of the simulation. It can be integrated into 3rd party training platforms if the customer subscribes to one, but the recommendation is to use the Microsoft Training Experience.

Assign Training for me: Microsoft will assign the courses and modules based on the simulations and training results.

Select training courses and modules myself: Based on the simulation we can assign selected modules.

The training will also have an assigned due date selectable from 7, 15 or 30 days after the end of the simulation.

We can also configure end user notifications for reporting phishing, for those who have been assigned training based on their response to the simulation and reminders to complete assigned training.

These can be customised as well to fit in with company branding.

wanstor

Configuration and Execution

After documenting the scope, Wanstor will configure the campaigns to align with the scope of each simulation. This includes specifying techniques, defining training assignments, and outlining the tracking process.

Subsequently, we will generate reports on training completion once the simulation period has concluded.

Types of campaign

As part of the M365 phishing simulations, attacks that mimic the following real-world examples can be run:

American Express password reset	Xerox Scanned Document
Expense report sharing	Sales order data
DHL Shipping Confirmation	Expired Password Notification
Netflix Account Suspension	New Voicemail Message
Facebook account verification	Office 365 Subscription Expiry

Reporting

Once each campaign has been completed. After 30 days Wanstor will provide a report detailing:

+ The scope, who was targeted.
+ The methodology, what method was used.
+ Number of reported emails (if applicable).
+ Who clicked on the link.
+ Who was compromised.
+ Who has completed the assigned training.

Wanstor will also provide a report detailing the users who have completed the company wide training assigned and ensure that new starters are assigned the training.

wanstor

Training

We will deliver statistics on the completion of training required from the attack simulations once completed.

Helping customers understand the efficiency of the training materials in reducing the likelihood of falling victim to a cyber-attack.

We will also deliver companywide training to ensure that those who have not been subject to training based on the outcome of the simulation campaigns are well versed in the subject of phishing as well as other areas of cyber awareness such as social engineering and data security.

Appendix 1

The following are pre-requisites for this service.

Administrative accounts: Sufficient permissions to complete the project are met before the start of the project. This includes M365 global admin, on-premises accounts, cloud accounts, and any third-party service that falls in scope of the completing the project. One account coving all permissions is also accepted.

Licenses: To use this service, the following licenses, or a combination thereof, are required. These licenses must be assigned to all users who are expected to participate in the campaigns.

Office 365 E5	Microsoft 365 E5
*Microsoft 365 E5 Security	*Microsoft 365 A5 Security
*Microsoft 365 F5 Security	*Microsoft 365 A5
*Microsoft 365 F5 Security and Compliance	
*Bolt-on licenses	