

Phishing Assessment Programme

XXXXXX

14 March 2022

NUMEN CYBER

Numen Cyber Labs - Security Services

Numen Cyber Technology Pte. Ltd.

11 North Buona Vista Drive, #04-09,
The Metropolis, Singapore 138589

Tel: 65-63555555

Fax: 65-63666666

Email: sales@numencyber.com

Web: <https://numencyber.com>

Table of Content

<i>Executive Summary.....</i>	<i>4</i>
<i>Background.....</i>	<i>5</i>
<i>1. Technical Summary.....</i>	<i>6</i>
1.1 Scope.....	6
1.2 Preparation	6
1.2.1 OSINT Open-Source Intelligence Gathering	6
1.3 Assessment Narrative	8
1.4 Assessment Matrix.....	9
<i>2. Summary of Assessment Activities, Model of Evaluation and Results</i>	<i>10</i>
2.1 Assessment Activities.....	10
2.2 Assessment Measurements and Results - User Actions	11
2.3 Assessment Measurements and Results - Action Time	13
2.4 Assessment Measurements and Results-Industry Level.....	14
<i>3. Assessment Conclusion</i>	<i>14</i>
<i>4. Solutions by NUMEN.....</i>	<i>15</i>
4.1 Policy solutions by NUMEN.....	16
4.2 Technical defenses solution by NUMEN.....	17
4.3 Training best practice by NUMEN.....	18
<i>5. Appendices.....</i>	<i>19</i>

Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document is considered proprietary information and should not be disclosed outside of the recipient organization's network.

Numen Cyber Technology permits to copy this report for the purposes of disseminating information within your organization or any regulatory agency.

Document Version Control

Issue No.	Issue Date	Issued By	Change Description
0.1			

Document Distribution List

NUMEN CYBER

Executive Summary

This report provides the assessment results for the XXXX led by Numen Security Lab from 7-11 Jan 2022. The assessment involves a specially designed practical exercise to support and measure the security awareness level and posture of the organization. The outcome of the assessment aims to show the susceptibility of XXX personnel to social engineering attacks by quantitative measurement of successful user actions and malicious link/content bypassing the organization's current security controls.

Numen measured XXX's level of vulnerability for a successful phishing attack by targeted user click rates, click times, response rates, and response times, as shown in the table below.

Overall Targeted User Targets vs Results

User Activity Metrics	Results
Total users targeted for phishing	Office A: 100 Office B: 150 Office C: 275 Office D: 356 Office E: 212 Office F: 198
Number of emails (phishing attempts) sent overall	3000 (~2 per user)
Number of clicked emails	268 (8.9% click rate)
Number of phished users overall	203 (13.5% of targeted population)
Number of user reports	148 (7.4% report rate)
Ratio of reports-to-click	.68
Average time to first click	52 minutes 30 seconds
Average time to first report	20 minutes 25 seconds
Most successful phishing template	Salary Payout Confirmation

Background

Cybercriminals use savvy phishing tactics to trick people into performing actions or divulging confidential information in a real-world case.

The objective of such attacks is to exploit the weakness of human psychology, using universal vulnerable human qualities such as fear, greed, curiosity, compassion, deference to authority, and so on.

While the plots of social engineering are constantly evolving but the fundamentals still boils down to the following techniques:

- Phishing
- Spear Phishing
- Pretexting
- Baiting and Quid Pro Quo

Phishing is **extremely dangerous** because it takes only one careless act to open the door for a cybercrime incident and resulting in a **significant impact** on data breach or infection of a device, server, or network that can **severely harm** the Organization's financial and reputation.

To address this issue, Numen has established a holistic solution to help organizations in:

- Security Awareness Training
- Reduce associated risk using Real-World Phishing Simulation with a different types of Risk categories

The delivery method during the assessment includes a specially crafted malicious link, QR code, attachment with embedded executable code, and so on. Numen utilized method(s) effectively based on the designed attack scenario catered for the engagement.

1. Technical Summary

1.1 Scope

The Phishing assessment was carried out during authorized working hours and it included the following scope:

- **Target:** Office A/500
Office B/1000
Total: 1500 Emails
- **Assessment period:** 7-11 Jan 2022 9-6 PM

1.2 Preparation

The Phishing assessment preparation includes the following:

- Phishing Email Templates
- C & C Server to capture the assessment results
- Links that simulates a malicious link
- The Document simulates malicious files
- QR codes that simulate malicious QR code

1.2.1 OSINT Open-Source Intelligence Gathering

OSINT intelligence is a powerful technique used for the extraction and analysis of information stored on the public internet to gain insights for adversary planning of a cyber-attack.

Numen used a variety of tools to achieve this attack that involve passive and active reconnaissance to build a profile of targets and target the potential weaknesses found.

The following is a non-exhaustive list of information that can be collected on XXX domains:

- Employee information
 - names
 - emails
 - phone numbers
 - titles

- addresses
- usernames
- Security policies
 - password complexity
 - physical security
- Network information
 - IP Ranges
 - Domain Names
- Job announcements to identify technologies used within your organization
- User-generated content
 - Company blogs
 - Project presentations or whitepapers
- Source code leakage
 - Github

In this activity, Numen discovered employees' information and corporate confidential information on the public internet.

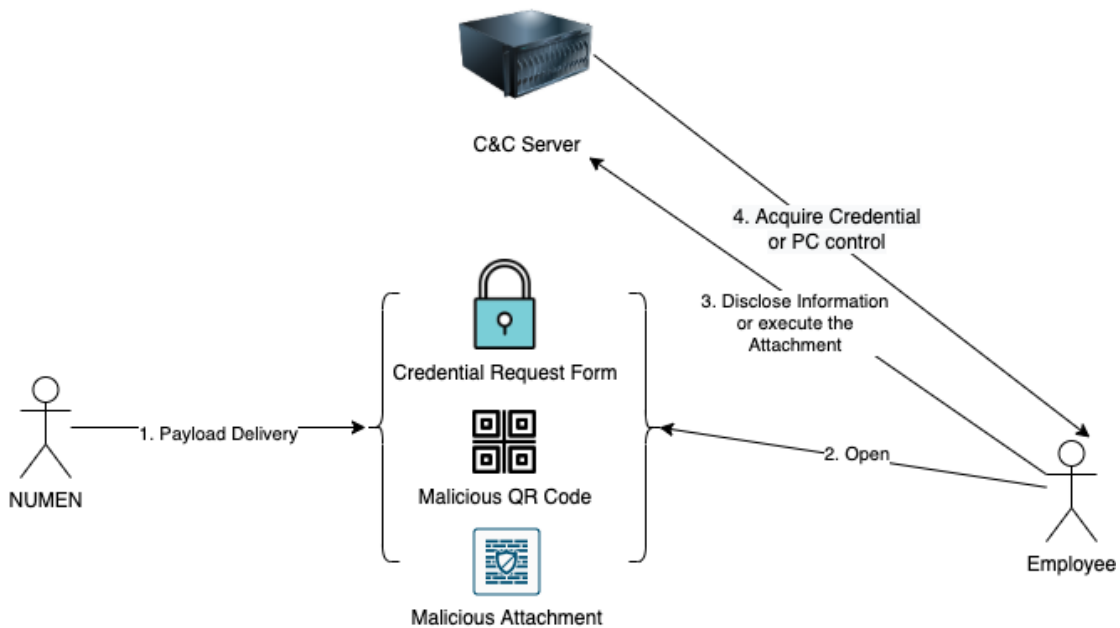
NUMEN CYBER

Reconnaissance Results

Item	Results
Number of Unique email addresses found	30
Number of Network information found	5
Number of Security related information found	1
Number of Confidential content found	2

1.3 Assessment Narrative

Numen simulates a real-world attack to target the organization's core website to obtain credentials and gain access control to personnel corporate machines. The assessment involves Numen setting up attack environments, phishing templates, and attacks strategies. The following diagram describes assessment flow based on the best-case scenario:



1. Numen adopted the methodology documented in **Appendix A** to deliver the payload to the unsuspected Employee
2. Employee open the phishing email and read the email content
3. The Employee either executes the malicious file or fills up the phishing form after being redirected to the phishing site that NUMEN has set up.
4. The C&C Server that NUMEN has set up during the preparation will capture the assessment results, the actual result is found in **Appendix B** of this report.

The assessment approach is divided into three aspects, and they are equally important for overall assessment.

1. Real-world attacks used by hackers - OSINT Intelligence
2. Email Phishing – using the mailing list provided by the client to conduct multi-dimensional and multi-scenario phishing email attack drills.

3. Other means of Phishing using phone number/corporate messenger of personnel provided by the client and launch spear phishing.

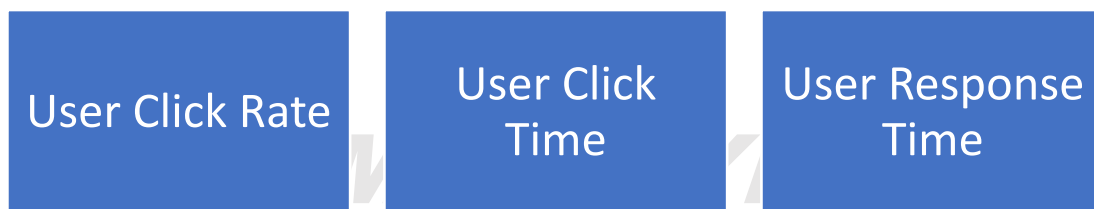
Numen divided the information collected into three groups and assigned them into 8 levels of exercise. The assignment of the group to levels of exercise is allocated based on the effectiveness of the exercise to the targets.

To allow Numen to effectively and accurately conduct the assessment, XXX performed the following:

- XXX whitelisted the Numen domain and IP address during the planning stage.
- XXX created specific mail receiving rules to permit the Numen emails to land in user inboxes

1.4 Assessment Matrix

The Assessment scoring is based user's behavior accounting to the following Matrix:



2. Summary of Assessment Activities, Model of Evaluation, and Results

2.1 Assessment Activities

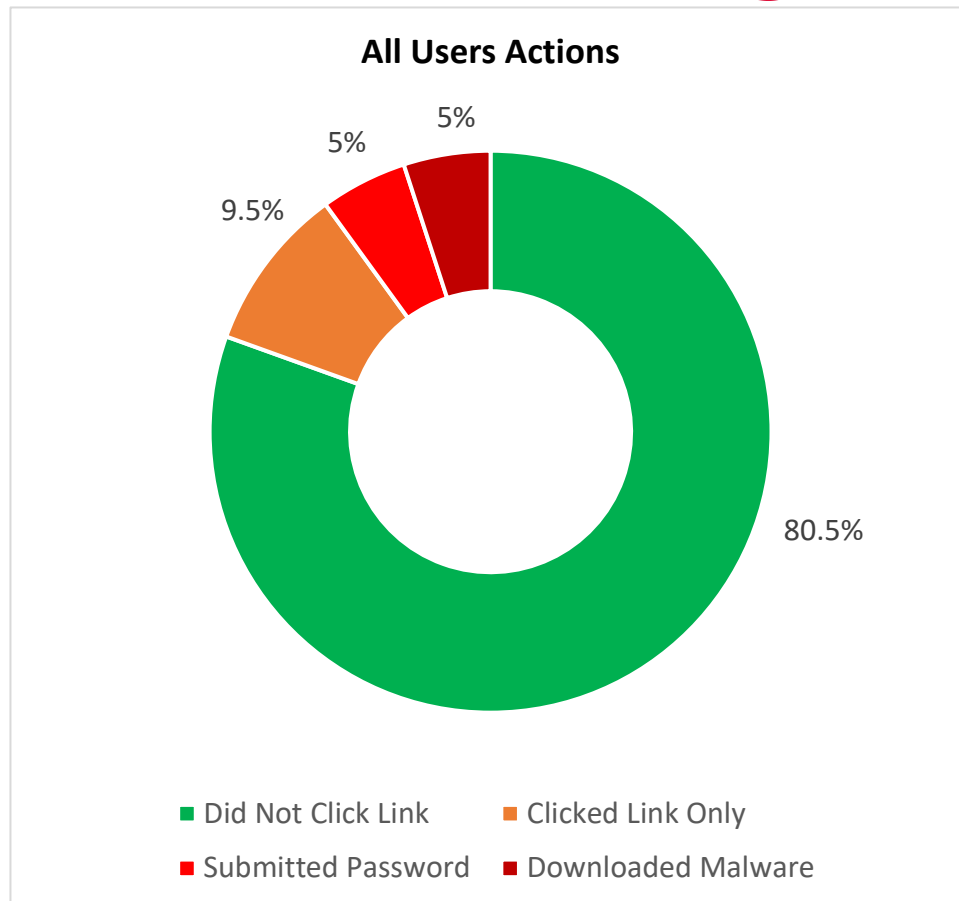
Numen used a mixed-method approach to explore employee susceptibility to targeted phishing emails and IM.

Level	Exercise	Description
1	Vaccination Status Update	Specially worded email from fake “HR Services” requesting vaccination status update
2	Urgent Software Update	Specially worded email from “IT Services” stating computer software is out of date and a critical patch is required for security reasons.
3	Password Reset Request	Specially worded email from “IT Services” requesting for Password Reset with reasons of New Password Policy or/and Account Lock due to unusual activities detected.
4	Staff Benefits Policy Update	A specially worded email with a fake link to view and download policy
5	Important Feedback Request	Specially worded email from “HR Services” requesting feedback on a new program.
6	OSINT Spear Phishing	Collection and analysis of data gathered from open sources to harvest sensitive information that can be exploited
7	Salary Pay-out Confirmation	Specially worded email from “Finance Services” to confirm salary payout due to payment system issues.
8	Deference to Authority	Specially worded email from “Higher Authority” with urgency influence techniques.

2.2 Assessment Measurements and Results - User Actions

Targeted users must agree to click on the malicious link or attachment for the attack to be successful. Submitting credentials or any sensitive information further proves the vulnerability of the targeted users.

Level	Exercise	Unique Clicks/ Response	User Click /Response Rate %	User Reports	User Report Rate %
1	Vaccination Status Update	200	3.60%	50	12.83%
2	Urgent Software Update	4	1.30%	14	3.50%
3	Password Reset Request	126	12.05%	32	10.50%
4	Staff Benefits Policy Update	37	11.08%	38	9.50%
5	Important Feedback Request	40	10.5%	20	5.40%
6	OSINT Spear Phishing	4	8.5%	1	10.5%
7	Salary Paycheck Confirmation	500	20.50%	100	6.6%
8	Deference to Authority	5	10.50%	40	4%



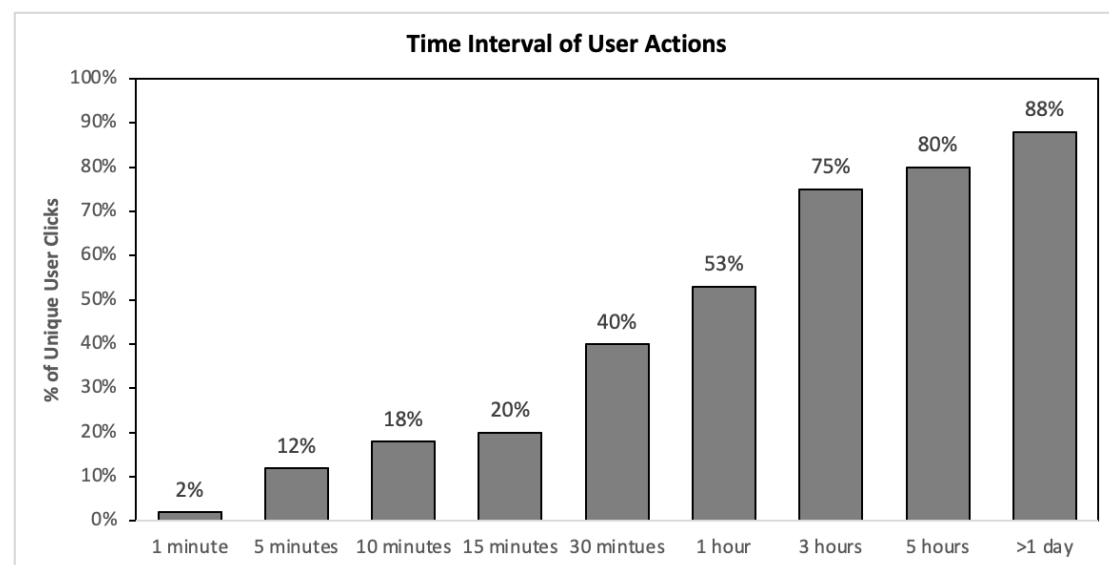
NUMEN CYBER

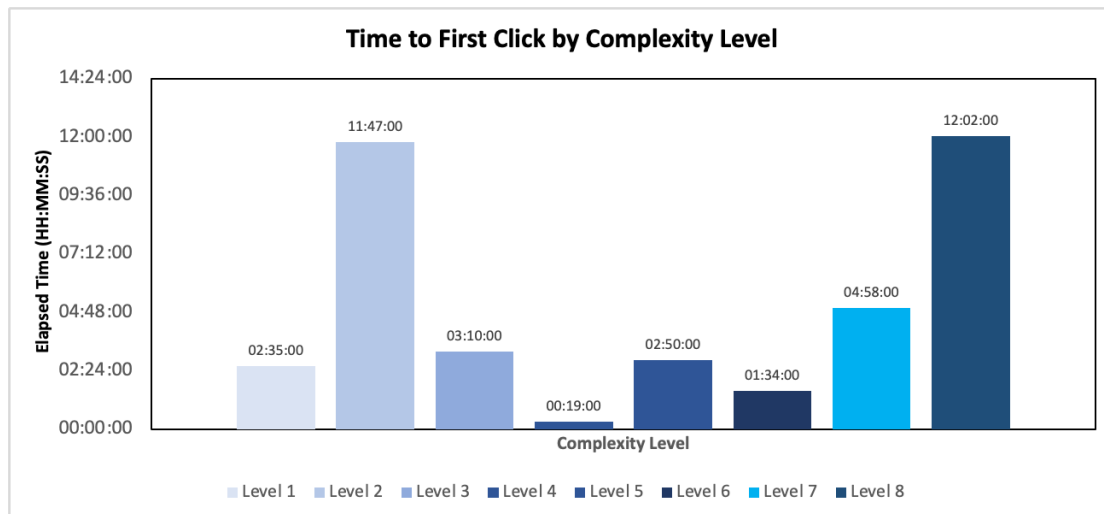
2.3 Assessment Measurements and Results - Action Time

Click time after receiving a malicious link shows the time to potential breach and the report time shows how fast the organization can take action to contain a potential breach. Timely user reporting decreases the window of opportunity that an adversary can gain access to data or gain further network entry.

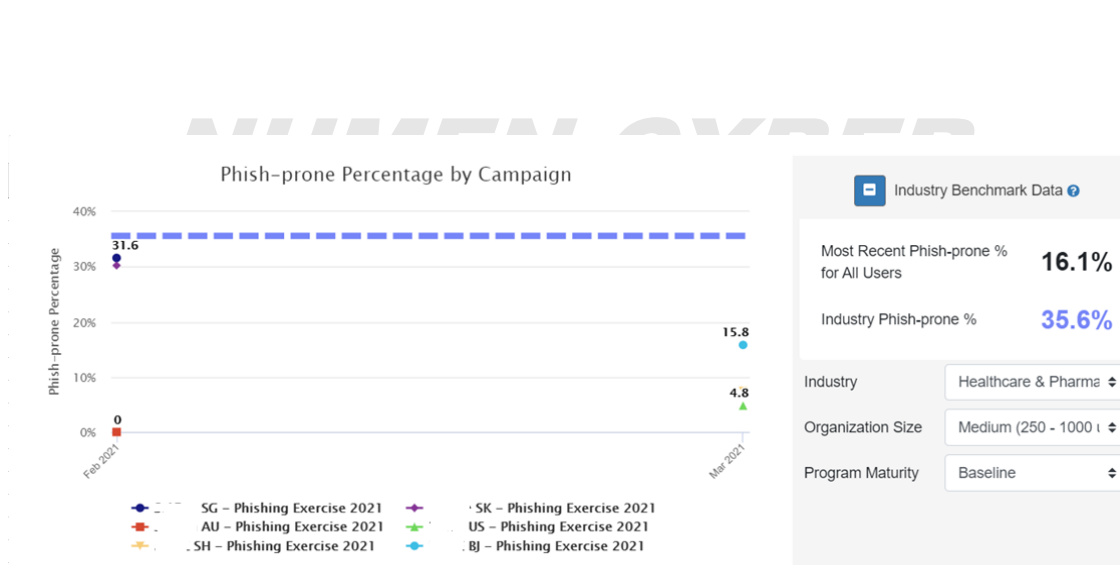
Level	Exercise	Time to First Click	Time to First Report	Time Gap (LEAD Time)
1	Vaccination Status Update	2:50:00	0:15:00	2:35:00
2	Urgent Software Update	12:07:00	0:20:00	11:47:00
3	Password Reset Request	3:40:00	0:30:00	3:10:00
4	Staff Benefits Policy Update	0:30:00	0:11:00	00:19:00
5	Important Feedback Request	8:05:00	5:15:00	2:50:00
6	OSINT Spear Phishing	6:40:00	12:15:00	1:34:00
7	Salary Payout Confirmation	5:03:00	0:05:00	4:58:00
8	Deference to Authority	15:07:00	3:05:00	12:02:00

The figure below shows the percentage of users who clicked during a certain time interval in the first 24 hours of the exercises. 53% of phishing targets clicked within one hour of receiving the malicious content.





2.4 Assessment Measurements and Results – Industry level



3 Assessment Conclusion

NUMEN concludes that most XXXX's employees have very **high-security awareness** based on the assessment result. The Assessment also identifies the individuals mentioned in **Appendix B** who are weak in security awareness, as these individuals may pose a threat to the cyber defence. We advise XXXX to provide more security awareness training to these individuals, which is identified in **Appendix B**.

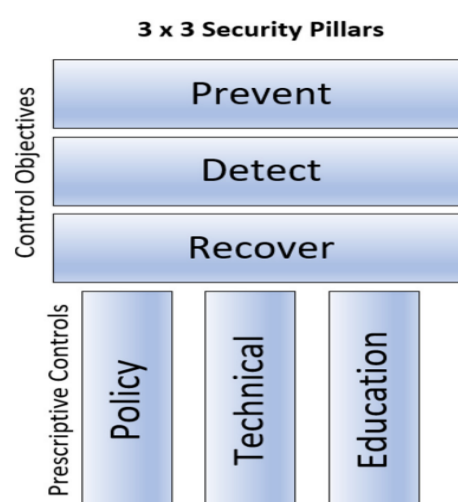
4 Solutions by NUMEN

Effectively fighting Phishing attacks requires the best defense-in-depth, a combination of policies, technical defenses, and security awareness training.

Security policies are the effectively and consistently communicated instructions, recommendations, and procedures that a stakeholder should follow to most effectively eliminate risk and the chance of a threat being successful. Policies can be verbal, written, exemplified by behavior, or posted online, and require attestation of understanding of the stakeholder. They can be voluntary recommendations or required (sometimes by law).

Technical defenses are all the physical and logical mitigations and controls implemented to prevent something harmful from happening. In the digital world, this often refers to logical implementations due to hardware devices (like firewalls, etc.), operating systems, and applications. Technical defenses are great at blocking large percentages of previously recognized, broad types of attacks.

Training is all the actions taken to teach another person a particular action or behavior. Security awareness training, in particular, is education used to make a person aware of a particular type of threat to make them less likely to be involved in the success of a malicious exploit. Some amount of social engineering and phishing will always get past your policies and technical defenses, so training is needed to help users recognize threats and take the appropriate actions




Effectively fighting cybersecurity attacks takes the best, defense-in-depth, cost/benefit-justified, combination of policies, technical defenses, and training possible.

4.1 Policy Solution by NUMEN

Every organization should create the best policies possible to fight social engineering and phishing. The policies should help mitigate the risks and damages from social engineering and phishing, and instruct all stakeholders to take appropriate actions should they be involved in an attempted or successful phishing attack.

NUMEN GRC can help create and implement policies as below to defend Phishing.

Checklist Item	Checkmark
Policies	
Acceptable Use Policy which stakeholders sign when hired and at least annually thereafter	
Specific Anti-Phishing Policies	
Specific policies to prevent business email compromise scams	
Training Content	
Teach stakeholders how to recognize rogue URLs	
Teach stakeholders how to spot phishing emails using Red Flags of Social Engineering	
Defined and communicated of how someone should handle/treat a simulated phishing test and/or real phishing event	
Defined methods of positive reinforcement for successfully spotting a simulated phishing test and/or real phishing event	
Defined and communicated consequences for failing simulated phishing tests	
Notice of simulated phishing training and methods	
Defined and practiced incident response plan and policies	
Defined and communicated crisis response plan (e.g. when to involve sr mgmt., HR, lawyers, recovery specialists, PR, etc.)	
Defined and practiced disaster recovery/business continuity plan(s)	
Ransomware handling and decision on whether to ever pay ransom	
Cybersecurity Insurance	

4.2 Technical Defences solution by NUMEN

There is a fundamental decision of where a cybersecurity defense should be located. Following the defense-in-depth concept, NUMEN suggests that computer defenses should be located everywhere: on the network edge, between networks, on ingress points, on egress points, on individual hosts and devices, and in the cloud. Many defenses work best located in a particular location and others work best in multiple locations. In general, NUMEN can provide technical services as below to defend phishing and social engineering.

Technical Defenses	
Defense-in-Depth plan	
Network security boundary defenses	
Content filtering defenses	
Anti-Phishing identification services/products	

Checklist Item	Checkmark
Feature like Phish Alert Button so stakeholders can easily report attempted phishing attacks	
Detonation sandboxes	
Reputation services	
DNS checks	
Anti-Malware defenses	
Implementing least-permissive permissions	
Email client protections	
Browser protections	
Implementing global phishing standards (SPF, DKIM, and DMARC)	
Network traffic analysis	
Data-leak detection and prevention solutions	

4.3 Training best practice by NUMEN

The overall goal should be to change your organization's overall culture so that all employees actively work to reduce risk from cybersecurity threats, particularly threats from social engineering and phishing. No matter how well thought out and deployed, some amount of social engineering and phishing will always get past your policies and technical defenses, so training is needed to help users recognize threats and to take the appropriate actions.

Training Best Practices	
Initial simulated phishing baseline test	
Longer, annual training	
Shorter, monthly or more often training	
Monthly or more often simulated phish testing	
Analyze results to determine where to concentrate more	
Professional Hints	
Make them care	
Train like a marketer (e.g. frequent, repeatable, entertaining)	
Offer interesting training	
Use a variety of training methods (e.g. videos, quizzes, documents, games, etc.)	
Create incentives	

➤ Phishing Training Methodology

- 1 Conduct Baseline Testing:** Conducting a baseline test is the first step in demonstrating the need for security awareness training to your senior leadership. This baseline test will assess the Phish-Prone percentage of your users. It's also the necessary data to measure future success.
- 2 Train Your Users:** Use on-demand, interactive, and engaging computer-based training instead of old-style PowerPoint slides. Awareness modules and videos should educate users on how a phishing or social engineering attempt could happen to them.
- 3 Phish Your Users:** At least once a month, test your staff to reinforce the training and continue the learning process. You are trying to train a mindset and create new habits. It takes a while to set that in motion. Simulated social engineering tests at least once a month are effective at changing behavior.
- 4 Measure Results:** Track how your workforce responds to both training and phishing. Your goal is to get as close to zero percent Phish-Prone as possible.

5 Appendices

Appendix A: Methodology

[Redacted due to Proprietary reasons]

Level	Campaign	Description
1	Internal Vaccination Update Form Request from HR	A Spoof email request from the "Human Resource" Department requesting the employee fill out the malicious "Internal Vaccination Update Form".
2	Password Reset Request	A Spoof email with an embedded malicious link from the technical support requesting the employee to reset passwords due to "new password policy" or unusual account activity.
3	Staff Benefit Announcement	A Spoof email announcement from the "Human Resource" Department about the upcoming "Staff Benefit". This email will contain a malicious "Staff Benefit" poster and a malicious link that allow the employee to log in to view the new "benefit".
4	Important Feedback Request	A spoof email from the "Human Resource" Department to request feedback regarding the company's work culture.
5	Software Update	A spoof email from the IT support to download an important software update that contains a malware
6	OSINT Spear Phishing	Creating personalized phishing based on the research done about the employee, understanding his likings and other details from OSINT
7	Finance salary issue last confirmation	A spoof email from Human resource department in the last week of the month informing the employee that due to a bank account issue salary won't be credited for the month and employee needs to fill out a form to fix the issue
8	Deference to Authority	A spoofed mail from someone with higher authority like CEO asking employees to fill a form or do a task

Appendix B: Detailed Results

[Redacted due to Proprietary reasons]