Cap Stone



Security Assessment

By Rashad Moore

Table of Contents

[Executive summary 3](#_Toc157272139)

[Introduction 4](#_Toc157272140)

[Open-source intelligence analysis 5](#_Toc157272141)

[Vulnerability Scan report 9](#_Toc157272142)

[Risk assessment 11](#_Toc157272143)

[Introduction 11](#_Toc157272144)

[Internal and external context 11](#_Toc157272145)

[Scope 12](#_Toc157272146)

[Risk assessment results summary 12](#_Toc157272147)

[Risk Matrix 13](#_Toc157272148)

[Reponse Plan 15](#_Toc157272149)

[Network Architecture 17](#_Toc157272150)

[Revised Network 18](#_Toc157272151)

[Firewall rules 19](#_Toc157272152)

[Training Plan 20](#_Toc157272153)

[Phishing Simulation 21](#_Toc157272154)

# Executive summary

Numerous areas have been uncovered from employee’s bad cyber hygiene to many vulnerabilities inside the infrastructure. Several inconsistencies within the network including the use of out-dated software were also identified within the network. It was also found that there are no security controls in place such as firewalls, intrusion detection systems, or antivirus software. These factors are all integral to the company and can all be exploited by malicious attackers to gain unauthorized access to the system.

To adequately address the identified issues, a risk and asset-based assessment was created to give a comprehensive understanding of what is at stake. This has revealed highvalue assets including the cloud servers, network infrastructure, staff and intellectual property. Several risks which could potentially threaten the security of these assets were also identified. These include cyber-attacks, reputational damage and financial strain.

To combat a 12 month phishing drill will be launched at random time to test cyber hygiene development. Topics such as social engineering and password management have also been included and will be tested in simulation. To ensure timely and successful reaction to security problems, we also recommend designing and testing incident response plans. Additionally, it is imperative to develop and implement methods to ensure the protection of high-value assets. Things such as access controls and data encryption.

In all THISISAFAKECOMPANY’s cyber hygiene has been assessed and recommended procedures have been given. Implementing them will raise the company’s security standard and protect sensitive data from being compromised.

# Introduction

THISISAFAKECOMPANY is currently in recovery after suffering from a breach. Professionals have been brought in to assess the company to aid in implementing and maintain good cyber hygiene in hopes to safeguard their data and maintain the trust of its stakeholders and clients.

This security assessment analyses security posture of THISISAFAKECOMPANY’S information technology systems, infrastructure, and procedures following a breach which occurred on December 5th, 2023. This assessment includes open-source intelligence analysis, vulnerability assessment, asset risk assessment and training plan.

Once recommended procedures to in place THISISAFAKECOMPANY will drastically lower its chances of being breached.

# Open-source intelligence analysis

Osint on THISISAFAKECOMPANY

This report focuses on information publicly available on THISISAFAKECOMPANY website. The goal is to see if any online resources contributed to the incident.

Operation statement values and physical location

The company’s mission is to reduce carbon emissions and develop technologies to aid. It’s commitment to ongoing research and the ways in which it is working to inspire and empower others to join in the fight against climate change.

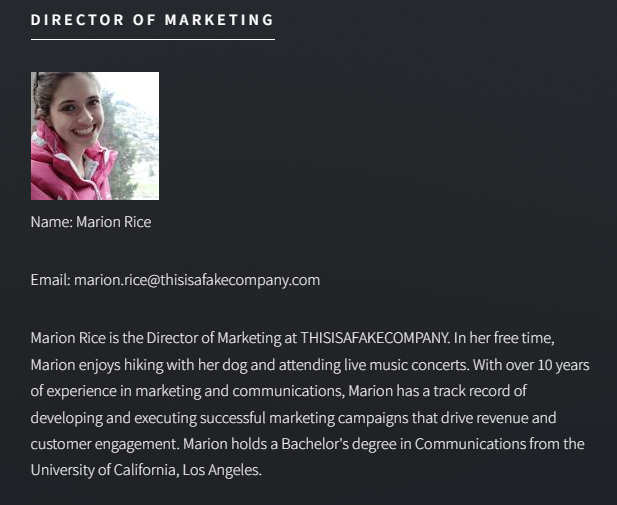
* Threat actors may target this information to understand the organization's core values, business direction, and commitment to sustainability and ethical practices. This knowledge can be used to exploit any contradictions between stated values and actual practices, potentially damaging the company's reputation or using it for social engineering attacks.

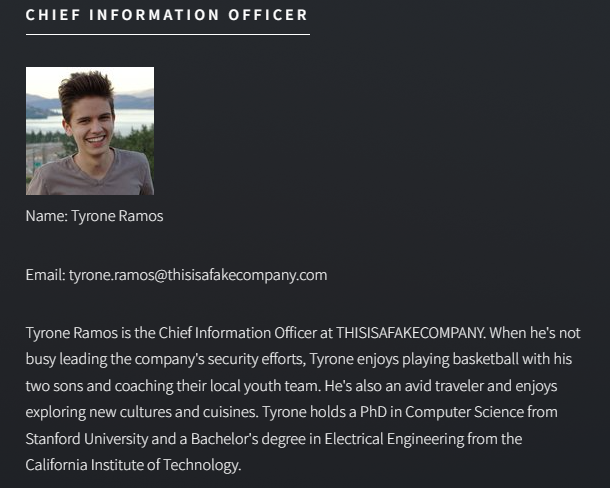
Company Address: 438 Richmond St W, Toronto, ON M5V 3S6

* Threat actors may target address information to plan physical attacks, such as break-ins, theft, or vandalism. Knowing the locations of the headquarters, manufacturing plant, and retail stores provides critical intelligence for carrying out such activities.

Leadership Team



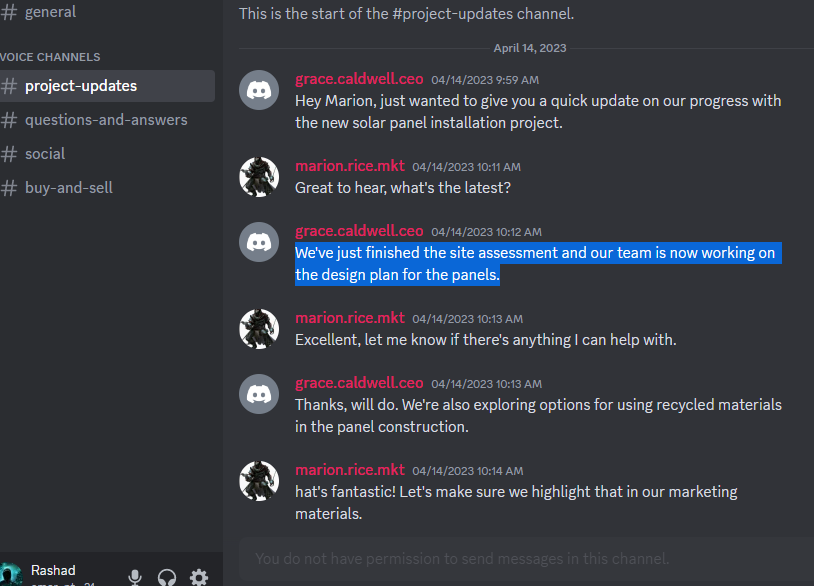


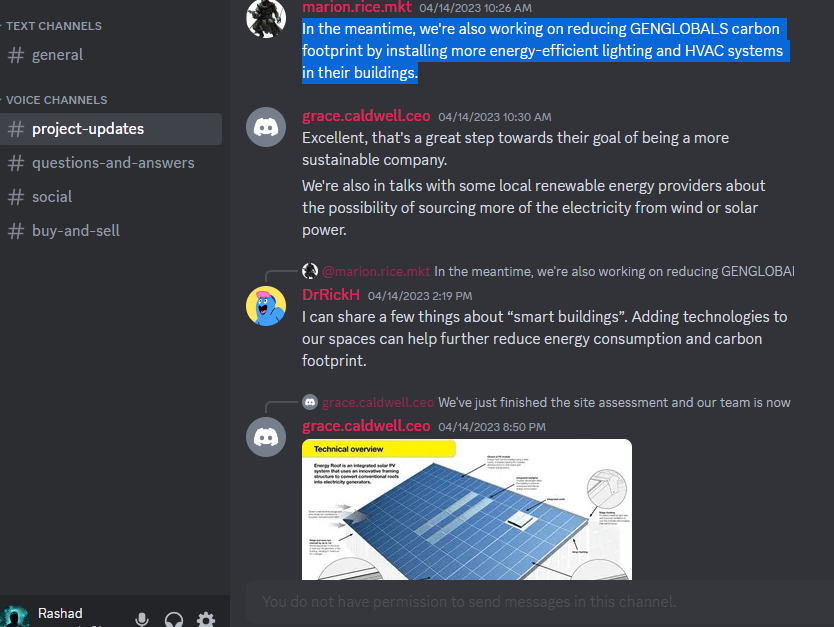


Unnecessary information about hobbies and past institute they attended.

- Threat actors may target this information to identify key decision-makers within the organization. This knowledge can be used for spear-phishing attacks or other social engineering attempts directed at the leadership team.

Insightful Discussions





The company’s website provide a direct link to discord rooms where employees are chating and talking about ongoing projects with detail.This information can be used by threat actor to craft phishing emails or lauch other socail engineer attacks putting employees at risk.

# Vulnerability Scan report

Vulnerabilities found on targets:10.13.26.211, 10.13.30.105, 10.13.30.242, 10.13.31.124. Rated by threat level.

Top five vulnerabilities which could directly be linked to breach and to be addressed immediately below is detailed information on said vulnerabilities.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vulnerability Name** | **Threat**  **Level** | **Vulnerability Description** | **Possible Link to**  **Incident** | **Risk Score** | **Remediations** |
| PHP Unsupported Version Detection | Critical | Outdated/unsecure version of PHP is on the host. | It could be likely that threat actor found this vulnerability after getting a foothold and built a exploit around this weakness. | 10 | Ensure you are using a supported PHP version. Check the PHP official website. |
| Apache 2.4.x < 2.4.56 Multiple Vulnerabilities | critical | Outdated/unsecure  Version of Apache.  all Apache HTTP Server versions up to 2.4.48 are vulnerable if mod proxy is in use | This could be how threat actors gained initial access. | 10 | Keep Apache updated.   * Patch management |
| PHP email header injection | medium | PHP email header injection occurs when attacker manipulates email headers to inject malicious content | Threat actor can make email address appear as if email is from trusted source, tricking recipient and also include malicious attachments, aiming to exploit vulnerabilities | 9 | To prevent ensure that user input is properly validated and sanitized. |
| Nessus syn scan | info | To determine the current state of a communications port, this vulnerability allows an attacker to establish a partial connection with their targe | This scan could have allowed the threat actors to detect an opened port | 7 | -Implement firewalls to block incoming / unknown SYN packets. -Implement Intrusion detection/protection systems |
| Telnet server | medium | telnet is a unsecure virtual communication service, everything transferred is unencrypted | Threat actors could of sniffed on this connection to gain information. | 8 | Use SSH as it provides secure/encrypted connection |

# Risk assessment

## Introduction

The purpose of this report is to present the findings of a risk assessment exercise carried out from December 20th to January 3rd with the scope described below. The main purpose of the exercise was to assess the risks to THISISAFAKECOMPANY and to identify which of these could be accepted and which may need some action to be taken to address them.

Once this risk assessment report has been approved, specific actions will be identified, discussed, agreed and then documented in a risk treatment plan to be managed as part of the Information Security Management System (ISMS).

The process used for this risk assessment is set out in the document Risk Assessment and Treatment Process which is part of the ISMS.

This risk assessment report describes:

* The context and scope of the risk assessment
* The assets within scope
* Threats to, and vulnerabilities of, those assets

This report is input to the risk treatment stage of the process and must be signed off by top management before continuing further.

This risk assessment was carried out by the following people:

|  |  |
| --- | --- |
| **NAME** | **ROLE IN ASSESSMENT** |
| Rashad O Moore | Lead risk assessor |

*Table 1: Risk assessment team*

As part of the assessment, the following additional people were consulted:

|  |  |  |
| --- | --- | --- |
| **NAME** | **TITLE** | **LOCATION** |
| Tyrone Ramos | Chief Imformation Officer | Toronto Canada |
| Maiki Tawfik | HR Manager | Toronto Canada |

## Internal and external context

This Risk assessment is being carried out because on December 5, 2023, at approximately 10:00 AM, their organization's email system was compromised by threat actors who used a vulnerability in the web service plugin to gain access and install malware onto the SMTP servers. This assessment will mitigate some risk, aid in creating response plan and position THISISAFAKECOMPANY to be compliant with the NIST framework.

## Scope

These assess the risk to the hybrid infrastructure polices and procedure, Network infrastructure in reference to critical business software and access control policy to ensure compliance with NIST. Does not cover personal customer data, financial information or intellectual property. May try to manipulate employees into revealing sensitive information to test cyber hygiene.

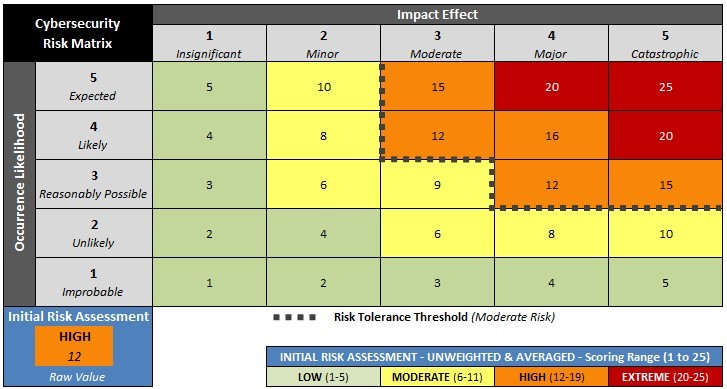
## Risk assessment results summary

A summary of the outcome of the risk assessment is shown in Table 3.1 below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REF** | **ASSET** | **TYPE (P/F/S)** | **THREAT** | **ADDITIONAL COMMENTS** |
| 1 | Physical Locations/Headquarters | P | Thief natural disaster and supply chain | Threat actor could plan heist |
| 2 | Customer Data | F | Data leaks/breach, Data loss and human error | Failure to safe guard this data could ruin reputation and make future business difficult |
| 3 | Money | P/F | Thief, Ransomware and APTs | Bank and other financial info could be stolen |
| 4 | Hybrid infrastructure | P/F | Cyber-attacks, Hardware failure | Should an attacker breach the network infrastructure, they would then have access to the network. Subsequently they’d be able to distribute malware to linked devices, conduct DOS attacks, exfiltrate data and numerous other malicious activities. |
| 5 | Employees/Staff | S | Internal Threats, Social engineering and weak passwords | Threat actor would target employee PI which could lead to them gaining access to the company |

## Risk Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assets | Risk 1 | Risk 2 | Risk 3 | Avg score |
| Physical location | Thief  Likelihood:3  Impact: 3  3x3=9 | Natural disaster  Likelihood: 3  Impact: 4  4x3=12 | Supply chain  Likelihood: 2  Impact: 4  4x2=8 | 29/3=9.2 |
| Hybrid Infrastructure | Cyber attacks  Likelihood: 3  Impact :5  3x5=15 | Hardware failure  Likelihood:4  Impact: 4  4x4=16 | Software bugs  Likelihood: 4  Impact: 4  4x4=16 | 47/3=15.6 |
| Employees | Social engineering Attacks  Likelihood: 4  Impact: 4  4x4=16 | Internal threats  Likelihood: 3  Impact: 5  5x3=15 | Weak passwords  Likelihood: 3  Impact: 4  4x3=12 | 42/3=14 |
| Customer Data | Identity thief  Likelihood: 2  Impact: 4  4x2=8 | Data loss  Likelihood: 1  Impact: 3  1x3=3 | Data leak  Likelihood: 3  Impact: 3  3x3= 9 | 20/3=6.6 |
| Money | Ransomware  Likelihood:2  Impact: 5  2x5=10 | APTs  Likelihood:2  Impact:5  2x5=10 | Thief  Likelihood:1  Impact:3  1x3=3 | 23/3=7.6 |



# Reponse Plan

This plan contains details of protecting the most valueble assest which is the the hybrid infrasturcture assuming threat actor compromised the network with a phishing email containing malicous link spooofed to seem like the CEO sent it. It then installed backdoor to endpoints.

Detection and Analysis – SOC Analyst Responsibility

* Anomaly Detection

-inspect machine learning algorithms to establish a baseline for regular system behavior, so then deviations from baseline behavior would indicate a breach.

-if anomaly appears to be a security incident, conduct digital forensics to determine the root cause. Preserve evidence, examine logs, memory, ad disk images to understand how incident occurred.

* Containment

-Isolate affected systems or network segment to prevent further damage or data exfiltration if it is indeed a security incident.

- Eradication after understanding the incident the next step is to eliminate the root cause of the incident. Removing malware, closing vulnerabilities, or fixing misconfigurations. The goal is to prevent incident from reoccurring.

* Monitoring and Scanning

-Continuously monitor systems, and physical Facilities for unusual or suspicious activity. Use intrusion systems and SIEMs for real time monitoring.

-Regularly scan systems and networks for vulnerabilities, and prioritize them based on severity.

Recovery- CISO and IRT

* Backup Strategy

-Regular and automated backups should be taken of critical data and systems. These backups should be stored in a secure location, both on-site and off-site, to ensure data availability in case of disasters.

-Data recovered should be verified for integrity to ensure it has not been tampered with or corrupted during the incident. Data validation processes are essential to guarantee the reliability of restored data.

* Continuity plan
* Remote work and telecommunicating, establish employees to work remotely, especially during situations that prevent physical access to the workplace, such as natural disasters or pandemics.
* Identify alternative work locations that can be used in case the primary site becomes inaccessible due to cyber or natural disasters.

Follow up and Review- CISO and Cyber analyst

* Documentation and Reporting

-Document all activities and incident details, as well as reporting to management and relevant authorities.

-Any additional information, templates, or references that may be useful during incident recovery

* Lessons learned for Improvement

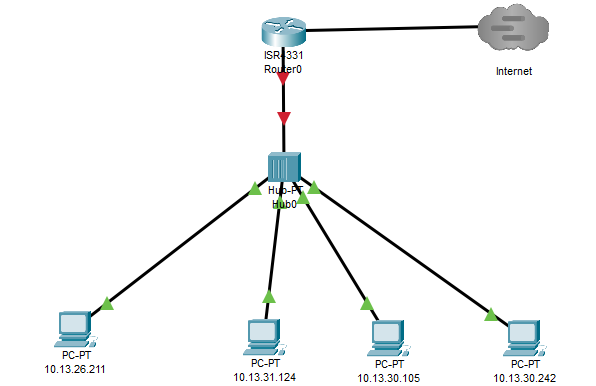
-Collect feedback from incidents, analyze any gaps or shortcomings, and use these insights to refine and improve the response plan

* Updating plan

-Stay current with software updates, security patches, and technology advancements. Implement a robust patch management process to address vulnerability promptly and reduce the risk of exploitation.

-Prioritize patching based on the criticalities of vulnerabilities that could be exploited by attackers.

# Network Architecture



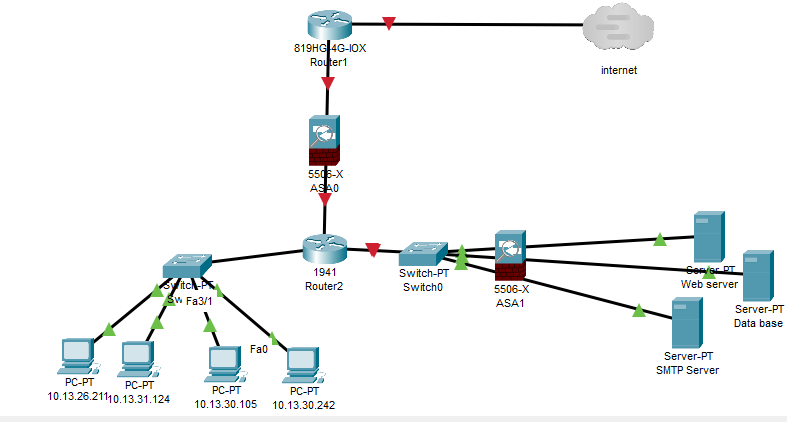
This network is known is a flat network and it is-

More prone to lateral attacks-

Using a flat network leaves you more prone to lateral attacks, which allow attackers togain access to the network through an entry point and then spread throughout the compromised networkwithout opposition.For example, if your organization uses a flat network and malware somehow infects one of your devices, it can quickly move laterally to infect other devices on the network until the entire network is infected.

A way out is to adopt a comprehensive defence-in-depth (DiD) strategy that helps protect your networks from cyberattacks. Network segmentation is a crucial part of a DiD security approach.

# Revised Network



A hierarchical network, where devices are segmented by intermediary hardware like routers, in a flat network, there is no hierarchy or division of a network into layers. When one connected device (A) sends a communication to another device (B), then all ports (we’ll call them X, Y, and Z) connected to the switch forward the exact same broadcast message—except the one that received the broadcast, in this case, device B. Ports X and Y may not need that information, yet they waste precious bandwidth in forwarding the message regardless. This happens because there is no logical segmentation, which restricts the traffic to non-designated devices.

# Firewall rules

Firewall rules are the access control methods firewalls utilize to protect your network from malicious applications and unauthorized access. Essentially, firewall rules govern which types of traffic are allowed and which are refused by your firewall. Refer to the few recommendations below regarding how to configure the firewall for THISISAFAKECOMPANY

Firewall 1- Stateful

* Implement least-privileged access and remove redundant rules
* Regularly review the firewall rules and audit the logs
* Block the following ports: 23 (telnet), 69 (TFTP), 135-139 (NetBIOS), 161 (SNMP), and 445 (SMB)
* Configure application-level control and use monitor mode to test the rules

Firewall 2 – Stateless

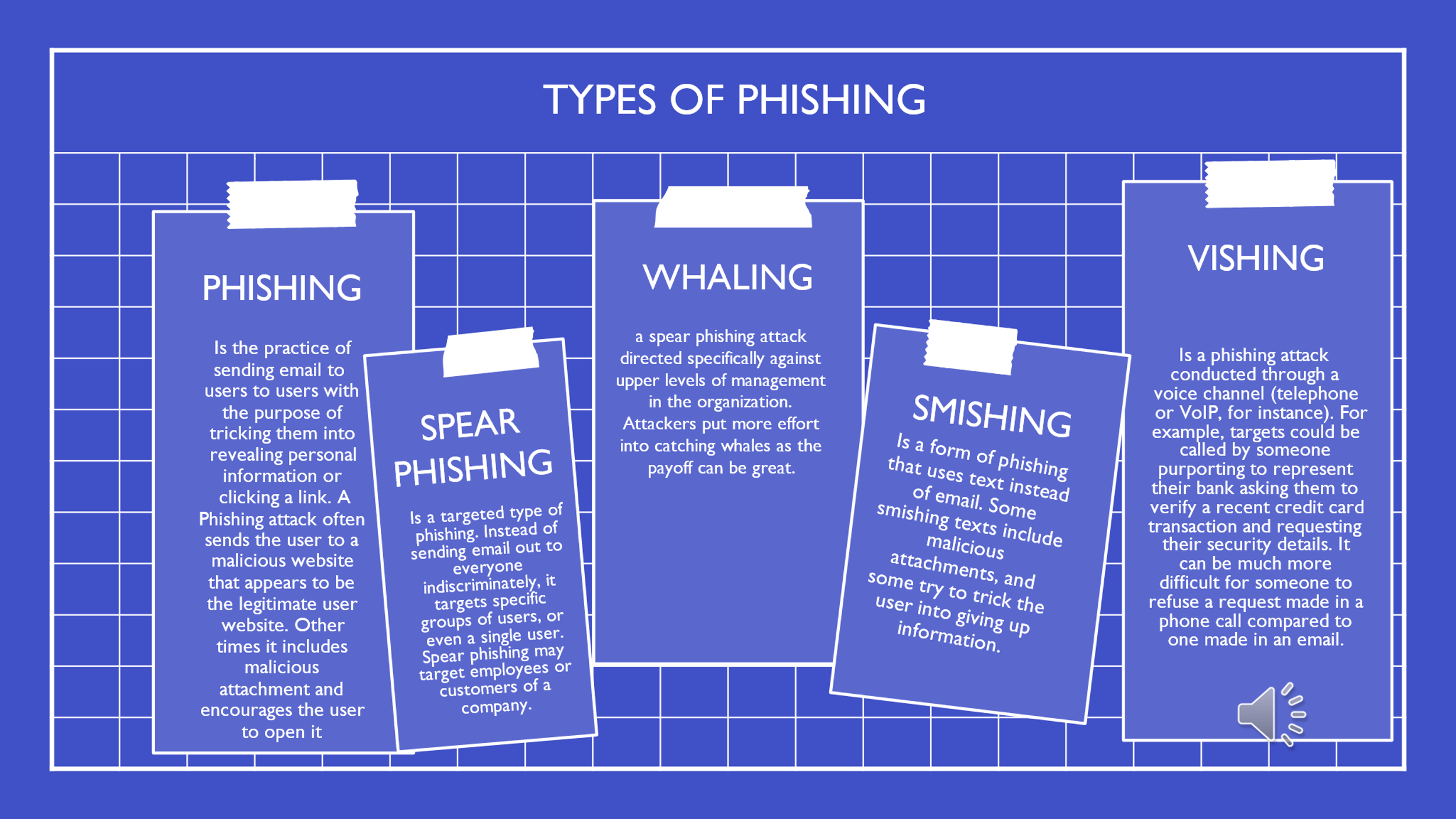
* Implement a deny by default policy and allow only approved traffic
* Monitor traffic

A DMZ firewall is usually part of a DMZ architecture that involves two firewalls: one that protects the DMZ from the Internet, and one that protects the LAN from the DMZ. This way, even if a hacker compromises a system in the DMZ, they still have to bypass another firewall to reach the internal network.

# Training Plan

Cyber hygiene Training for employees

Phishing



Social Engineering

- Social engineering is a type of human hacking that manipulates people into sharing information, downloading software, or making mistakes that compromise their security. Social engineering attacks can use various techniques, such as phishing, baiting, impersonation, pretexting, and water holing, to exploit human psychology and emotions. Social engineering is a major threat to individuals and organizations, as it can bypass many technical security measures and cause significant financial, reputational, or operational damage.

Password management

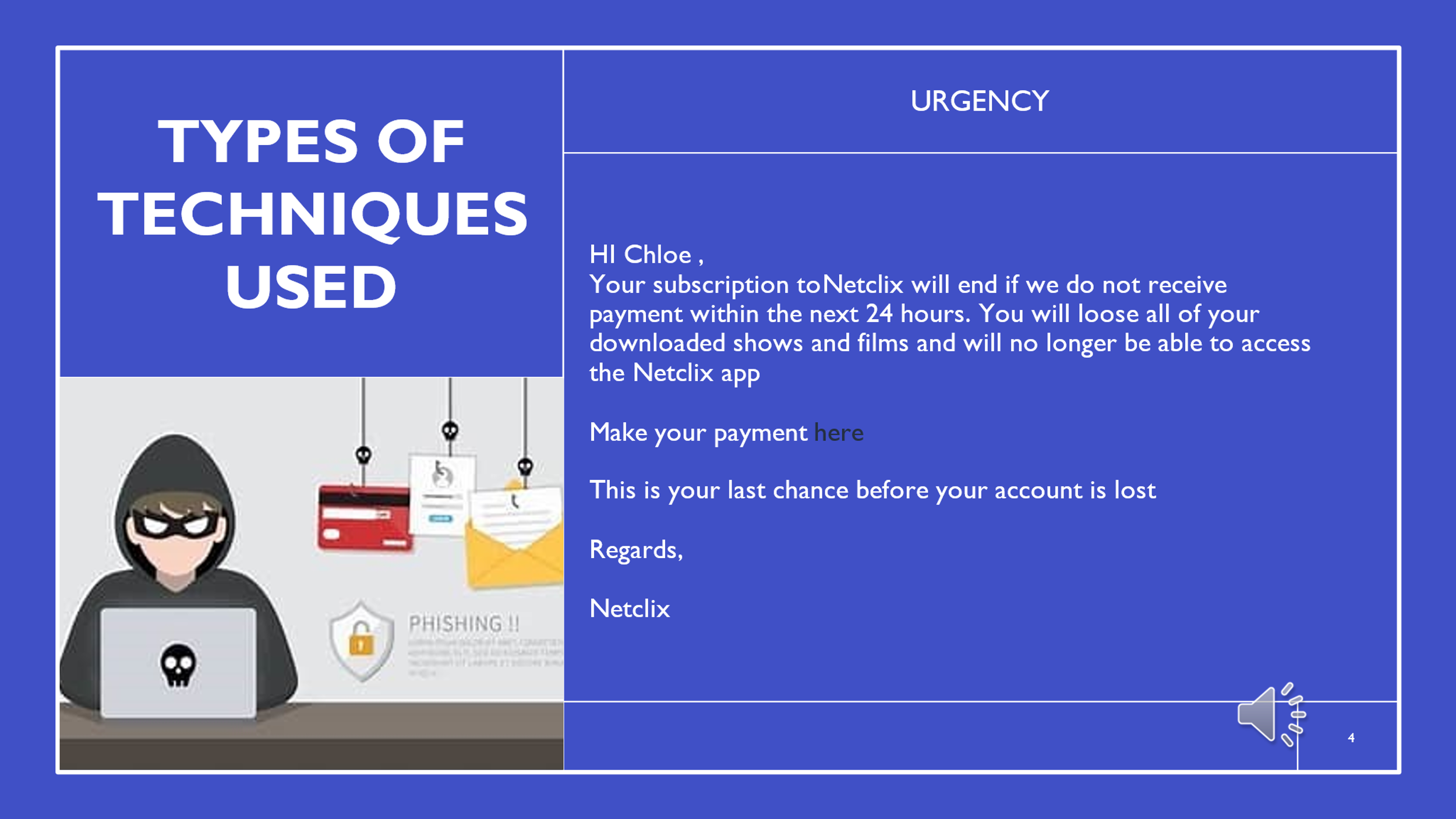
* A minimum and maximum password length, usually between 8 and 16 characters.
* A password complexity requirement, such as using a mix of uppercase and lowercase letters, numbers, and symbols.
* A password history and expiration policy, which prevents users from reusing old passwords or keeping the same password for too long.
* A password lockout policy, which blocks users from logging in after a certain number of failed attempts.
* A multi-factor authentication (MFA) option, which adds an extra layer of security by requiring users to provide another piece of information, such as a code sent to their phone or email, or a biometric scan, to verify their identity

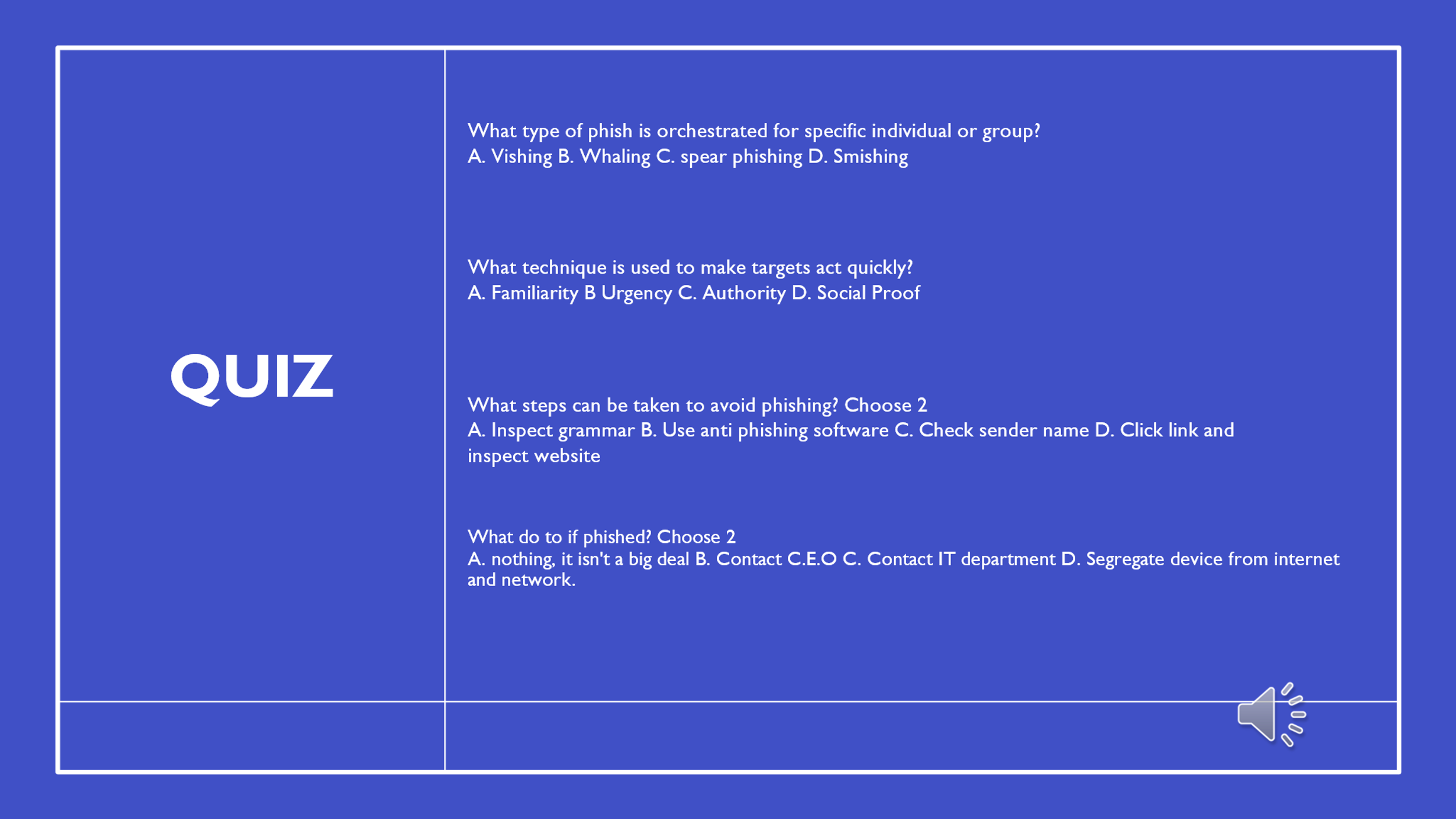
## Phishing Simulation

* Phishing Email Drills

At random times employees will be sent fake phishing emails and be expected to handle and report them appropriately.

Attachments and links accessed within these emails can be tracked when accessed. Reports will be given to department head to inform them on development of cyber hygiene of their employees





Cyber training for IT staff

Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities, training will also help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events.

KPI

-The overall security posture of the organization has improved

-More employees participating in security initiatives.

-Increase in spoofing email detections and reports and less successful phishing attacks

-Significant decrease in passwords/ credentials being compromised and the percentage of staff which follows PM best practices

12-month training outline

Month 1

* Explain types of phishing
* Highlight Different techniques used

Month 2

* Explain Social engineering
* Demonstrate ways to avoid

Month 3

* Understand Password management
* Give examples of good and bad passwords

Month 4

* Demonstrate how email spoofs are used in phishing attacks.
* Know how to identify email spoofs

Month 5 – For IT team

* Containment
* Analysis
* Mitigation
* Recovery

Month 6

* Conduct assessment to test employees
* Highlight and focus in on weaknesses

After Month 6 the first five months will be resume to reenforce knowledge.

Month 12

* Conduct a simulation assessment which will essentially encompasses everything employees have been taught throughout the year, in a real-life scenario. The results will give an idea of how influential or successful the training session was. Employees who do not pass this final assessment will be required to complete another mandatory Training session to be evaluated again in three months.

For sake of company and targeted victims’ employees need to be extremely vigilante and aware to have the required standard of cyber hygiene. The company should also inherit strict polices regarding work operations to enforce keeping environment safe.