TRIANZ℠

Phishing Guidelines

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. OVERVIEW **4**

2. PURPOSE **4**

3. TYPES OF PHISHING **5**

3.1 Spear Phishing: 5

3.2 Whaling: 5

3.3 CLONE PHISHING 6

3.4 VISHING AND SMISHING: 6

3.5 PHARMING 6

3.6 Quishing or QR Phishing 6

4. COMMON PHISHING INDICATORS **7**

5. WHAT TO DO IF YOU SUSPECT A PHISHING ATTEMPT **7**

6. BEST PRACTICES TO PROTECT NETWORK RESOURCES FROM PREVALENT PHISHING THREATS: **8**

1. Overview

Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime. Phishing attacks are a form of social engineering

Phishing is a deceptive tactic where attackers impersonate legitimate entities to steal sensitive information. Recognizing and avoiding phishing attempts is crucial to protect personal and organizational data.

2. Purpose

Phishing guidelines, are essential for safeguarding both individual and organizational security. These guidelines empower employees to recognize and respond appropriately to phishing threats, thereby reducing the risk of data breaches and financial losses

3. Types of Phishing

Common Phishing Attacks:

3.1 Spear Phishing:

Spear phishing emails are sent to a select target, which could be an individual or organization. For example : A spoofed email from the attacker (acting as a vendor) requesting a payment which looks like authentic request

Spear phishing attacks are extremely effective because the attackers spend a lot of time studying the victims and the email sent appear to come from a trusted source. It is the most common phishing on social media websites

3.2 Whaling:

A whaling attack is essentially a spear-phishing attack, but the targets are bigger.

Often targets are companies who conduct wire transfers and have suppliers abroad.

Cybercriminals impersonate senior managers in companies, asserting their authority and thus gaining access to sensitive data or money.

They use the data they find on the internet (and often social media) to trick high-level employees into replying with fraudulent transfers or personal data

3.3 CLONE PHISHING

The attacker creates an almost identical replica of a message previously received by the victims to make them think it is real.

The e-mail is sent from an address similar to the legitimate sender. The only difference is that the attachment or link in the message is exchanged for something malicious. It may claim to be a re-send of the original or an updated version to the original

3.4 VISHING AND SMISHING:

Vishing and smishing are phishing over the phone.

In vishing the victim receives a call with a voice message that looks like a communication from a known institution. It creates a sense of urgency for the user who for this reason provides information, like the PIN of a card.

In smishing malicious text messages are sent to induce users to click on a malicious link or to deliver personal information.

3.5 PHARMING

Some fraudsters are abandoning the idea of “baiting” their victims. Instead, they switched to pharming.

This phishing method exploits the cache poisoning compared to the Domain Name System (DNS), a naming system that the Internet uses to convert the alphabetical names of websites into numeric IP addresses in a way that can identify and then direct visitors to IT services and devices

3.6 Quishing or QR Phishing

Quishing, or QR phishing, is a cybersecurity threat where attackers use malicious QR codes to deceive individuals into visiting harmful websites or downloading malware. When a user scans a QR code, they may be redirected to a site designed to steal sensitive information, such

as passwords or financial data. This method combines the convenience of QR codes with traditional phishing tactics, making it a growing concern in cybersecurity. All Internet communication is to be logged, monitored and audited periodically, for unauthorized access and ensuring availability.

4. Common Phishing Indicators

1. **Generic Greetings**: Phishing emails often use impersonal salutations like "Dear Customer" instead of addressing you by name.
2. **Urgent or Threatening Language**: Messages that create a sense of urgency, such as claiming your account will be suspended unless you act immediately, are common in phishing attempts.
3. **Suspicious Links or Attachments**: Hover over links to check their destination URL. Be wary of unexpected attachments, as they may contain malware.
4. **Unusual Sender Email Addresses**: Phishers often use email addresses that mimic legitimate ones but may have slight variations or misspellings.
5. **Spelling and Grammar Mistakes**: Professional organizations typically proofread their communications. Frequent errors can be a sign of phishing.

5. What to Do if You Suspect a Phishing Attempt

- **Do Not Click on Links or Open Attachments**: If you suspect an email is phishing, avoid interacting with any links or attachments.
- **Report the Incident**: First, do not click on any links within the email or download any attachment.
- Click on the report message feature in the outlook and report those email as phishing. Forward the suspicious email to IS@Trianz.com to examine and determine if legitimate**.**

- Please check and report if you are receiving an email internally with the below message. This may be spoofed externally but the sender email may look genuine like how you receive internally. [Note: All Internal mails are labelled with green ribbon and external mails with Red Ribbon]
- [EXTERNAL EMAIL] DO NOT CLICK links or attachments or DO NOT reply unless you recognize the sender and know the content is safe.**

6. Best practices to protect network resources from prevalent phishing threats:

- **Verify the Source**: If you receive an unexpected email, contact the organization directly using known contact information to verify its legitimacy.
- **Be Cautious with Personal Information**: Avoid providing sensitive information like passwords or credit card numbers in response to unsolicited requests.
- **Use Security Software**: Keep your antivirus and anti-malware software up to date to help detect and block phishing attempts.
- **Educate Yourself and Others**: Regularly update your knowledge about phishing tactics and share this information with others to raise awareness.
- **User phishing awareness training:** Implement a standard anti-phishing training program and require employees to review phishing training material annually.
- CLEAR program evolution with a training check that certifies that the employee has retained all the information outlined in the training program.
- **Identify network phishing vulnerabilities:**
- **Enable MFA:** Activating a strong MFA is the best way that small businesses can protect their internet facing business accounts from phishing related threats.
- **Implement strong password policies to authenticate users.** These passwords must adhere to a password strength policy which requires minimum character length, numbers, special characters, and case sensitivity, along with prohibiting users from recycling previously used passwords.
- **Implement DNS filtering or firewall** denylists to block known malicious sites.

- **Implement anti-virus solutions** to mitigate malware and to stop malware from executing if a malicious hyperlink or attachment from an email is opened.
- **Implement file restriction policies that prevent malicious high risk file extensions** e.g., .exe or .scr from being downloaded and executed. These types of files are unnecessary for daily operations and should be heavily restricted on standard business accounts.
- **Mandatory Training:** All associates mandatorily need to attend training conducted by Infosec and IS Team
- **Simulation Test:** All associates need to participate in Simulation Tests enabled by IS team
- **Mandatory Training:** All associates mandatorily need to attend training conducted by Infosec and IS Team
- **Simulation Test:** All associates are required to participate in simulation tests administered by the IS team, which are designed to help them better recognize and respond to phishing threats in realistic, hands-on scenarios.

Document Control

Owner:	Management Representative	**Release ID:**	PHIS-GUID-0080

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Author	Reviewer	Approver	Date	Reason for Change	Change Description
0.1	Vijaya Rajeswari	Balu, Pranesh & Siva		6-Jun-2025	Initial Review	• None
1.0	Vijaya Rajeswari	Balu, Pranesh & Siva	Srikanth Mantena	28-Aug-2025	For Approval	• Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com

The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.