Phishing
Materials




Overview

- Introduction
- Common features of phishing emails
- How to identify phishing emails
- How to respond to phishing emails
- Technological protection measures
- Case Study

Introduction

Types of phishing

- For example: email phishing, SMS phishing, voice phishing, spear phishing, etc.

Definition of Phishing Email

- It disguises itself as information from a trusted entity, tricking victims into clicking malicious links, downloading attachments, or providing sensitive information, which may lead to the disclosure of victims' personal privacy and company secrets, the theft of bank accounts, credit card information, etc., and cause direct financial losses.

Characteristics of phishing emails

Sender forgery

The sender address may look like a legitimate company, but may actually be slightly different.
Example: support@bank.com may be disguised as support@bank-secure.com.

Characteristics of phishing emails

Urgency

Urgent language is often used in emails to make the recipient feel that they must take immediate action, for example:
- "Your account will be frozen!"
- "Click now to prevent data loss!"

Unusual links and attachments

Messages containing irrelevant or unusual links or attachments that may lead to malicious websites or download viruses.

Common bait

Winning notice, Discount promotion, Financial warning, Unusual account activity, etc., trying to attract recipients to click.

How to identify phishing emails

Check the sender address

Don't just look at the sender name, check the full email address to see if there are any typos or unusual domain names.

Hover to check links

Before clicking on a link in an email, hover your mouse over it to see where it actually leads to, to make sure it leads to a trusted website.

Avoid opening suspicious attachments.

Be extra cautious with email attachments from unknown sources, especially compressed files, executable files, or document files.

Be suspicious of urgent requests

Most legitimate companies will not ask for passwords or other sensitive information immediately via email.

How to respond to phishing emails

Do not click on links or download attachments.

If you receive an email that looks suspicious, do not click on links or download attachments until you verify their authenticity.

Contact the sender directly

If you receive an urgent email from a bank, company, or other organization, confirm it using the official contact information on the website instead of replying to the email.

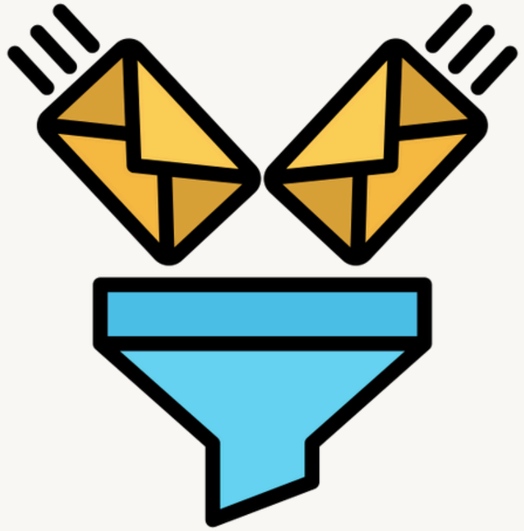
Report suspicious emails

Enterprises should set up a dedicated IT or security team, and employees should report suspicious emails immediately to help the organization prevent larger scale attacks.

Technological protection measures

Enable spam filters.

Use your corporate email system's anti-spam and phishing filtering features to reduce the amount of malicious emails you receive.



Enable two-factor authentication (2FA).

In addition to your password, enabling two-factor authentication (such as SMS, authentication apps) can add an extra layer of protection even if your password is stolen.

Update systems and software in a timely manner.

Regularly update operating systems, browsers, office software, and antivirus software to ensure they have the latest security patches and reduce the risk of being attacked due to vulnerabilities.

Case Study

Classic Phishing Email Case

Content:
Analyze well-known phishing attack cases to show how attackers carry out attacks and how companies are invaded.

Case 1: Phishing incident of a well-known company
The attacker sent an email impersonating the company's IT department, asking employees to change their login credentials.
The employees changed their credentials after believing the email, resulting in a large number of company accounts being stolen, posing serious security risks.

Video

1.https://www.youtube.com/watch?v=Y7zNlEMDmI4

2.https://www.youtube.com/watch?v=Ex00XJnKHh4&list=PLG3zFBI_Jy2nusVjUJKYyjrqtzmCTHqNU

3.https://www.youtube.com/watch?v=H4bLUpdFDYo

4.https://www.youtube.com/watch?v=o0btqyGWIQw

5.https://www.youtube.com/watch?v=gSQgbCo6PAg

6. https://www.youtube.com/watch?v=Yz0PnAkeRiI