

PHISHING AWARENESS PRESENTATION



AGENDA

Familiarize Yourself with Phishing

What is Phishing?

**Learn To Spot Phishing
Emails**

**How do we stop getting
phished?**

What is Phishing?

- Impersonating legitimate organizations to deceive individuals into providing sensitive information
- Executed through deceptive emails or messages

Phishing is a form of cybercrime where impersonate legitimate organizations to deceive individuals into providing sensitive information, such as passwords or credit card numbers.

The term "phishing" plays on the idea of fishing for personal data, using bait to lure victims. Understanding the context and history of phishing helps highlight its evolution, from simple email scams to sophisticated, targeted attacks.



The Problem

Learn to spot Phishing emails

Identifying phishing emails is vital for protection. Look for signs such as unfamiliar sender addresses, generic greetings, and poor grammar. Phishing emails often contain urgent requests, prompting quick action without proper consideration. Additionally, hovering over links can reveal misleading URLs, exposing the true destination.

Security vulnerabilities, inefficiencies, and lost revenue

Example structure of a Phishing Email:

This is one example of an improved phishing email. There are many different ways you could have done this.

Spelling of Mastercard fixed and email comes from a relatable address

From: Mastercard Staff Rewards
To: employee@email.com
Subject: Your Black Friday Employee reward card

Body: Hello <name>.

Email is personalized and poor grammar is fixed

Contextualize to upcoming Black Friday event

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming Black Friday sales as a small token of our appreciation. Please find attached your Employee reward card.

Link is masked in plaintext to hide phishing link

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit [here](#).

For any questions or queries, please contact Staff Rewards support at: [rewards-support@email.com](#)

To increase legitimacy, buffer text is added

From, Staff Reward Services

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Simple confidentiality disclaimer to add legitimacy to email. This was taken from an article on Exclaimer.com

THE SOLUTION

How do we stop getting Phished

Preventative measures are essential in combating phishing. Utilizing email filters and security software can significantly reduce the chances of phishing attempts reaching your inbox. Implementing multi-factor authentication (MFA) adds an extra layer of security, making it harder for attackers to gain access even if they obtain your password. Regular training and awareness programs are crucial in keeping everyone informed about the latest phishing tactics.

Security vulnerabilities, inefficiencies, and lost revenue

02

Rapid pace of technological change

Response to Phishing Attacks

If you suspect a phishing attempt, it's critical to act quickly. Do not click on links or download attachments from suspicious emails. Report the incident to your IT or security team immediately. If you have fallen victim to a phishing attack, change your passwords and monitor your accounts for any unauthorized activity. Taking swift action can mitigate potential damage.

Security vulnerabilities, inefficiencies, and lost revenue

Rapid pace of technological change

03

Conclusion

In conclusion, staying informed about phishing is essential in today's digital landscape. By recognizing the signs, implementing preventive measures, and knowing how to respond, we can protect ourselves and our organizations from potential threats. Continuous education and vigilance are key to combating phishing attacks.



The background features several light gray squares of varying sizes scattered across the slide. A cluster of four squares is in the top right, another cluster of three is in the bottom left, and a single square is in the bottom right. There are also some overlapping squares on the left side.

Q&A

Thank You

Thank you for your time. We believe Arowwai is poised for significant growth and ready to make a substantial impact .

We invite you to join us on this exciting journey.