HASHOM.

HASHOM PHISHING AWARENESS CAMPAIGN

Empowering Employees to Defend AgainstCampaign: Cyber Threats

INTRODUCTION TO HASHOM:

- Problem statement:

Phishing attacks are a leading cause of data breaches, exploiting employees' lack of awareness. The challenge is to create continuous and engaging phishing awareness campaigns that educate employees on recognizing and responding to phishing attempts in real time."

- Introduction:

Hashom empowers organizations against phishing threats through education, awareness, and security solutions, providing interactive training, real-time simulations, and tools to foster a cybersecurity-conscious workplace.

- Why Phishing Awareness is Crucial:

1. Growing Cyber Threats
2. Financial & Data Loss
3. Human Error Exploitation
4. Business Continuity Risks
5. Compliance & Legal Consequences
6. Strengthening Cyber Hygiene

- Objectives of the Awareness Campaign:

1. Educate Employees
2. Enhance Cybersecurity
3. Simulate Real-World Attacks
4. Reduce Security Risks
5. Ensure Compliance
6. Strengthen Incident Reporting

WHAT IS PHISHING:

Phishing is a type of cyberattack where attackers impersonate legitimate entities such as banks, companies, or government organizations to deceive individuals into providing sensitive information like passwords, financial details, or personal data. These attacks often occur via email, phone calls, or fake websites and can lead to identity theft, financial loss, or unauthorized access to systems. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), over 90% of successful cyberattacks start with a phishing email. Similarly, Deloitte reports that 91% of all cyberattacks begin with a phishing email to an unsuspecting victim

Common Phishing Methods

- Email Phishing – Fake emails pretending to be from legitimate organizations.
- Spear Phishing – Targeted attacks on specific individuals or organizations.
- Whaling – High-level phishing attacks aimed at executives or senior management.
- Vishing (Voice Phishing) – Phone scams impersonating banks or tech support.
- Smishing (SMS Phishing) – Fraudulent text messages with malicious links.

How Phishing Attacks Work

1. Bait (Deceptive Message) – The attacker sends a fraudulent email, text, or message pretending to be from a trusted source.
2. Lure (Creating Urgency or Fear) – The message often creates a sense of urgency, such as claiming suspicious activity on an account or offering a too-good-to-be-true reward.
3. Hook (Malicious Link or Attachment) – The victim is encouraged to click on a link leading to a fake website or download an attachment containing malware.
4. Data Theft (Credential Harvesting) – If the victim enters their information on the fake website, the attacker captures sensitive details like usernames, passwords, and banking credentials.
5. Exploitation (Unauthorized Access or Fraud) – The attacker uses the stolen information to gain unauthorized access to accounts, commit fraud, or launch further cyberattacks.

HASHOM.

HASHOM.

CONTACT US

Nikunj Pandey: 9321554553

Om Joshi : 9326560402

Yash Patkar : 9757226482

Jay Sharma: 9321743683

Arowwai Industries

THANK YOU!

FOR YOUR ATTENTION