CodeAlpha

PHISHING ATTACKS

BY: MOURAD EL OUATIK

CodeAlpha

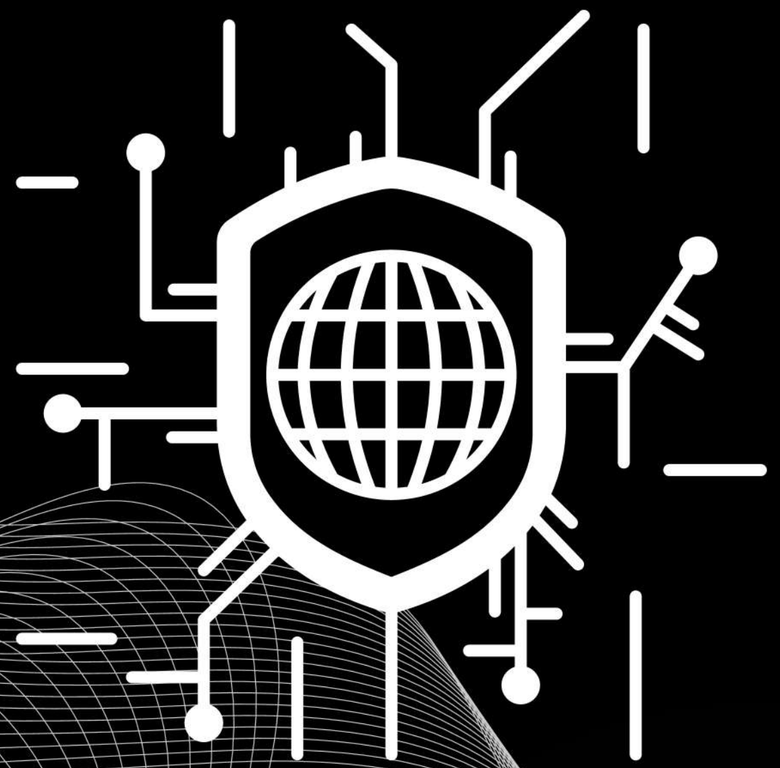
INDEX:

- INTRODUCTION
- WHAT ARE PHISHING ATTACKS
- GOALS OF PHISHING ATTACKS
- THE NECESSARY SKILLS.
- HOW TO AVOID PHISHING ATTACKS:
-
- HAVE BEEN YOU PWNED ?

CodeAlpha

INTRODUCTION:

In cybersecurity, we're trying very hard to keep information safe from attackers, often referred to as the 'Black Hat Team.' These attackers use various methods to access your information, which we call attacks. One of the most well-known and commonly used attacks are phishing attacks



CodeAlpha

WHAT ARE PHISHING ATTACKS?

Phishing attacks are a form of cybercrime where malicious actors try to deceive individuals into revealing sensitive information, such as usernames, passwords, credit card numbers, or other personal details. These attacks typically involve fraudulent emails, messages, or websites that mimic legitimate entities, such as banks, social media platforms, or reputable companies.

So what are the goals of these attacks ?

CodeAlpha

GOALS OF PHISHING ATTACKS:

Phishing attacks aim to trick victims into thinking they're dealing with a legitimate entity, so they willingly share sensitive information. Attackers then use this information for identity theft, financial fraud, or unauthorized system access.

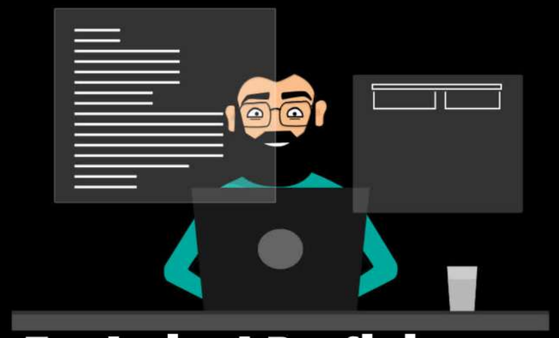
Attackers take a long time to collect the necessary data to access your information, and they combine various skills to succeed in these attacks. What are those skills ?

CodeAlpha

THE NECESSARY SKILLS:

CodeAlpha

Social Engineering



Technical Proficiency

Research skills

communication skills

Psychological Insight

Deception Techniques

SOCIAL ENGINEERING:

Social engineering is a manipulation technique that exploits human psychology to gain access to confidential information, systems, or valuables.

For example, an attacker might pose as a trusted entity, like a bank or IT support, to convince someone to reveal their passwords or other personal details.

There are some books to master the social engineering tools like **“L'Art de la supercherie”** a book of **Kevin Mitnick et William L. Simon**

TECHNICAL PROFICIENCY

Technical proficiency, also known as technical skills or hard skills, refers to the knowledge and abilities required to perform specific tasks related to technology, machinery, or specialized fields.

Attackers use their technical skills to design emails and websites that closely mimic legitimate ones. This involves understanding HTML, CSS, and JavaScript to create realistic-looking interfaces.

RESEARCH SKILLS:

to crafting convincing messages that prompt victims to act. Research skills are crucial for phishing attackers.

Attackers use various resources to gather information about their targets, including social media and frequently visited websites. This provides them with enough information to set up an appropriate trap.

COMMUNICATION SKILLS:

Communication skills are important in phishing attacks because they enable attackers to craft convincing messages that deceive their targets. Here are some key roles these skills play:

- **Emails and Texts**
- **Voice Phishing (Vishing)**
- **Impersonation**
- **Scenarios**

EMAILS AND TEXTS:

Attackers use language that creates a sense of urgency or fear, prompting targets to act quickly without thinking critically. Phrases like “Your account will be locked” or “Immediate action required” are common

Click on the photo to returne to the main page

VOICE PHISHING (VISHING)

Effective communication skills are essential for attackers to sound convincing over the phone, often posing as customer service representatives or technical support.

Click on the photo to returne to the main page

IMPERSONATION

Attackers often impersonate trusted figures or organizations. Good communication skills help them convincingly adopt the language and mannerisms of these entities. And guess what, Artificial Intelligence has made this mission much easier by simulating someone's voice or even their appearance. Not all targets are able to differentiate between the attacker and the real person

Click on the photo to returne to the main page

SCENARIOS:

attackers crafte believable scenarios that require immediate attention, such as security alerts or urgent requests for information, relies heavily on effective communication1.

Click on the photo to returne to the main page

CodeAlpha

HOW TO AVOID PHISHING ATTACKS:

BE SKEPTICAL OF UNEXPECTED EMAILS OR MESSAGES:

Question It:
If you receive an unexpected email or text message, especially from a company or organization, pause and verify its legitimacy.

Examine It:
Look for signs of phishing, such as generic greetings, urgent requests, or misspelled words.

DON’T CLICK ON SUSPICIOUS LINKS:

Hover First:
Hover your mouse over any link in an email to see where it leads. If it looks suspicious, don’t click on it.

Avoid Pop-Ups:
Be cautious of pop-ups that ask for personal information or claim you’ve won something.

USE SECURITY SOFTWARE:

Install Antivirus:
Use reliable antivirus software to protect against malware and phishing attempts.

Enable Spam Filters:
Set up spam filters in your email client to keep phishing emails out of your inbox

SECURE YOUR ACCOUNTS.

Avoid Public Wi-Fi:
Don’t access sensitive accounts or provide personal information over public Wi-Fi networks

Strong Passwords:
Use unique, strong passwords for each account. Enable two-factor authentication (2FA) wherever possible, and change your passwords after a while of using them

EDUCATE YOURSELF AND OTHERS:

Security Awareness Training: Stay informed about common phishing tactics and educate family members and colleagues.

Report Suspicious Emails: If you receive a phishing email, report it to your email provider or organization.

CodeAlpha

HAVE BEEN YOU PWNED ?

There is a web site that checks if your passwords or emails are mentionned in a phshing raport or had been sold somewhere, you can check it by clicking on the link bellow:

Have I Been Pwned

CodeAlpha

CONCLUSION:

Phishing attacks are really da
ngerous when it comes to protecting information, but they require a lot of time and effort to set up. An attacker could spend weeks or even months preparing for a single attack.

Despite this hard work, there is a high probability that the target is aware of phishing attacks, which threatens the success of the attack. So, if you have completed this presentation, don’t worry you are secure enough to avoid these attacks

CodeAlpha

THANK YOU

MOURAD EL OUATIK