FAMILIARIZE YOURSELF WITH PHISHING ATTACKS

AGENDA

WHAT IS PHISHING

TYPES OF PHISHING

HOW TO SPOT PHISHING

HOW TO PROTECT YOURSELF

WHAT IS PHISHING

Phishing is a type of cybercrime where attackers act as legitimate entities to trick victims into revealing sensitive information such as passwords, credit card details, or social security numbers.

COMMON TYPES OF PHISHING ATTACKS

- **Email phishing:** The most common type, involving fraudulent emails.
- **Spear phishing:** Targeted attacks on specific individuals or organizations.
- **Whaling:** Attacks aimed at high-profile targets like executives and CEOs.
- **Smishing:** Phishing via SMS text messages.
- **Vishing**: Voice phishing using phone calls.
- **Search engine phishing:** Creating fake websites to appear in search results.
- **Social media phishing**: Using social platforms to spread scams.

HOW TO RECOGNIZE PHISHING ATTEMPT

Be on the lookout for these red flags:

1. Carefully examine sender email addresses for slight misspellings.
2. Creating a sense of urgency or fear
3. Look for grammatical errors or odd phrasing
4. Hover over links before clicking to reveal the true destination. Ensure the link is at least **https** and not **http.**
5. Be cautious of unexpected attachments
6. Offering deals that seem “too good to be true”. For example click this link for Prizes.

HOW TO PROTECT YOURSELF

- Use robust email filters and spam protection to automatically detect known spammers
- Install anti-phishing browser extensions
- Enable two-factor authentication on all accounts
- Update security software regularly
- Never click on suspicious links
- Don't download unexpected attachments
- Be cautious about sharing personal information online

THANK YOU