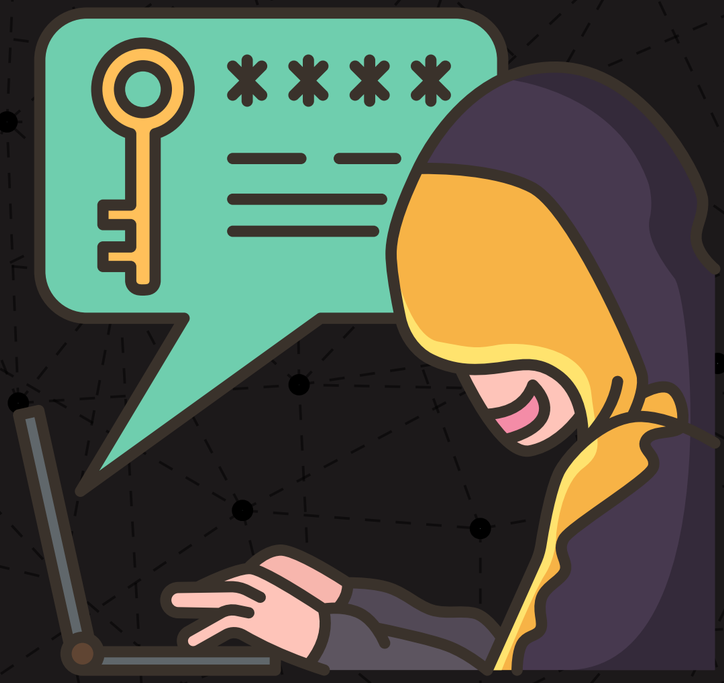
CYBERSECURITY THREAT

PHISHING ATTACKS

Think Before You Click!



WHAT IS PHISHING?

Phishing is when someone tries to trick you into revealing personal information like your password, credit card numbers, or social security number.

Phishing can happen through emails, text messages, or other online platforms.

Canva.com

AFFECTED INFORMATION

PERSONAL AND CORPORATE EMAIL ACCOUNTS

ONLINE BANKING

SENSITIVE DATA REPOSITORIES

MODUS OPERANDI OF THE THREAT

Phishing attacks typically involve fraudulent attempts to obtain sensitive information, such as usernames, passwords, and financial details. Attackers often send deceptive emails or messages that appear to be from a trustworthy source, tricking individuals into revealing confidential information.

THREAT ACTORS

The level of sophistication can vary, with some attacks being relatively simple and others employing advanced techniques.

01 CYBERCRIMINALS

02 ORGANIZED CRIME GROUPS

03 STATE-SPONSORED ACTORS

RELATED PROTECTION MEASURES

1. **User Education**
   Training individuals to recognize phishing attempts and avoid clicking on suspicious links or providing sensitive information.

2. **Email Filtering**
   Implementing advanced email filtering systems to detect and block phishing emails before they reach the inbox.

3. **Multi-Factor Authentication (MFA)** Enabling MFA adds an extra layer of security, even if credentials are compromised.

4. **Regular Security Audits**
   Conducting routine security audits to identify vulnerabilities and improve overall cybersecurity posture.

5. **Up-to-Date Software**
   Keeping software, especially security software and email systems, up to date to patch known vulnerabilities.

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING

Don't share your personal information online!