Digital Defense 101.

Protecting Yourself Against Cyber Threats.

Presented By: Huzaifa Abbasi

Roll Number : 23-Ai-21

Contents.

Introduction

- Digital technologies have revolutionized the way we work and communicate, but they've also brought about new challenges.
- Today, we'll delve into the essentials of Digital Defense - safeguarding against cyber threats like phishing, malware, and ransomware.
- In this presentation, we'll explore what these threats are, how they operate.
- how to protect ourselves and our organizations from falling victim to them.

What is Phishing?

- Definition:
- Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.
- Often comes through emails, text messages, or social media posts that appear to be from legitimate sources.

How to Identify Phishing?

- Phishing attempts can be subtle, but by being vigilant, you can spot and avoid falling victim to them.

➢ Here are some key indicators:

- Suspicious Email Addresses:
- Spelling and Grammar:
- Attachments and Links:
- Employee Training:
- Enhances Awareness.

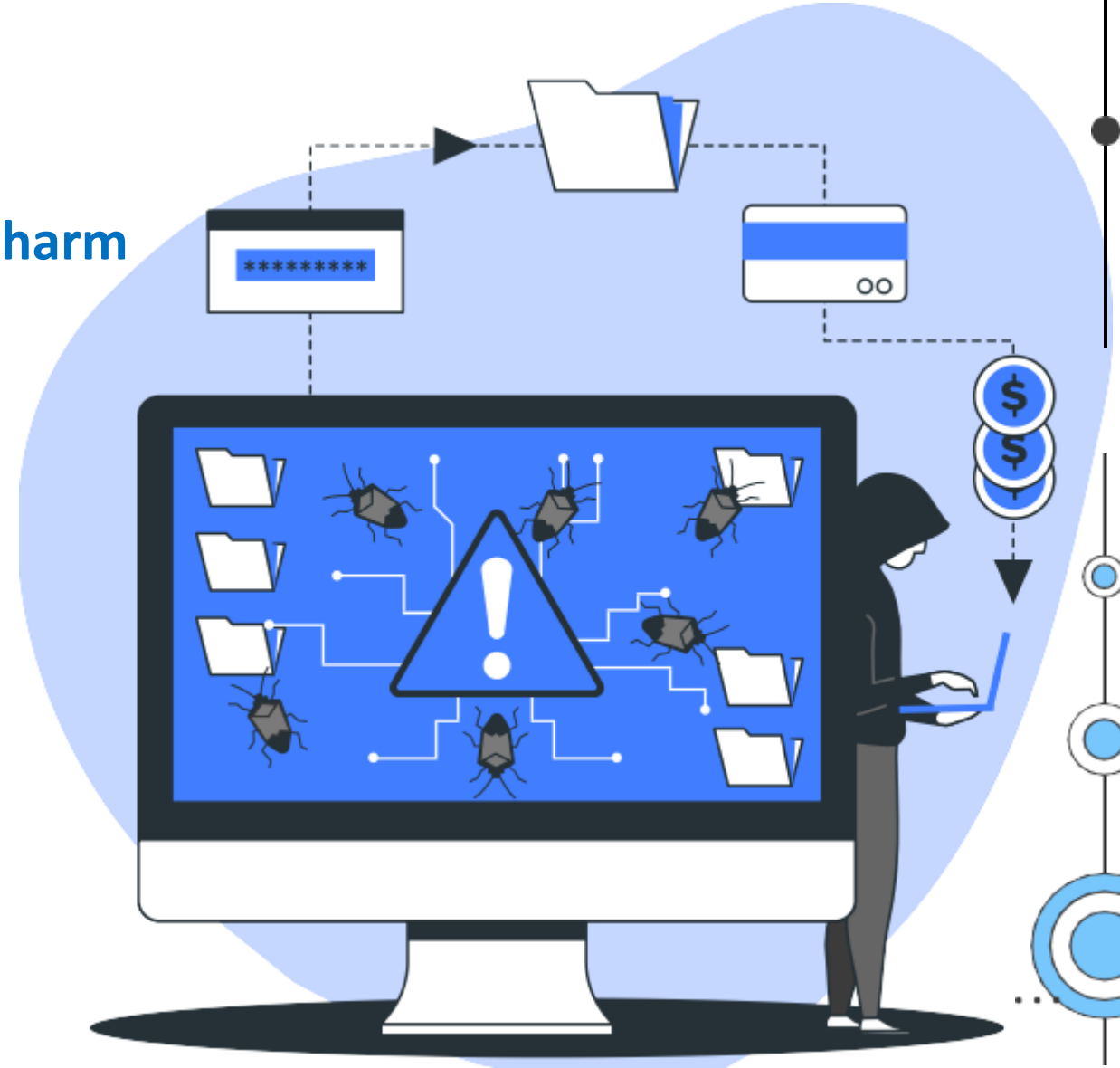
What is Malware?

- **Definition:**

Malicious software designed to harm or exploit computer systems.

- **Types:**

Viruses, Trojans, Spyware, etc.



How Malware Spreads?

- Opening infected email attachments.
- Visiting malicious websites.
- Downloading files from untrusted sources.
- Keeping software and systems outdated.

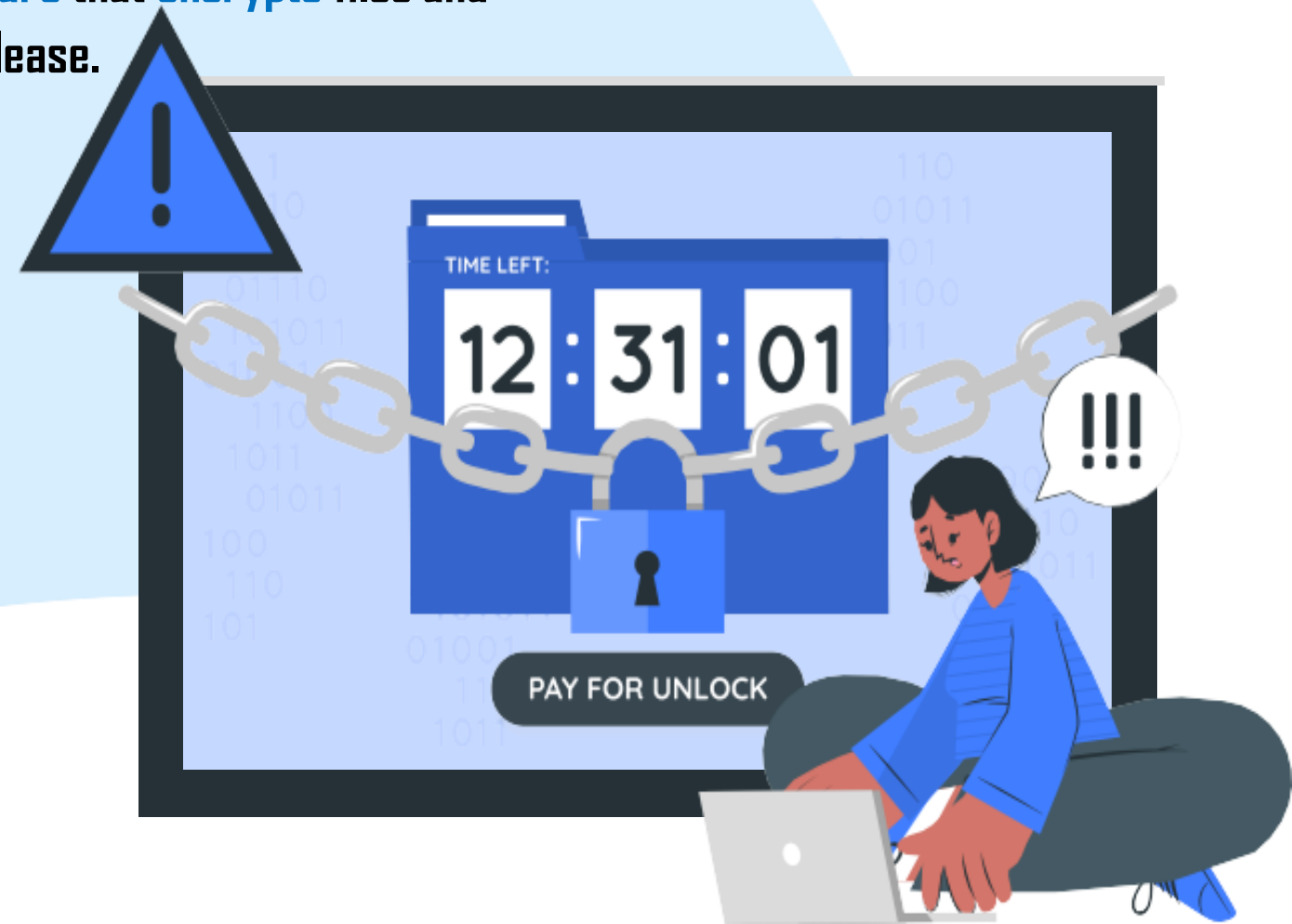
Malware Prevention

- Install reputable antivirus software.
- Regularly update operating systems and software.
- Educate employees on safe internet practices.

What is Ransomware?

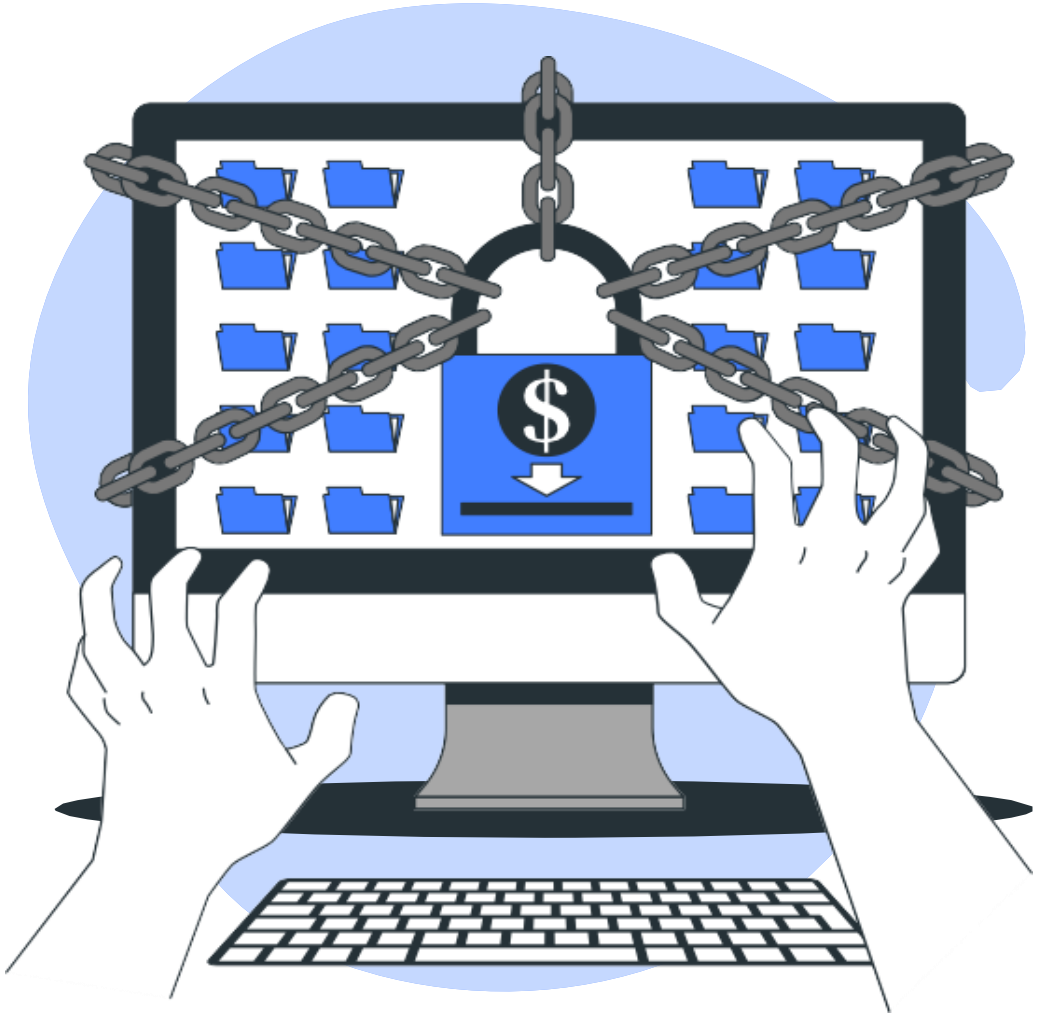
Definition:

Ransomware is a type of malware that encrypts files and demands payment for their release.



How Ransomware Works?

- Infiltration through malicious links or attachments.
- Encryption of files and demand for ransom.
- Consequences of not paying the ransom.



Ransomware Precautions.

- Regularly backup important files
- Be cautious with email attachments and links
- Keep software updated
- Train employees on ransomware awareness

Digital Defense Best Practices

- ✓ Use strong, unique passwords.
- ✓ Enable two-factor authentication.
- ✓ Conduct regular security audits.
- ✓ Implement a cyber security policy.

Conclusion.

- Cyber security is everyone's responsibility.
- By being aware of the threats and taking precautions, you can protect yourself from phishing, malware, and ransomware.

THANKS!

Do you have any questions?