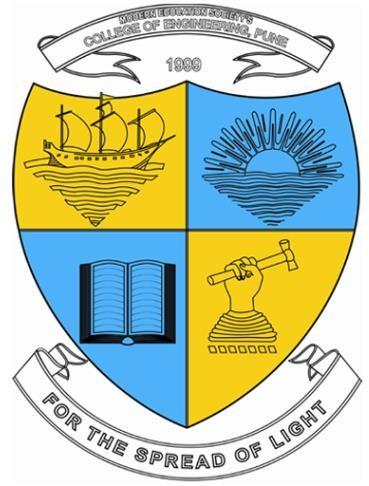
# Savitribai Phule Pune University

**Modern Education Society’s Wadia College of Engineering, Pune**

19, Bund Garden, V.K. Joag Path, Pune – 411001.

**ACCREDITED BY NAAC WITH “A++” GRADE**

**DEPARTMENT OF COMPUTER ENGINEERING**



A REPORT ON

**Case Study of Social Engineering Threat (“I love You” worm)**

## B.E. (COMPUTER)

*SUBMITTED BY*

Ms. Mugdha Arvind

Ms. Megha

Mr. Aryan Chogale

Mr. Sarthak Jadhav

**DEFINITION:**

Social engineering is a technique used by cybercriminals to manipulate people into revealing confidential information or performing actions that may compromise security.

### ISSUE:

# The main issue with social engineering is that it exploits human psychology rather than technical vulnerabilities. It relies on deception and manipulation to gain unauthorized access to systems, data, or physical locations..

### LOSSES THAT CAN HAPPEN:

### Social engineering can lead to significant losses including

* Financial Losses
* Confidentiality losses
* Trust Losses
* Reputational damage
* Operational disruptions
* Security Losses

### PREVENTING MEASURE:

### Awareness and Training: Educate employees and individuals about common social engineering tactics and how to recognize them. Regular training sessions and updates are crucial.

### Strict Policies and Procedures: Implement and enforce strong security policies and procedures that govern access to sensitive information and systems. This includes protocols for verifying identities and handling requests for information.

### Verification and Authentication: Always verify the identity of individuals requesting sensitive information or access, especially if the request is unexpected or unusual.

### Use of Technology: Employ technological solutions such as multi-factor authentication (MFA), encryption, and intrusion detection systems to bolster security and detect suspicious activities.

### Incident Response Planning: Have a well-defined incident response plan in place to quickly address and mitigate the impact of social engineering attacks if they occur.

### Limit Information Sharing: Minimize the amount of sensitive information publicly available and ensure that internal information is shared on a need-to-know basis.

By combining these prevention methods, organizations and individuals can significantly reduce the risk posed by social engineering threats.

### CASE STUDY:

### 

The “I Love You” worm, also known as the Love Letter worm or Love Bug, was a malicious self-replicating computer program that spread via email. It was released on May 4, 2000, and within hours had caused extensive damage across the globe. Originating in the Philippines, the worm infected millions of computers, making it one of the most destructive malware incidents in history.

Attack Vector

* Email Propagation: The worm spread through an email with the subject line “ILOVEYOU” and an attachment named “LOVE-LETTER-FOR-YOU.txt.vbs”. The “.vbs” extension indicated a Visual Basic Script file, which contained the malicious code.
* Social Engineering: The subject line and the attachment name were designed to entice recipients to open the email and run the script, exploiting human curiosity and the desire for love and attention.
* Self-Replication: Once the attachment was opened, the script would execute and perform several malicious activities:

It would send copies of itself to all contacts in the user’s Microsoft Outlook address book.

It would overwrite files on the infected computer, including important documents and media files, replacing their content with copies of itself.

It would modify registry keys to ensure it ran each time the system started.

**YEAR:**

2000

**ORIGIN:**

Philippines

### LOSS HAPPENED:

* Global Infection: The worm spread rapidly, infecting an estimated 10% of the world’s internet-connected computers within the first few days.
* Data Destruction: The worm overwrote various file types, including JPEG images, MP3 audio files, and other documents, making them unusable.
* Financial Damage: The financial impact was massive, with estimates of the total damage ranging from $5.5 billion to $8.7 billion. Costs included lost productivity, system restoration, and other recovery efforts.
* Affected Organizations: Major organizations worldwide were affected, including government agencies, corporations, and individuals. The speed and reach of the worm highlighted vulnerabilities in email systems and the lack of preparedness for such attacks.

### PREVENTING MEASURES TAKEN:

* Antivirus Updates: Antivirus companies quickly developed and distributed updates to detect and remove the worm. These updates helped to contain the spread and mitigate further damage.
* Network Segmentation: Organizations implemented network segmentation and disconnection of infected systems to prevent the worm from spreading.
* User Education: Efforts were made to educate users about the dangers of opening unsolicited email attachments and the importance of verifying the legitimacy of emails before interacting with them.
* Legal Action: Onel de Guzman, a student in the Philippines, was identified as the creator of the worm. However, at the time, the Philippines did not have specific laws against computer hacking, and he was not formally charged. This incident led to the creation of new cybercrime legislation in many countries.

# 