# Cyber Security Awareness: Understanding and Mitigating Common Threats

**Dr. Sarasvathi V**
**Professor,**
**Dept of CSE**
**PES University**

# Contents

- Cybersecurity
- Why cybersecurity Awareness
- Motives
- Common Cyber Threats
- Security Tips
- Useful Websites

# Introduction

## WHAT is Cybersecurity ?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

## WHY is Cybersecurity needed?

- Safeguards sensitive data from unauthorized access.
- Maintains the integrity and availability of information.
- Protects organizational reputation and customer trust.

# Security vs. Privacy

Privacy

- refers to the control you have upon your private information.

Security

- how this information is protected.

What's the difference between privacy and security?

You might share personal information with your bank when you open a checking account.

What happens after that?

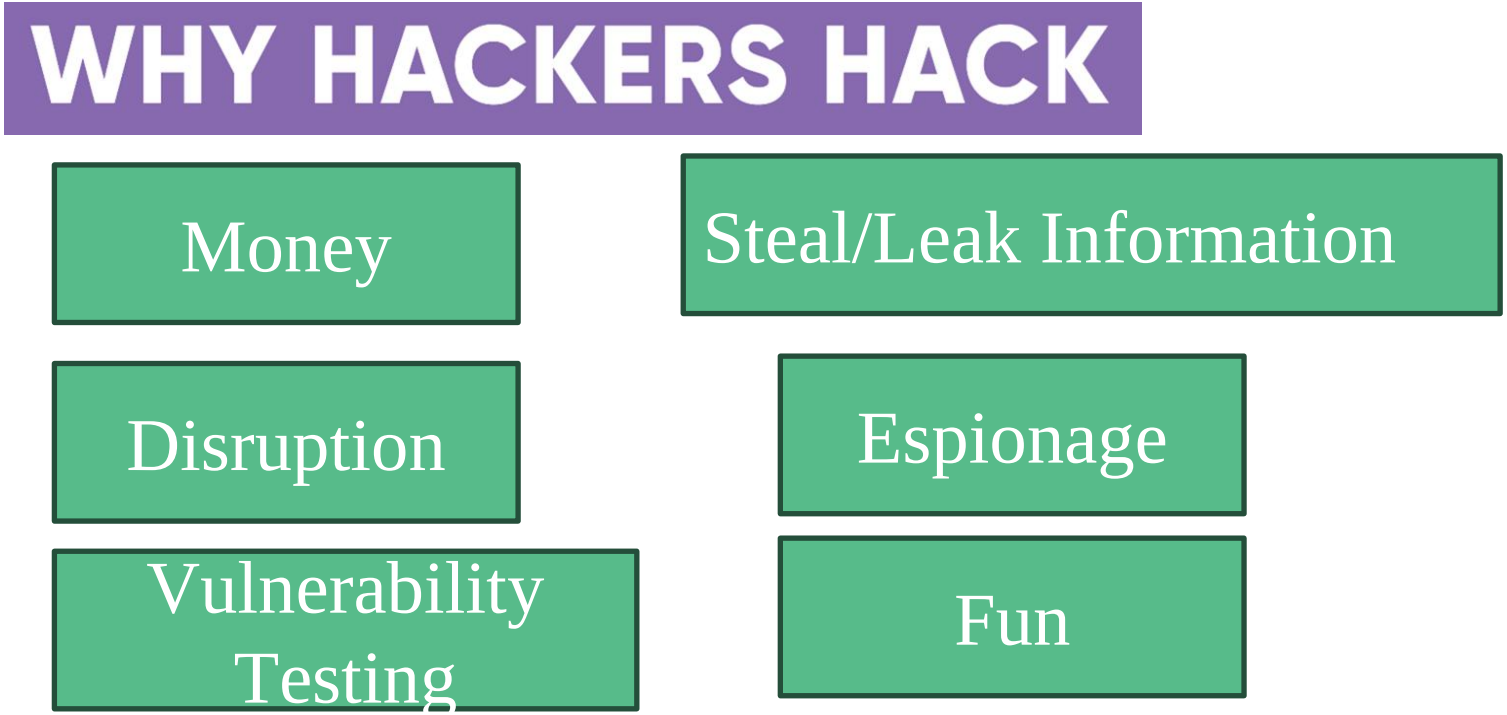
Three possible outcomes

- **Your privacy and security are maintained**
- **Your privacy is compromised, and your security is maintained**.
- **Both your privacy and security are compromised**.

# Why Cybersecurity Awareness?

- Cybersecurity awareness will always keep our workplace safe.
- Educating people, employees, stakeholders etc. and then regularly reminding them of potential cyber threats reduces risk of cyber attack.
- Technology provides the 1st Line of Defense for Cybersecurity Threats
- Generally Cybersecurity Attacks happen through the weakest link
- Employees: a link in the chain & need to be considered our last line of defence

# Cyber Crime Motives




Source: https://techwell.com.au/7-reasons-why-hackers-hack-how-to-prevent-it/

# Common Cyber Threats

PES UNIVERSITY

## PHISHING

Deceiving users into clicking malicious links or downloading attachments

## RANSOMWARE

Permanently blocks access to the victim's personal data unless a "ransom" is paid

## THREATS

Malicious software designed to harm computers or networks

## MALWARE

Manipulating people to reveal sensitive info or perform actions.

## SOCIAL ENGINEERING

# Phishing

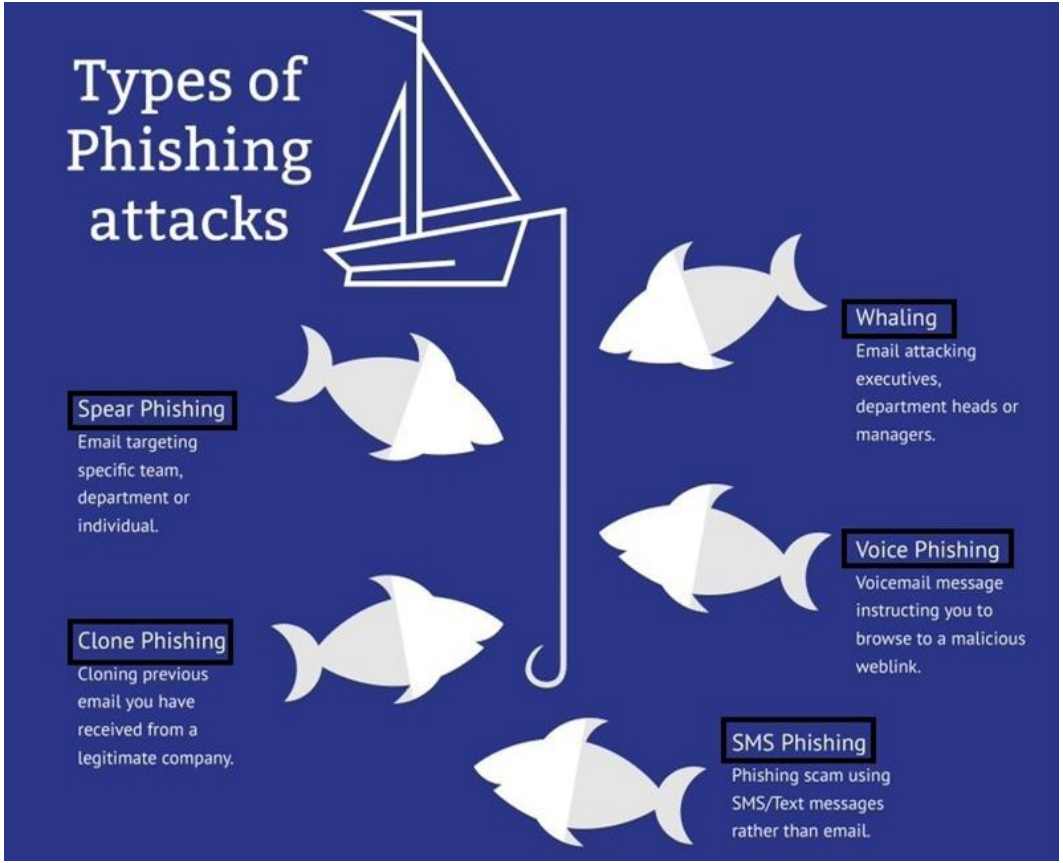
## What is PHISHING ?

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source.

## How is Phishing Attack Launched ?

Targets individuals through email, text messages, phone calls, and other forms of communication

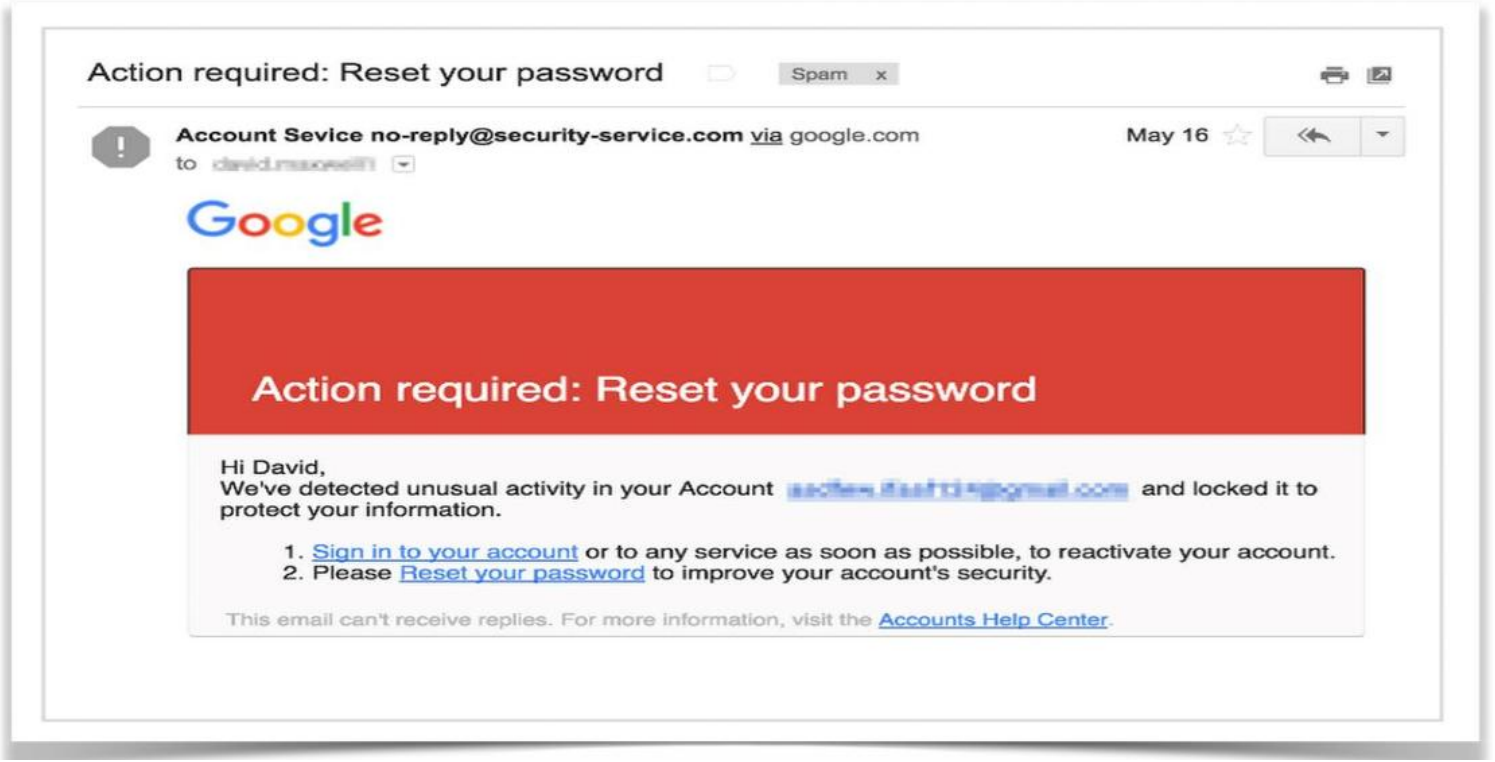
# Phishing




Source: https://www.linkedin.com/pulse/what-phishing-attack-how-do-you-prevent-them-mallya-cams-came

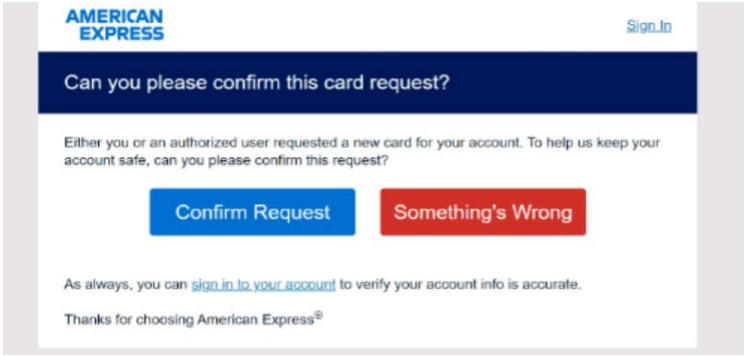
# Email Phishing

**A Phishing Email Depicting an malicious attacker targeting victim**

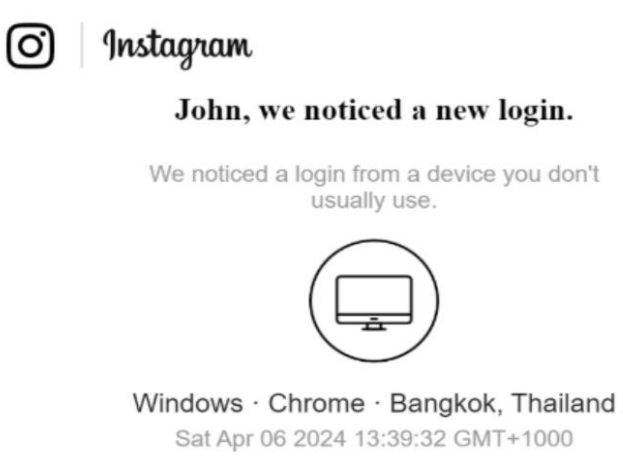



Source: https://blog.google/technology/safety-security/fighting-phishing-smarter-protections/

# Email Phishing






Source: https://caniphish.com/free-phishing-test/phishing-email-templates

# Latest Phishing Scams: University of Chicago

From: Karen Davidson <karen.davidson@student.cgcc.edu>

Date: Friday, July 5, 2024 at 12:24 AM

Subject: UCHICAGO ACTION REQUIRED

THE UNIVERSITY OF CHICAGO

Part Time Administrative Assistant needed.

Dear Student, In the interest of Professor Kenneth Pomeranz,you have been preferred to work as a part-time administrative assistant which gives you the opportunity to earn (350 per week) Submit your full name in a text message to (443) 807-5357 for more information. Best Regards

Jun 5, 2024

Sent: Wednesday, June 5, 2024 2:49 PM

Subject: UCHICAGO SECURITY ALERT: All Students are required to enroll now

Email Scam (June 6, 2024): UCHICAGO DUO ALERT: All Students Should Verify Immediately

Email Scam (July 3, 2024): UOFT ALERT: Job Opportunity for UofT Students

Source: https://security.uchicago.edu/phishing/latest/page/2/?et_blog

# Phishing Emails

Fake Sense of Urgency

Grammatical Errors - check for typos

Name of Sender can trick

Suspicious Subject of Mail

File Attachment or Hyperlink

Too good to be true

Hover but don’t click

# Whatsapp Security

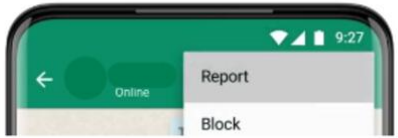
## Missed Call Scam

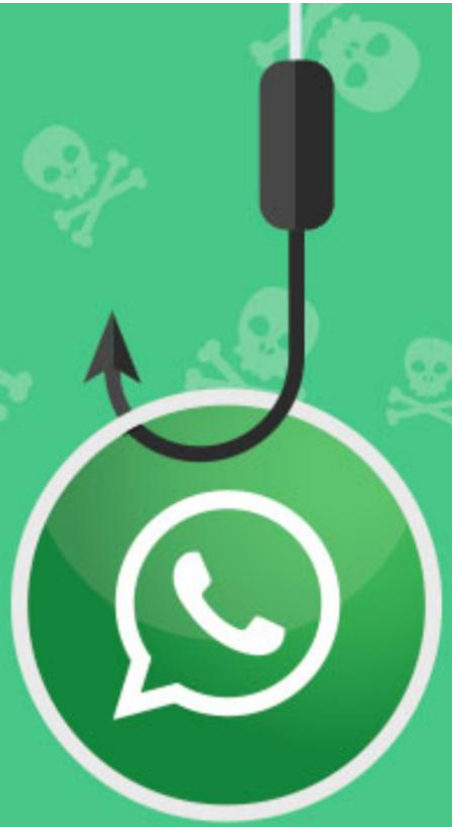
- Scammers claim wrong number dialed or urgent communication
- Request for shared code or personal details
- Prey on target's curiosity or concern

## Suspicious Numbers and Malicious Links Alert


- Avoid replying to job offers and messaged from unknown international numbers
- Don’t click on malformed links and random QR codes

## Report Suspicious Activity



# How to Report Scam Email

https://www.cyberforensics.in/

https://cybersafe.gov.in/

To verify whether a contact or identifier is associated with known cyber fraudsters in India

https://fotoforensics.com/

# Malware

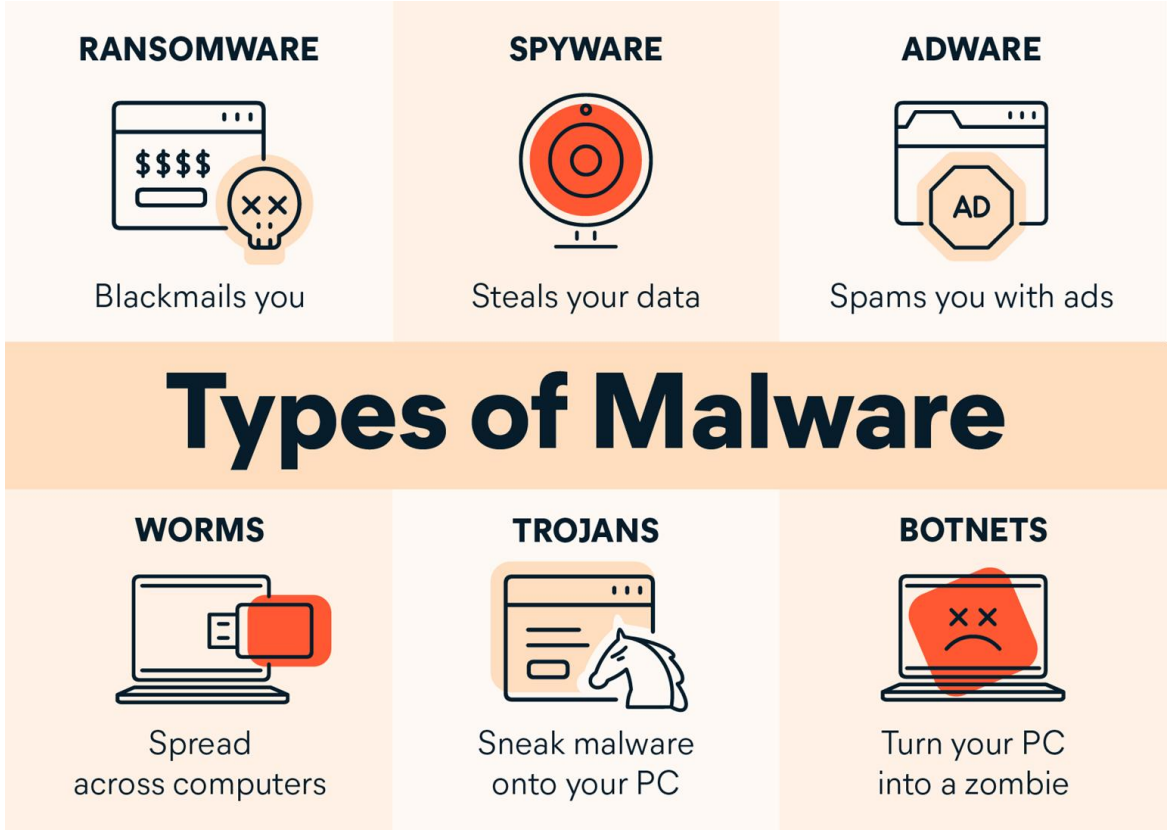
## What is MALWARE ?

Malware = Malicious Software
Specifically designed to gain access or damage a computer without the knowledge of the owner

## How is Malware Attack Launched ?

Entry -> Distribution -> Exploit -> Infection -> Execution

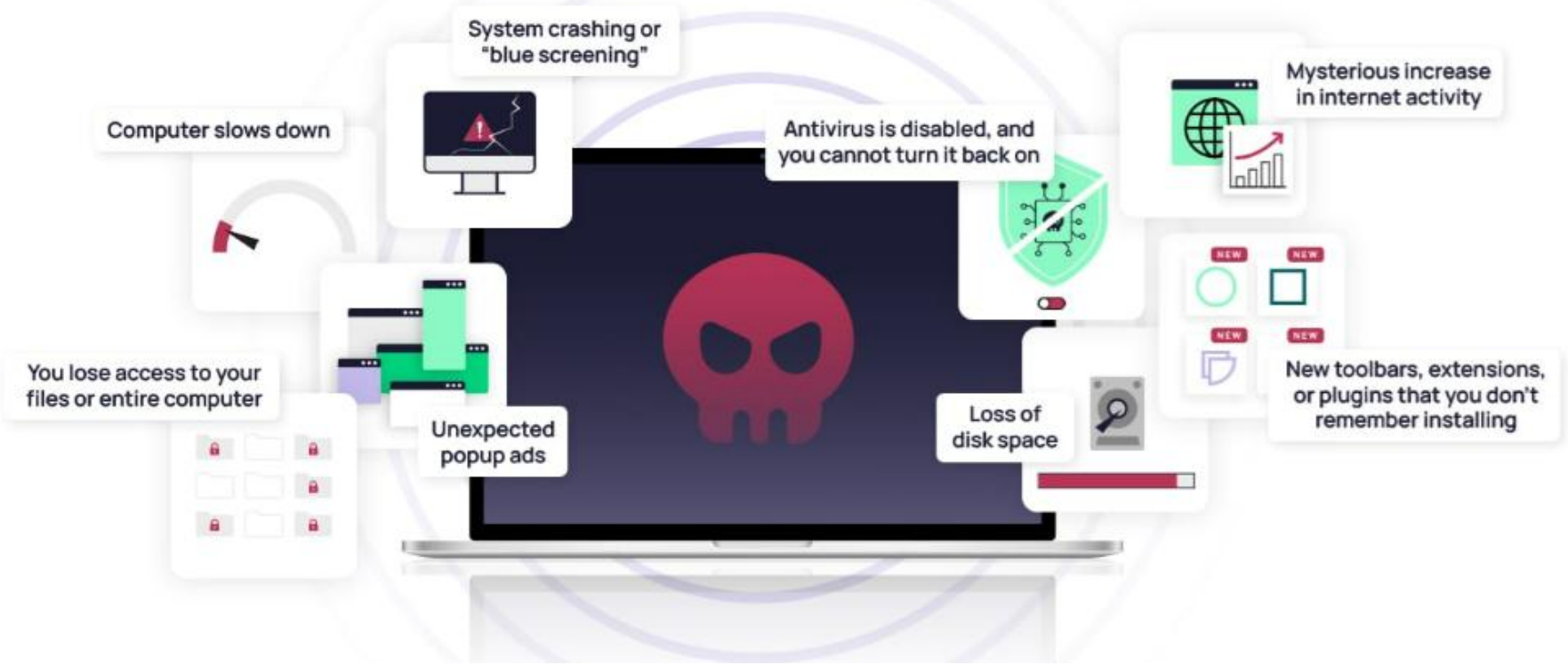
# Malware




Source: https://www.avast.com/c-malware

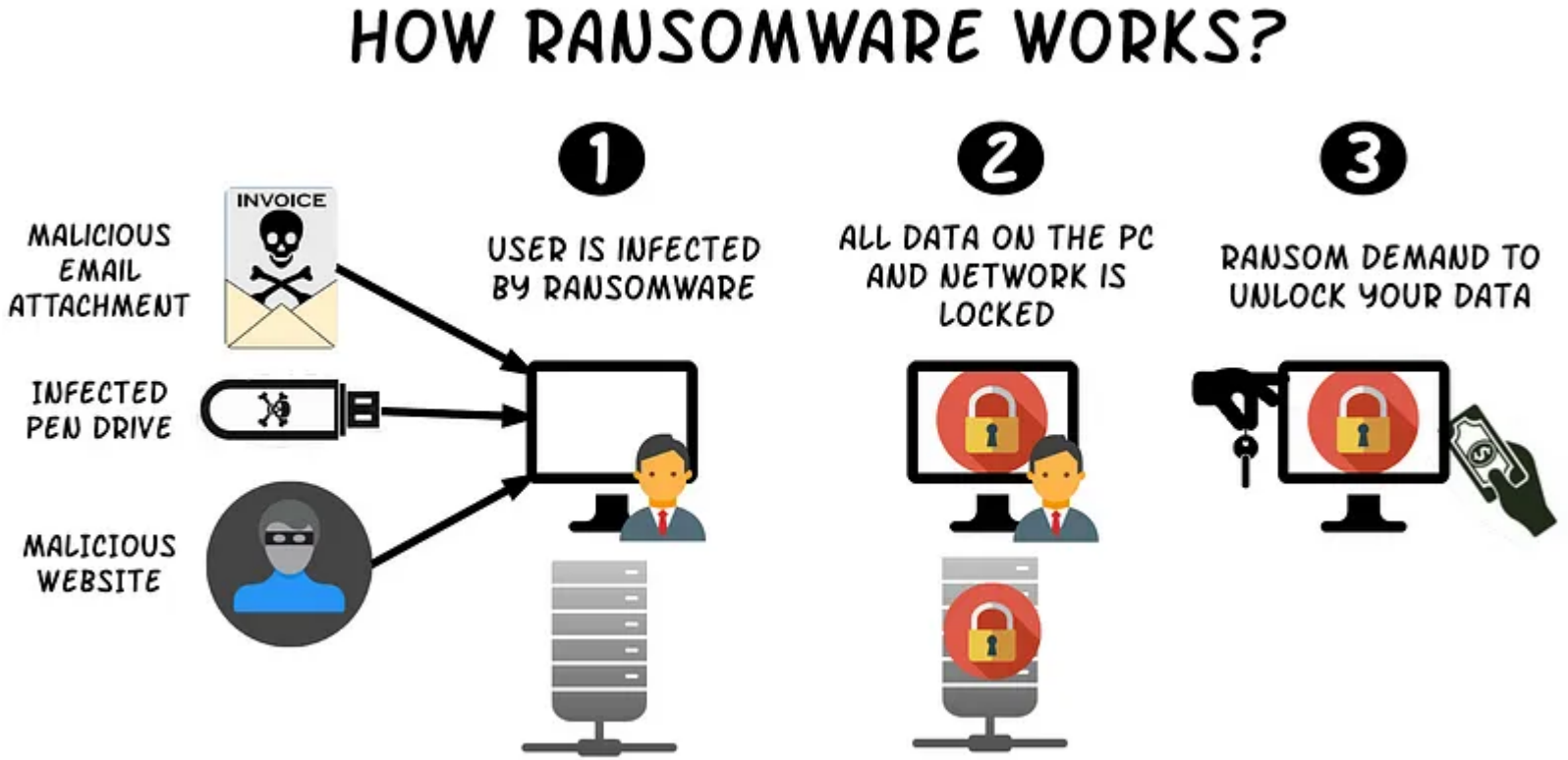
# Malware

## How to know if you have malware




Source: https://sosafe-awareness.com/glossary/malware/

# Ransomware




Source: https://stopdjvudecryptor.ru/remove-donex-virus/

# Adware

## What is ADWARE ?

Adware in cyber security refers to a type of malware that displays unwanted advertisements on your computer or device.

## How is Adware Launched ?

Adware is commonly activated unknowingly when users are trying to install legitimate applications that adware is bundled with.

# Adware

Don’t download unnecessary software

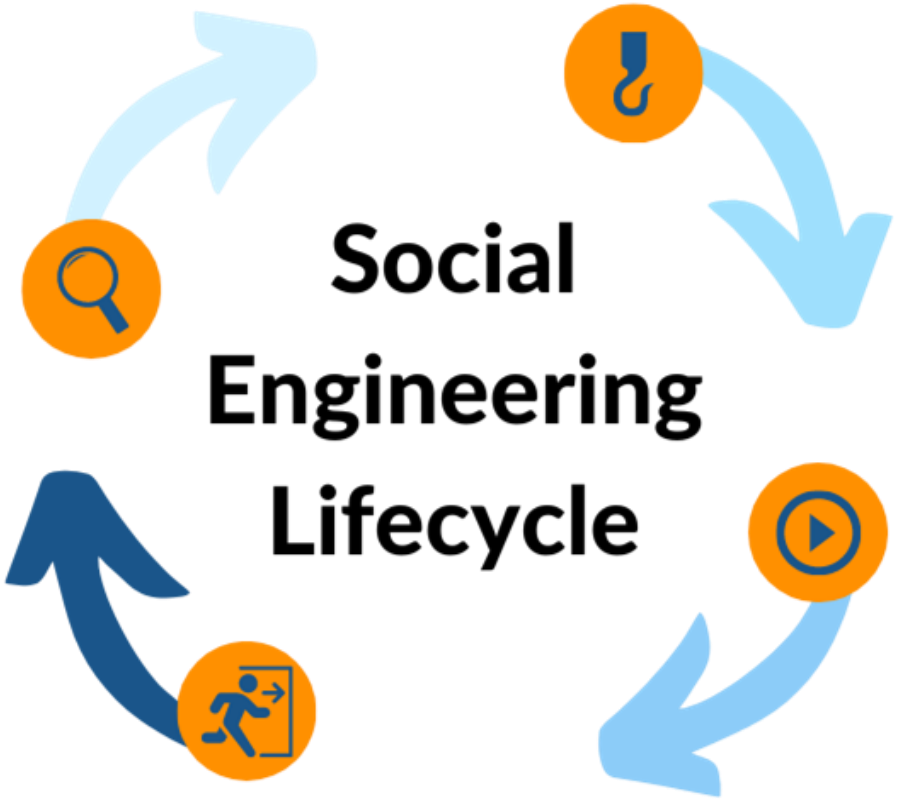
Enable firewall when browsing Internet

Use Secure websites for downloads

Regular Anti-Virus Scans

Avoid clicking advertised popups

# Social Engineering




1. **Investigate**
   - Identify the victim.
   - Gather background information.
   - Select attack method.

2. **Hook**
   - Engaging the target.
   - Spinning a story.
   - Taking control of the interaction.

3. **Play**
   - Expanding the foothold.
   - Executing the attack.
   - Disrupting business and/or siphoning data.

4. **Exit**
   - Removing all traces of malware.
   - Covering tracks.
   - Bringing the play to a natural end.

Source: https://www.linkedin.com/pulse/role-employee-training-cybersecurity-risk-management-brian-kimathi

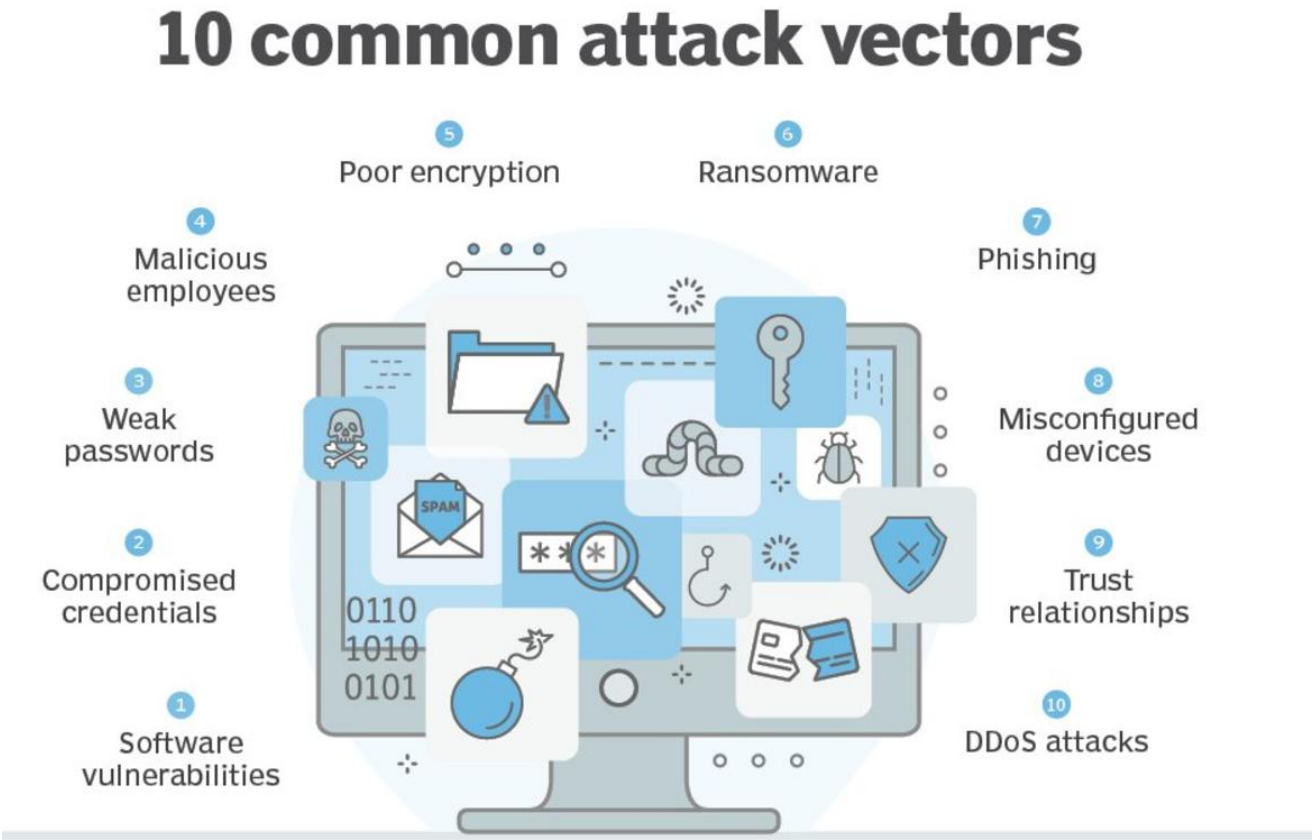
# Digital Payments

1. Never share PIN/OTP over SMS/Email/Call


2. Don't entertain calls from people posing as bank representatives asking for CVV / bank account info

3. Perform Online Banking on HTTPS secured websites only (never use open/unsecure Wi-Fi networks)


# Attack Surfaces




Source: https://www.techtarget.com/whatis/definition/social-engineering-penetration-testing

# Password Security


Source: https://www.phishprotection.com/cybersecurity/companys-guide-email-policies-include-policy-implement

# Password Security


Source: https://www.facebook.com/story.php/?story_fbid=421372739535978&id=111090043897584&_rdr

# Statistics on Password Security


Percentage of users that use birthdays/names in passwords


Percentage of users that use same password for every account


Percentage of users that have shared password


Percentage of users that rarely reset their passwords


Percentage of users that have experienced data breach due to weak passwords

Source: https://explodingtopics.com/blog/password-stats

# Password Security

- Use Different Strong Passwords for Different Accounts - Don't Reuse Passwords
- Use Secure Password Managers
- Use Biometric Authentication for apps
- Use Multi-Factor Authentication
- Never reveal username and password , as important as Bank PINs
- Immediately change any shared/leaked password
- Update Passwords at regular intervals

# Tips for Strong Password

**LENGTH** should be greater than 8 characters (12-16 characters)

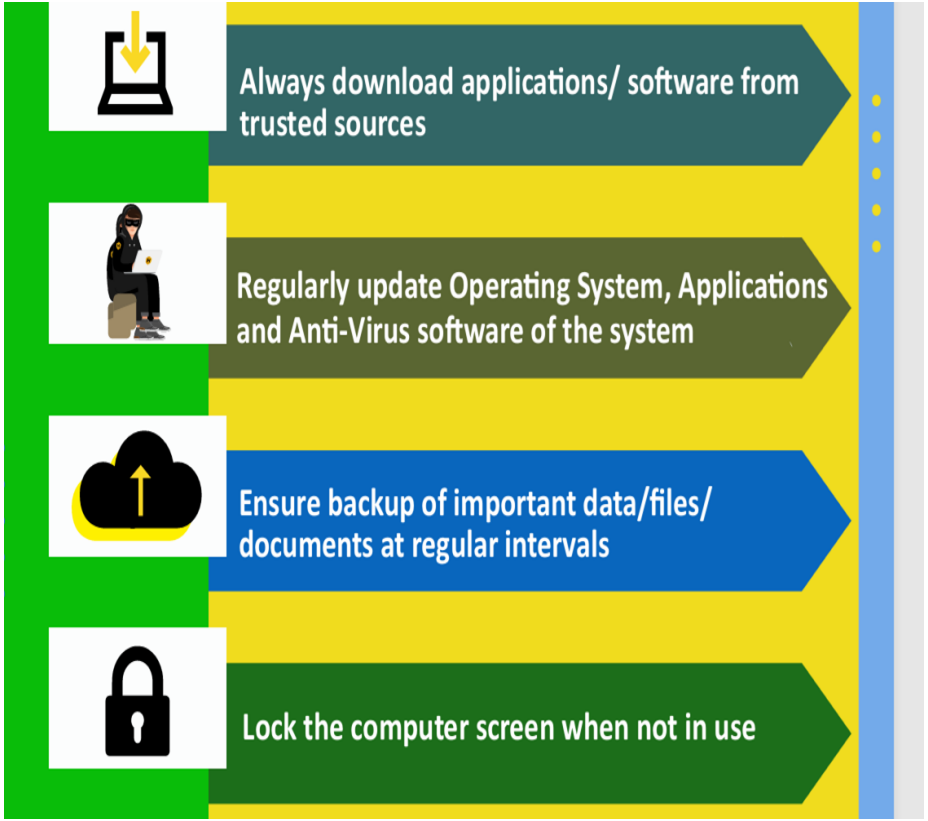
**COMPLEXITY** should be high
-Use uppercase, lowercase, numbers and special characters

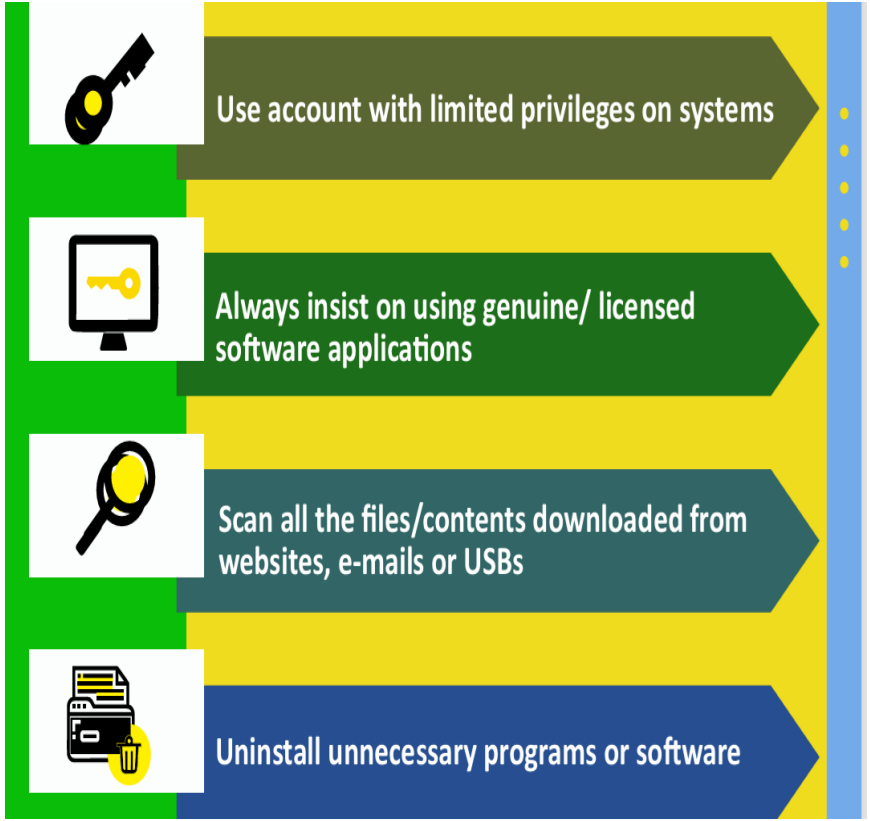

**UNPREDICTABILITY** in contents
-Don't use common phrases, birth dates, personal information names of family, pets, friends


**RECOVERY ANSWERS** of Password should not be guessable

# Computer Security Tips

PES UNIVERSITY



# Browsing Security


Source: https://www.centralcoalfields.in/ind/cybercrime/article_pdf/financialfraud.pdf

# Incident Response

Report the Incident to IT Team or government site

https://cybercrime.gov.in/


1. Disconnect from the network to prevent further damage
2. Change passwords for affected accounts
3. Run antivirus and malware scans

Thank You

# References


[1] https://www.cisa.gov/news-events/news/what-cybersecurity
[2] https://techwell.com.au/7-reasons-why-hackers-hack-how-to-prevent-it/
[3] https://www.raconteur.net/infographics/why-hackers-hack
[4] https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
[5] https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/
[6] https://www.business-standard.com/india-news/govt-warns-against-fake-banking-app-targeting-union-bank-account-holders-124042200248_1.html
[7] https://www.dailyexcelsior.com/cyber-cell-recovers-rs-3-lakh-lost-in-online-fraud/
[8] https://blog.usecure.io/what-is-phishing-awareness-training
[9] https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html
[10] https://www.linkedin.com/pulse/what-phishing-attack-how-do-you-prevent-them-mallya-cams-came
[11] https://caniphish.com/free-phishing-test/phishing-email-templates
[12] https://blog.google/technology/safety-security/fighting-phishing-smarter-protections/
[13] https://security.uchicago.edu/phishing/latest/page/2/?et_blog
[14] https://sosafe-awareness.com/glossary/malware/
[15] https://www.avast.com/c-malware
[16] https://medium.com/@rahulsharma0856/ransomware-how-it-works-a-growing-cyber-attack-d976aee62944
[17] https://stopdjvudecryptor.ru/remove-donex-virus/
[18] https://www.eset.com/uk/types-of-cyber-threats/adware/#:~:text=Adware%20definition%3A,that%20adware%20is%20bundled%20with
[19] https://www.linkedin.com/pulse/role-employee-training-cybersecurity-risk-management-brian-kimathi
[20] https://www.techtarget.com/whatis/definition/social-engineering-penetration-testing
[21] https://www.phishprotection.com/cybersecurity/companys-guide-email-policies-include-policy-implement
[22] https://www.facebook.com/story.php/?story_fbid=421372739535978&id=111090043897584&_rdr
[23] https://explodingtopics.com/blog/password-stats
[24] https://www.techopedia.com/how-to/how-to-create-a-strong-password
[25] https://www.centralcoalfields.in/ind/cybercrime/article_pdf/financialfraud.pdf
[26] https://economictimes.indiatimes.com/magazines/panache/safer-internet-day-54-social-media-users-havent-change-their-password-in-6-months/articleshow/67844890.cms?from=mdr
[27] https://www.backblaze.com/blog/2023-state-of-the-backup-as-data-needs-grow-backups-need-to-fill-the-gaps/