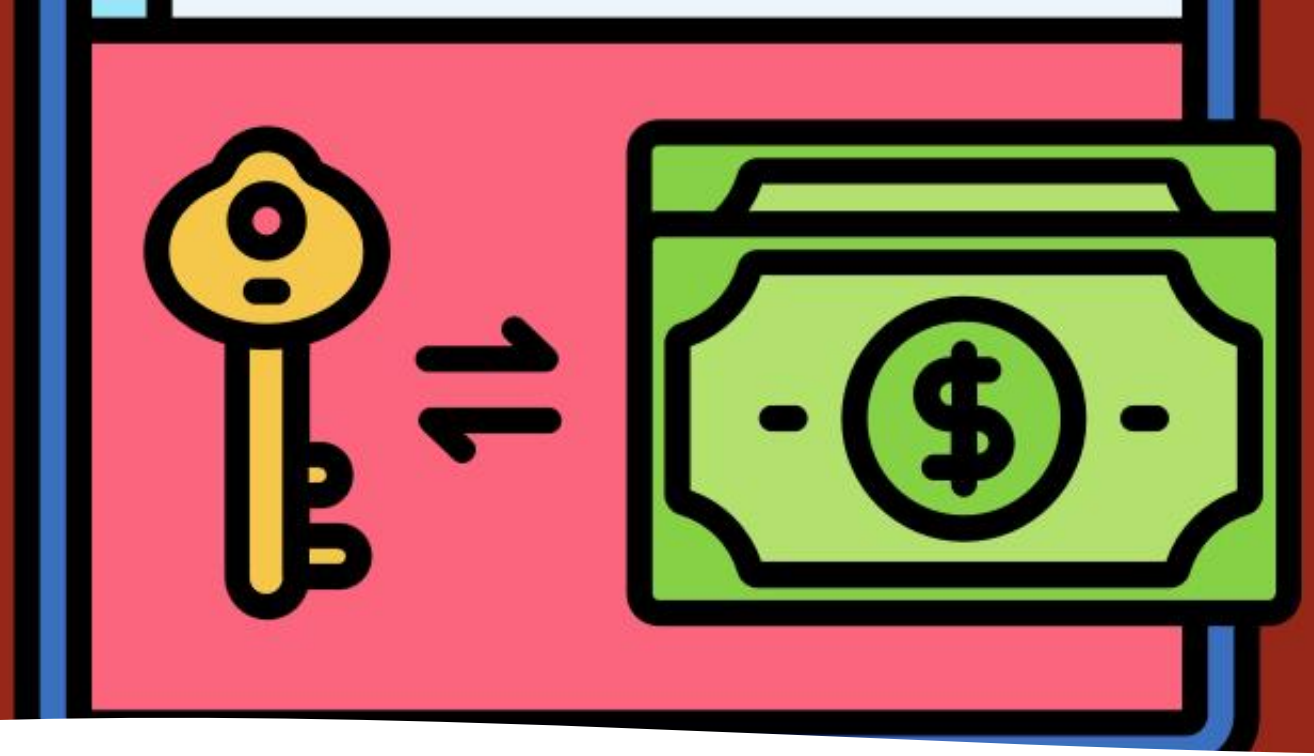
PREVENTING NETWORK ATTACKS & INCIDENT RESPONSE

PHISHING & SOCIAL ENGINEERING

- One of the biggest threats to cybersecurity
- Accounts for 22% of all data breaches
- Attacks increased by 61% in 2022
- Phishing is fraudulent emails purporting to be from reputable companies enticing individuals to reveal information to gain access to systems/networks
- Attackers attempt to trick users into clicking on bad links downloading malware
- Example-email from the IT department claiming your account has been compromised

BIGGEST THREATS TO ORGANIZATIONS AND NETWORK:

- Phishing
- Social Engineering
- Malware Attacks
- Ransonware
- Weak Passwords
- Insider Threats



What is Ransomware –

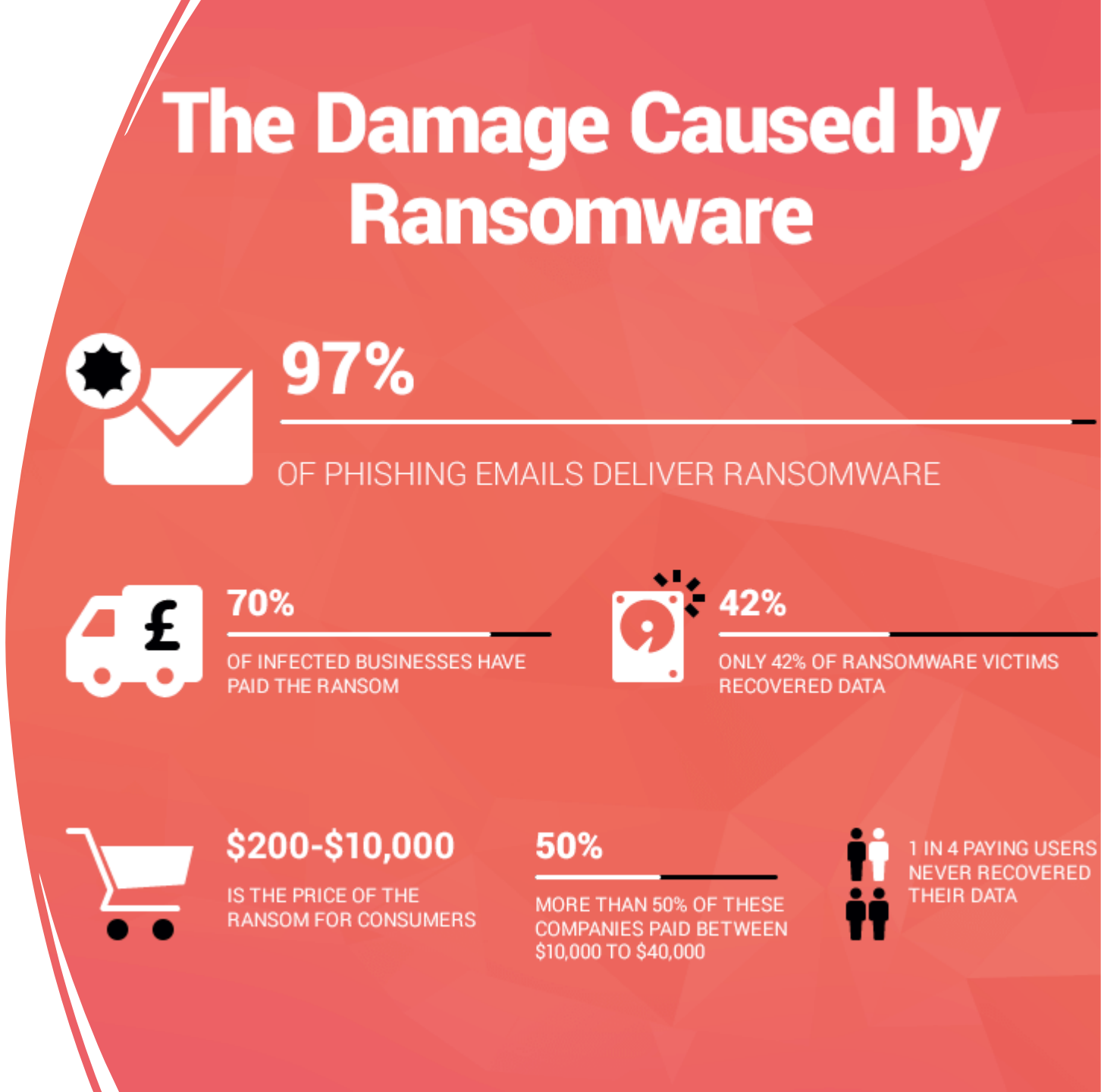
How Does it Work?

- Ransomware is a type of malware threat that actors use to infect computers and encrypt computer files until a ransom is paid.
- After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers.
- Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive.
- Ransomware generally adds an extension to the encrypted files such as .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, or cryptolocker

How Does Ransomware Occur?

Ransomware is commonly delivered through phishing emails or via “drive-by downloads.”

A “drive-by download” is a program that is automatically downloaded from the internet without the user’s consent or often without their knowledge. It is possible the malicious code may run after download, without user interaction. After the malicious code has been run, the computer becomes infected with ransomware.



Tips to Prevent Ransomware

UPDATE AND PATCH YOUR SYSTEMS/NETWORK

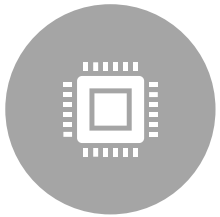
USE CAUTION WITH LINKS AND WHEN ENTERING WEBSITE ADDRESSES

OPEN EMAIL ATTACHMENTS WITH CAUTION

KEEP PII AND SENSITIVE INFORMATION SAFE-USE ENCRYPTION

VERIFY EMAIL SENDERS

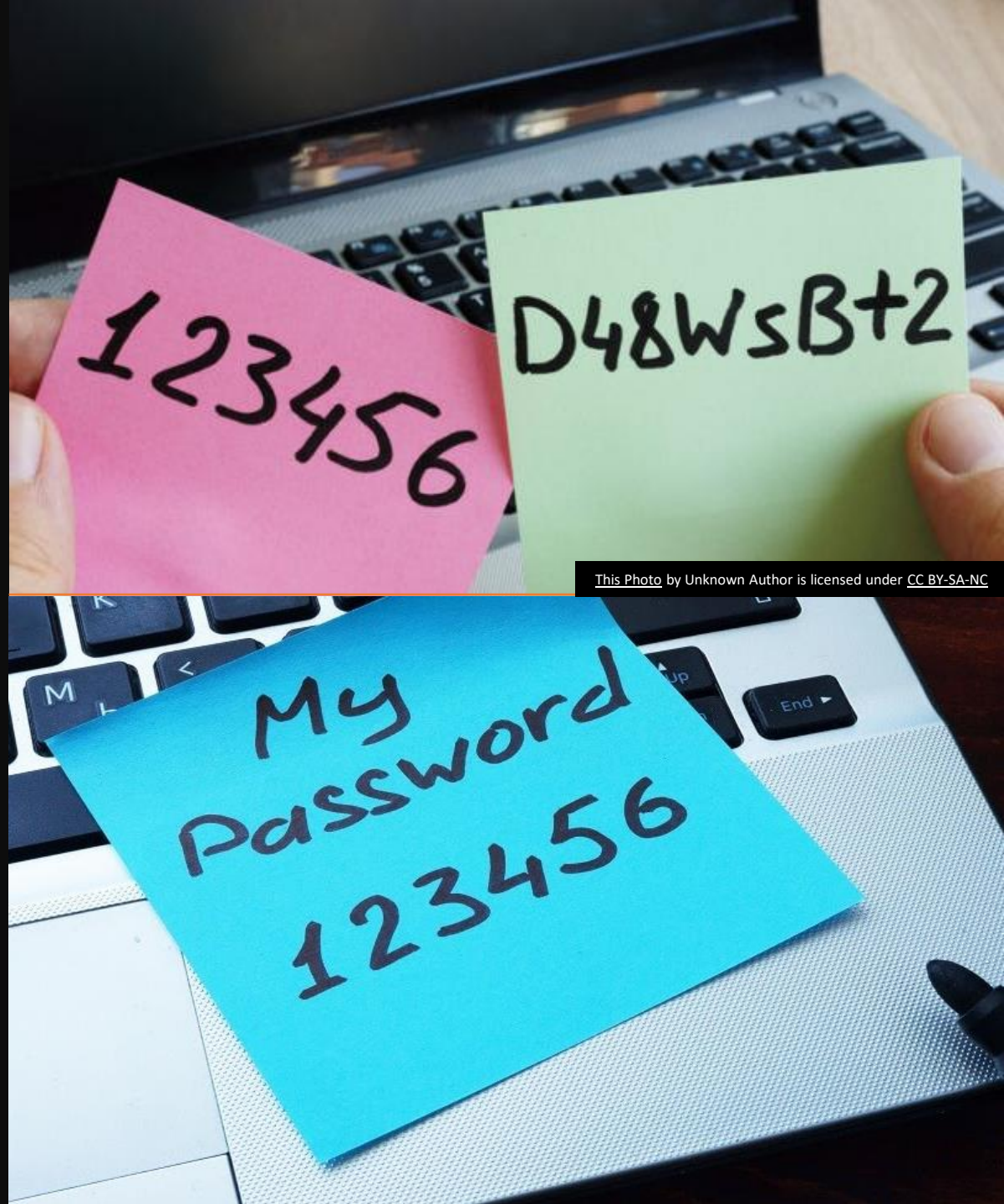
INFORM YOURSELF - QUESTION, RESEARCH, VERIFY AND INVESTIGATE



INSTALLING ANTIVIRUS SOFTWARE, FIREWALLS AND EMAIL FILTERS HELP

Weak Passwords

- Easy or generic passwords pose a weak link to cybersecurity
- Nearly 20% of passwords are compromised each year due to weak passwords
- A secure password should be at least 12 characters
- Create a password with capital letters, lowercase letters, numbers and special characters
- Use a passphrase to remember passwords
- Commit passwords to memory and not leave them near your computer or desk



Insider Threats

Cyber threats don’t always come from anonymous criminals hundreds of miles away

Affect over 34% of businesses globally every year

Insider incidents increased by 47% over the past two years

Objective is to sabotage an organization’s data, systems/network or steal confidential information for financial gain

Can occur with a current or former employee, contractor, or business partner who has or has authorized system access

Indicators of Insider Threats

Remotely accessing the network while on vacation, when sick, or at odd times

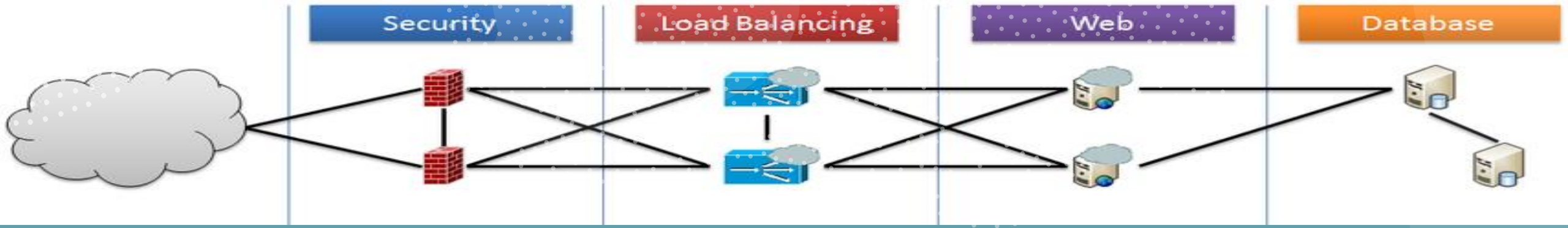
Working odd hours without authorization

Unnecessarily copies material, especially proprietary or classified information

Expresses interest in matters outside the scope of their duties

Shows signs of drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health, or hostile behavior towards others

HOW TO PROTECT DATA AND NETWORKS



NETWORKS AND DATA ARE PROTECTED BY THESE FOLLOWING MEASURES:

Back up of agency systems/network. Perform frequent backups of your system and other important files. If your systems become infected, you can restore your system to its previous state using your backups.

Store backups separately. Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive, or separate device from the network or computer.

Train your organization. Organizations should ensure that they provide cybersecurity awareness training to their personnel. Conduct regular and mandatory cybersecurity awareness training sessions to ensure all personnel are informed about current cybersecurity threats.

Antivirus Scans Highly Recommended

- Scans are highly recommended of your data and networks to identify malware and viruses
- Identifies any vulnerabilities within your organization
- Quick scans may not detect some malware or viruses
- Full scans can require much more time, but it detects all known viruses

Total global damage to businesses for cybercrimes in 2021 around $5 billion dollars

Home Depot-PII breach in 2015 exposed 56 million customers and credit card information

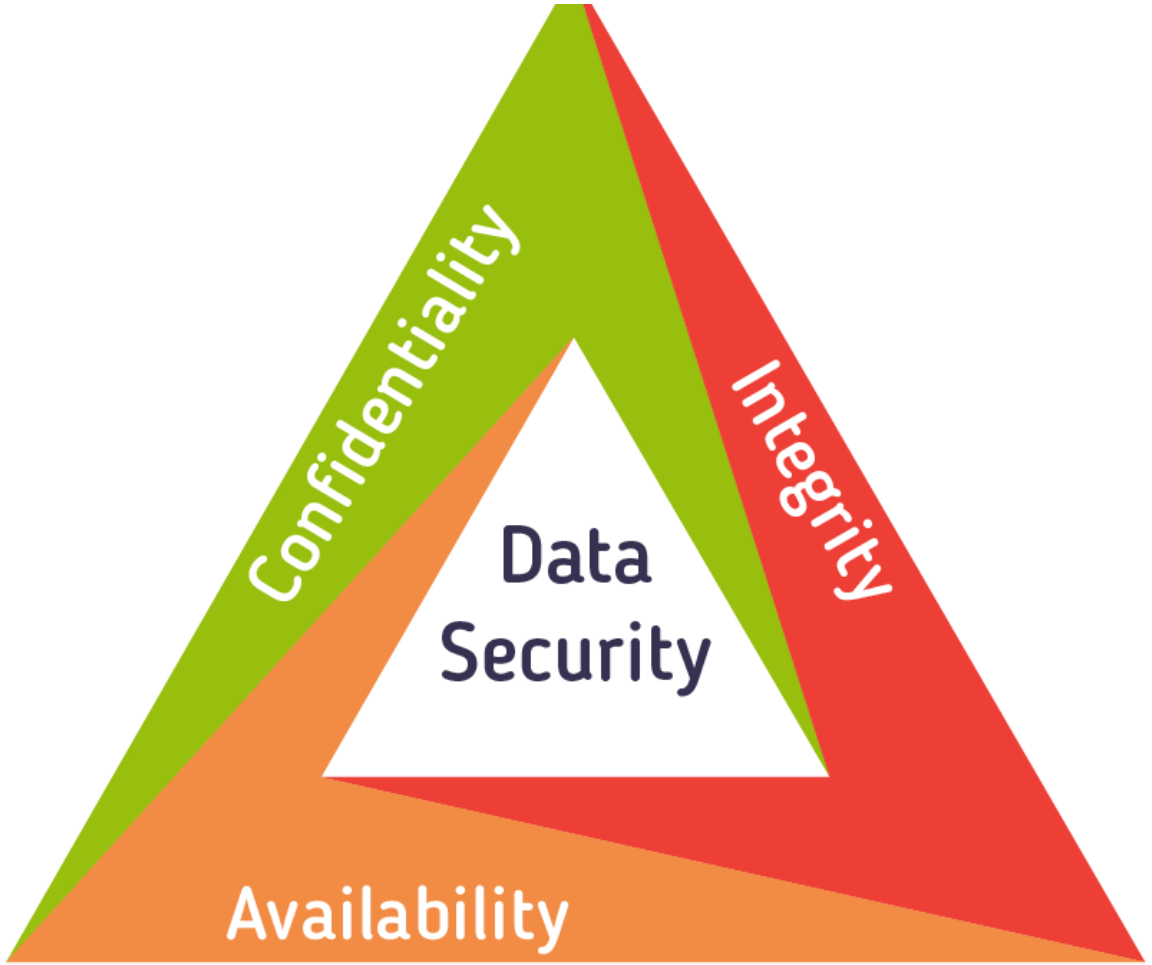
Data Security

Three most crucial components of data security:

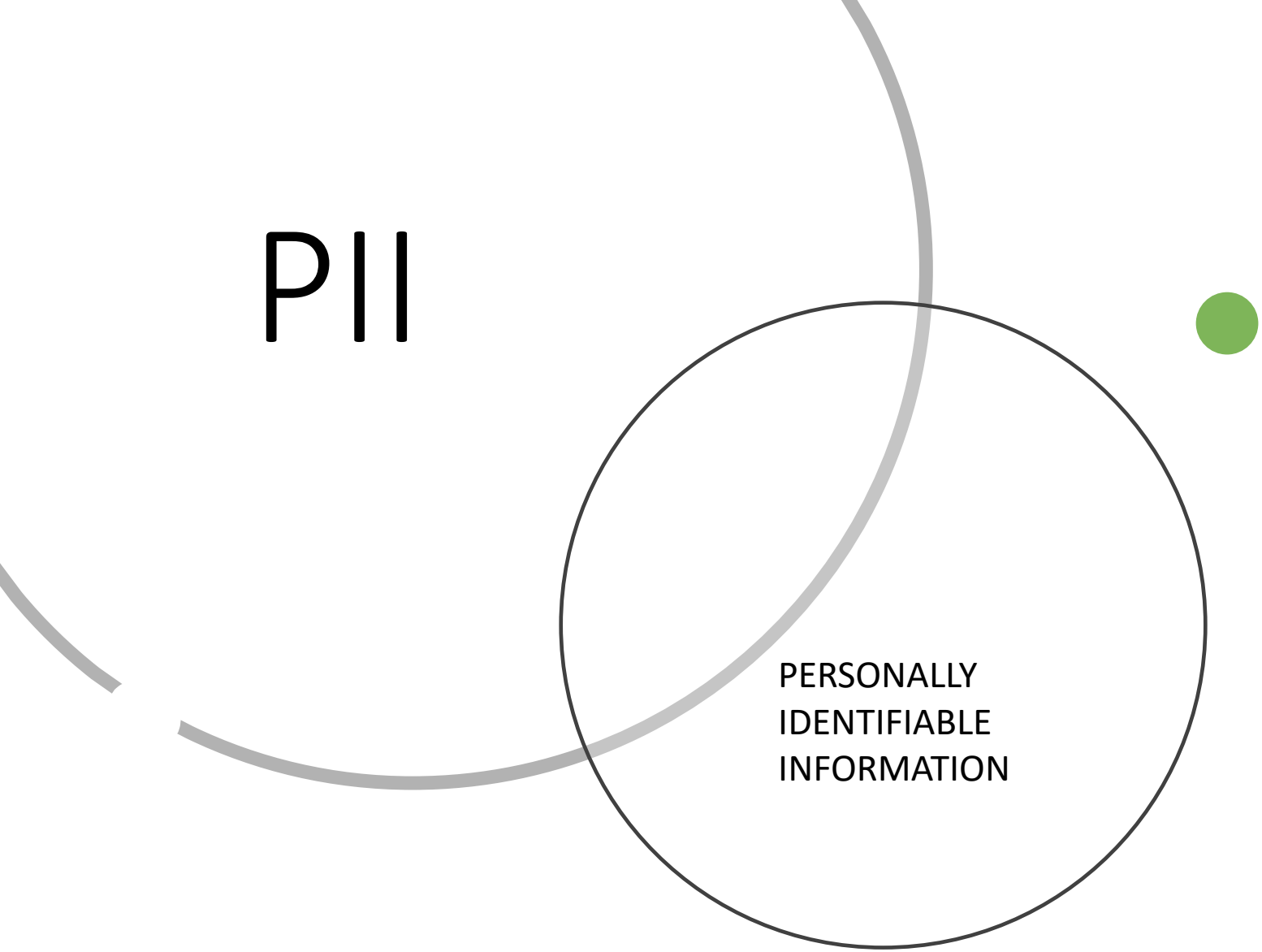
CONFIDENTIALITY–prevent unauthorized disclosure of information

INTEGRITY–assure that data cannot be modified in an unauthorized manner

AVAILABILITY–information should be readily available for the authorized users



PII



The Effects if PII is Lost or Stolen

Your agency reputation takes a hit: Customer confidence is lowered as trust is breached

Data loss can be expensive: Investigations, litigation, compensation, and other monetary losses can be incurred

Lost productivity and availability of data: Some downtime might be required to investigate or remediate the data breach

Fraud/direct monetary loss: This can be detrimental to your agency and assets

How to Protect PII

Don’t open suspicious email or email from unknown sources

Don’t click on URL links in emails or respond with PII

Incident Response and Reporting

- Know the types of security incidents to report
- Know your role and responsibility in the reporting process
- Report known or suspected incidents within 1 hour
- The integrity and reputation of your agency depends on how quickly incidents are reported, managed, and resolved

Security Incidents to Report

- Child Support Portal password is compromised
- Office break-in
- Unauthorized access to FPLS data
- Re-disclosure of FPLS data verbally, or on paper or electronic format to unauthorized person
- Laptop/case files stolen (especially from cars)
- Victim of ransomware / malware attacks
- Infected files
- Insider threats from disgruntled employees

Reporting Responsibilities

1

Report incidents immediately upon discovery but not less than 1 hour

2

Report real or suspected incidents even if you are not sure if it is an actual incident

3

Document as much of the specific details as possible including the time and date of discovery

Incident Reporting – Where to Report Incidents

Report to your Supervisor and CSS Security immediately.

Report an incident to: https://security.ncdhhs.gov/

Also, the IRS Office of Safeguards must be notified immediately, but no later than twenty-four (24) hours after identification.