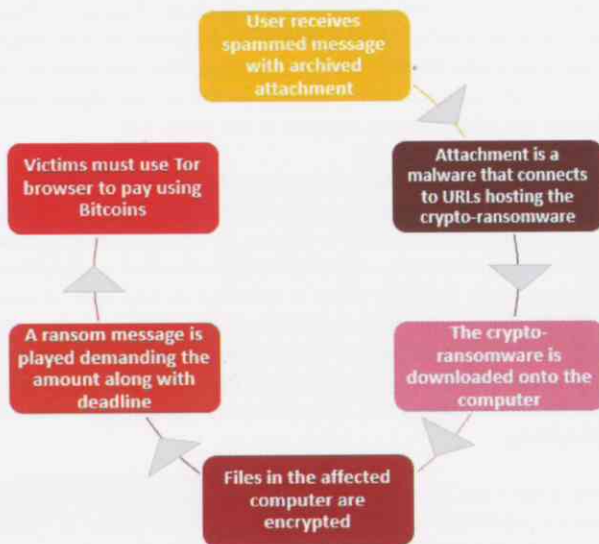# Cyber Suraksha Dishanirdesh

Ransomware attack

Ransomware is a type of malware that locks your computer screen and prevents you from accessing your files until you pay a certain fee or "ransom", which involves handing your password or your money to the anonymous attacker.
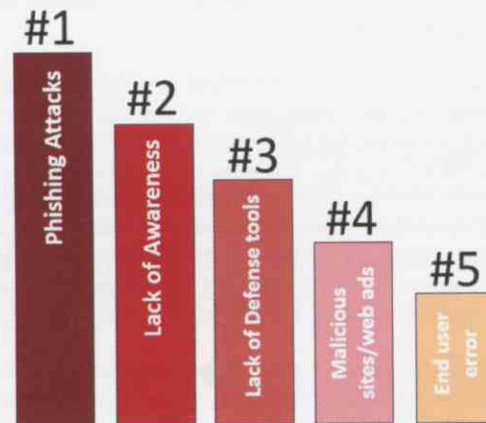
Ransomware attack process


```
User receives spammed message with archived attachment
    →
Attachment is a malware that connects to URLs hosting the crypto-ransomware
    →
The crypto-ransomware is downloaded onto the computer
    →
Files in the affected computer are encrypted
    →
A ransom message is played demanding the amount along with deadline
    →
Victims must use Tor browser to pay using Bitcoins
```

Common causes of Ransomware Attacks

Five most common leading causes of Ransomware infection are:

In order to protect NHA and its beneficiaries' Health and Personally Identified Information more effectively from ransomware, it's imperative to understand the cause and be wary of the attack itself.

#1 Phishing Attacks
#2 Lack of Awareness
#3 Lack of Defense tools
#4 Malicious sites/web ads
#5 End user error

Fact:
In May, 2017 India was hit with ransomware "WannaCry" attack. Almost 40,000 computers were affected.

What to do in case of Ransomware attack?

- Immediately disconnect the affected system to stop it from spreading.

- Since the encryption does not happen instantly, the user should immediately try to back-up the essential files as soon as possible. This will help minimize the damage.

- Report any such cases to NHA Helpdesk and NHA IS team.

Stay Safe from Ransomware
Here is the checklist !

DOs	DON'Ts
Install all security updates for your computer. Keep automatic updates enabled	Do not click on links in unwanted or unexpected emails
Beware of emails that ask you to enable "macros" to view the content	Do not download attachments received in unknown emails
Always keep a secure backup of your important data	Do not click on pop-up ads in unknown websites
Keep your antivirus software updated and ensure you are using the latest version	Do not pay ransom. There is no guarantee of getting your files back even if you do so
Do keep your security software patches and operating systems up to date	Do not give everyone full user permissions