

---

# Emerging Security Threats & Safety Mitigations

---



- Hitain Singh, NIC



# Agenda



- 1 Cyber Security Objectives
- 2 Cyber Hygiene
- 3 Emerging Security Threats
- 4 Cyber security Precautions

# Cyber Security Objectives

## Confidentiality

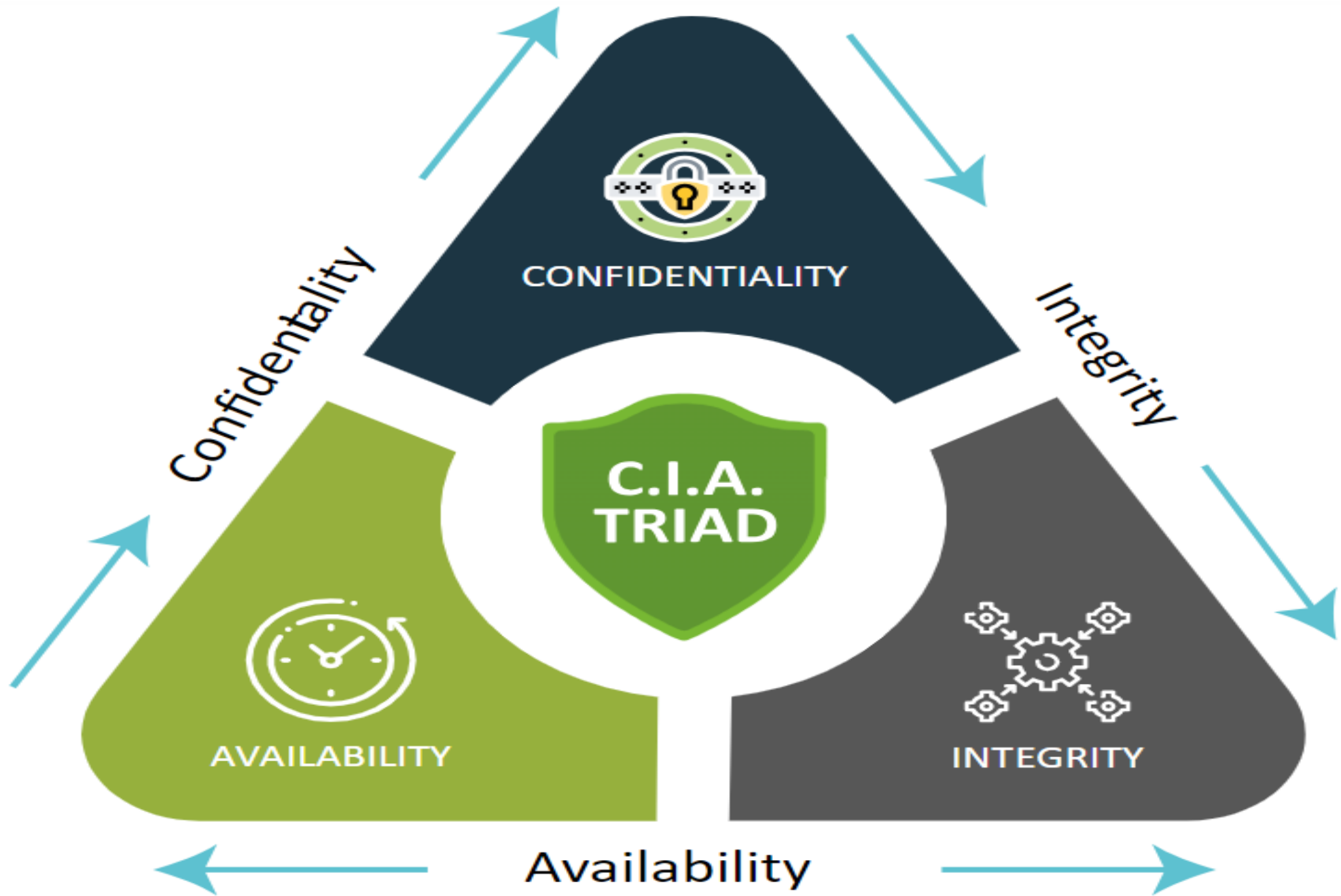
- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

## Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system

## Availability

- Assures that systems work promptly and service is not denied to authorized users



# What is Cyber Security & Threat in Cyber Security?

- Cyber Security refers to technologies, processes, and practices designed to protect assets (networks, devices, programs and data) from attack, theft, damage, modification or unauthorized access.
- Cyber Security can also be defined as the set of principles and practices designed to protect our computing resources and online information against threats.
- Cyber security threat can be broadly classified into three categories: threats to confidentiality, threats to integrity, and threats to availability. These categories correspond to the three main objectives of cybersecurity, often referred to as the CIA Triad (Confidentiality, Integrity, and Availability).

# Threats to Confidentiality

These threats involve unauthorized access to information. They aim to breach privacy by accessing sensitive data without consent. Examples of such threats include:

- **Phishing Attacks:** These attacks aim to trick users into divulging sensitive information, such as login credentials or financial information.
- **Spyware and Keyloggers:** These software programs are designed to collect and transmit personal or organizational data from a computer without the owner's knowledge or consent.

# Threats to Integrity

These threats involve unauthorized modification of information. The goal is to manipulate or destroy data to disrupt the organization's operations or credibility. Examples include:

- **Data Breaches:** These occur when an attacker gains unauthorized access to data in a system or database and alters it with malicious intent.
- **Malware Attacks:** Rootkits, Logic bombs, Trojan Horse, credential stealers can change or delete data on a system, disrupting its normal function.
- **Man-in-the-Middle (MitM) Attacks:** Attackers can intercept and alter communications between two parties without their knowledge.

# Threats to Availability

These threats prevent legitimate users from accessing information or systems. The goal is often to disrupt operations or services. Examples include:

- **Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) Attacks:** These attacks overwhelm a system's/Infra resources, making it unable to handle legitimate requests and thus rendering it unavailable to users.
- **Ransomware Attacks:** These attacks encrypt data on a system and demand a ransom to decrypt it, effectively denying the owner access to their own data.

# Why is security so hard?

- The complexity of ICT including software/applications and networks
- Increased Internet and AI usage
- User expectation and sense of responsibility.
- Lack of awareness of threats and risks
  - Social engineering
- Defense is inherently more expensive
  - Offense only needs the weakest link
- Ample cracking tools

# Key Challenges

- Lack of User Awareness
- Sharing and use of same of Credentials
- Downloading links or attachments hosted on external sites
- Govt Email configured in 3<sup>rd</sup> party Apps or Services (IMAP/POP3)
- Use of Email services in compromised machines/mobiles, or through 3<sup>rd</sup> party VPNs, Proxy Services
- Attackers by-passing Geo-fencing, Encrypted Attachments, Phishing Mails sent through compromised Govt Email IDs



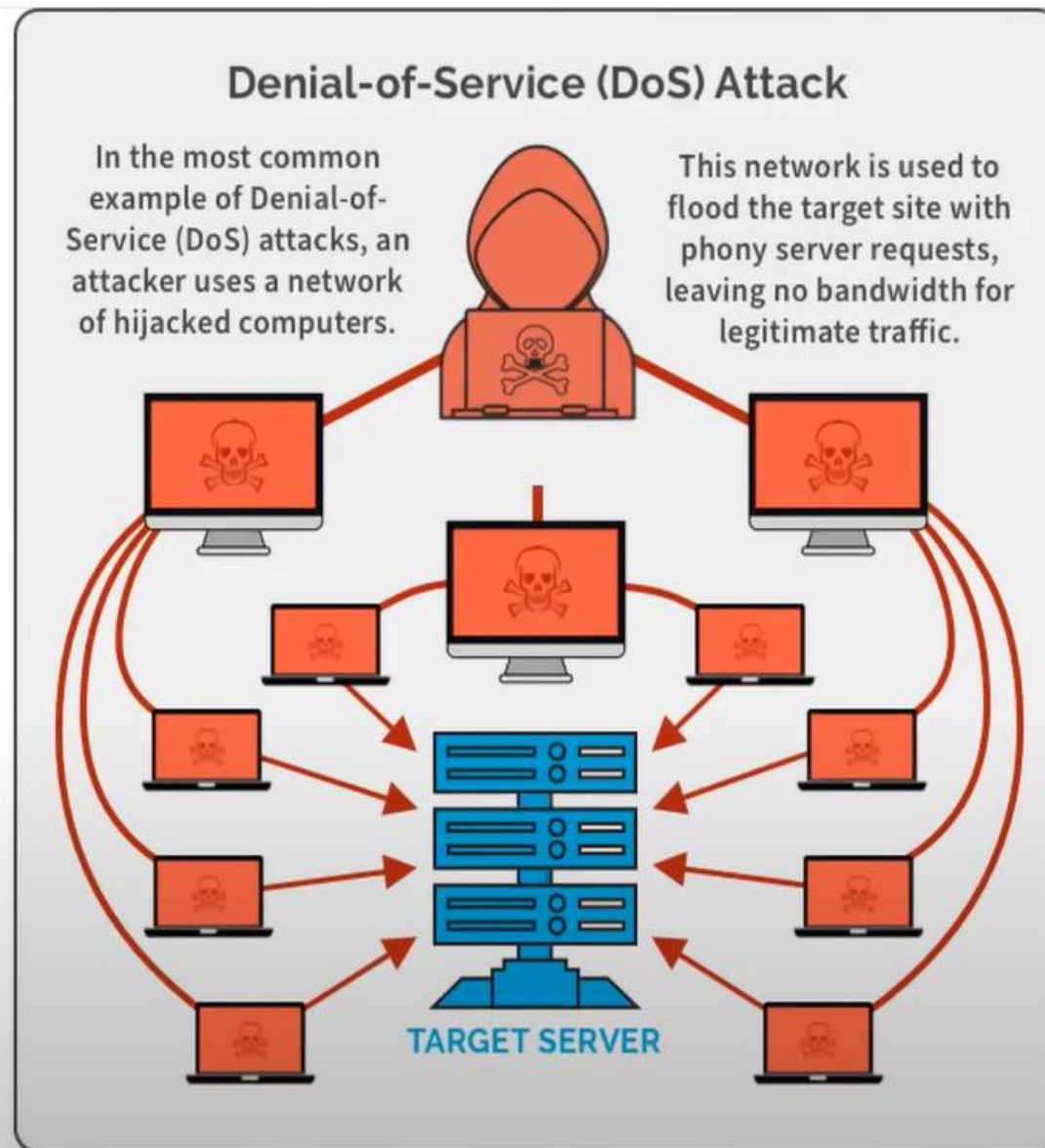
# Key Challenges

- Use of Obsolete OS and applications.
- Lack of Uniform AV/ Endpoint solutions, Hardening and access policies
- Targeted attacks + APTs and Lateral Movements
- Use of Pirated & Free Softwares, toolbars, download managers, Remote Admin tools, ...etc
- Monitoring and Compliance



# Most Common Attacks & Surface

- **Denial of Service (DoS and DDoS)**
- **Application-Layer attacks**
- **Social Engineering**
- **Misconfigurations**
  - Lack of encryption
  - Missing access restrictions
  - Weak permissions
  - Lack of compliance program
  - Improper data handling and retention
  - Insecure policy settings
  - Poor IAM controls



# Types of Cyber Attacks



# Hacking Evolution – Website Defacements

YOU HAVE BEEN  
HACKED !

=====

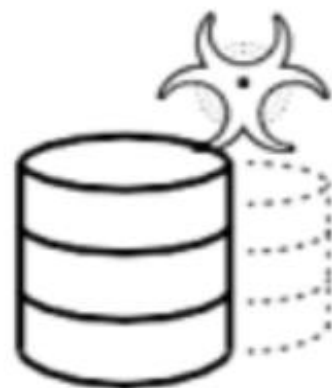
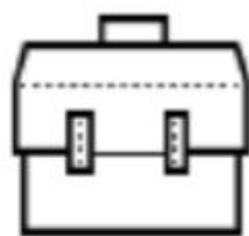
[\*] [Red] [R] Afghanistan: hacked by **hacked by Pakistan Cyber Army | Pakistan Cyber Army !!**  
[\*] [R] [Red] [R] Afghanistan Central Bank - Secured !!  
[\*] A message for all Afghanistan script kiddie's , stop playing with fire you bunch of script kiddie noobs  
[\*] This is a Payload from Pakistan Cyber Army after our Army sites was hacked and looted by Afghanistan Lameez Army  
[\*] You are warning you best code kids  
[\*] [R] [Red] [R] hacked by Pakistan Cyber Army | Pakistan Cyber Army  
[\*] [R] [Red] [R] We are sleeping but not dead!  
[\*] How Run with the full backup of Afghan Central Bank :D  
[\*] Download: [http://www.itsnot.com/backup-0.24.2002\\_04-03-04\\_download.gz](http://www.itsnot.com/backup-0.24.2002_04-03-04_download.gz)

**Pakistan Zindabad**

[\*] [Red] [R] **hacked by Pakistan Cyber Army | Pakistan Cyber Army | Dept of Cyber Army**

=====

# The CyberAttack Lifecycle



Reconnaissance

Weaponization  
and Delivery

Exploitation

Installation

Command  
and Control

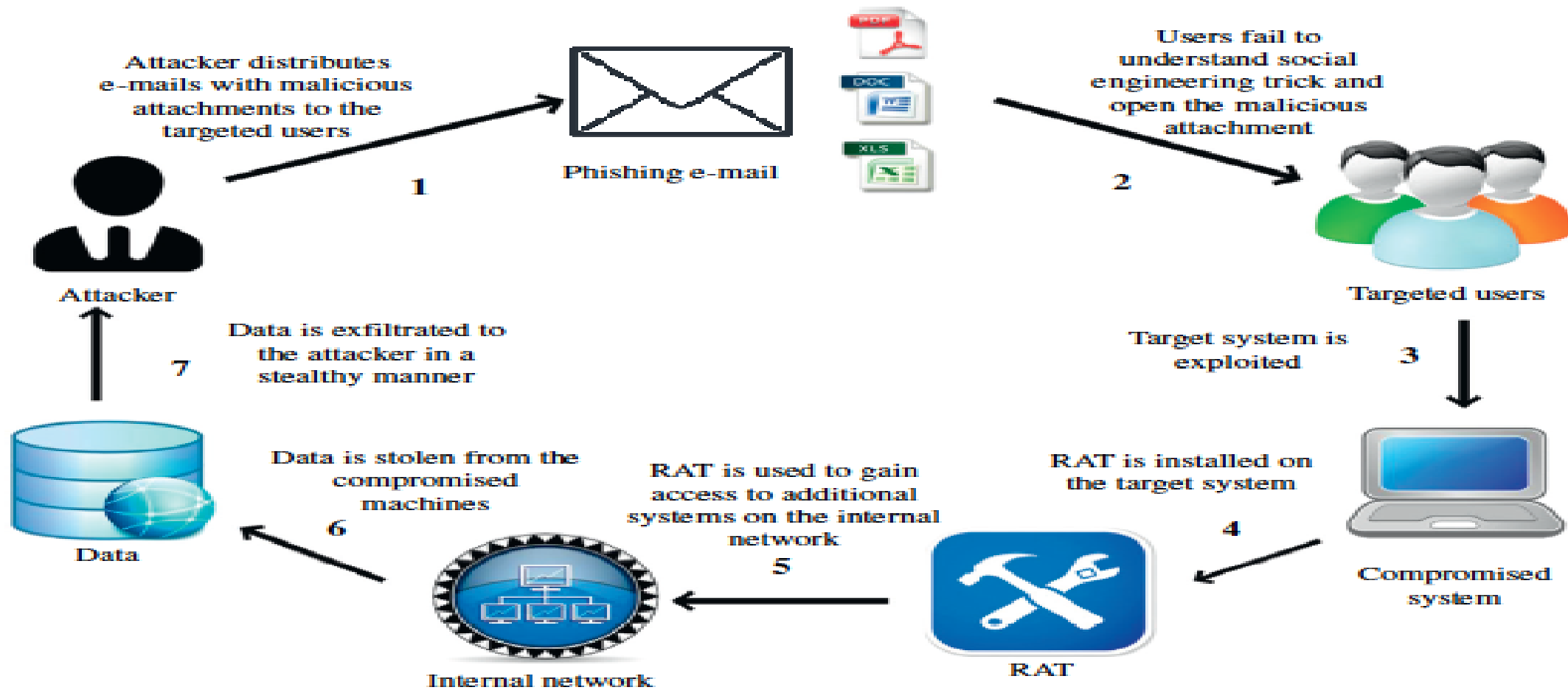
Actions on  
the Objective

**Preventive Controls**

**Reactive Controls**

Phishing – Spam – Social Engineering

# How Phishing Attack Works?



# APT Case Study

# Phishing Mail



**Covid-19 Agenda & application**

From:

To:

Sir,

As directed by DG Sir, Kindly download file of **Covid-19 agenda & application** developed for the 90th Board meeting which could not be held due to unforeseen circumstances and lockdown.

download link:

<https://tinyurl.com/y38qgew5>



*With best wishes and regards,*


F.No.833-BM/NAT/2020  
Dated: September 15, 2020

 150 YEARS OF  
CELEBRATING  
THE MAHATMA

"Cleanliness is next to Godliness"

# Phishing Mail

Close Reply Reply to All Forward Delete Spam   Actions ▾

 **Re: scan\_new**

From:

To:

On Wed, Oct 14, 2020 at 4:43 PM Manmohan Singh <manmsingh32@gmail.com> wrote:

Dear sir/madam,

please check this document,

<https://drive-nic.online/?file/d/1PxZ-JbjkDK5sCzuAqGT4b8lwkZaEPIDt/view?usp=sharing>

thank you

# Phishing Mail

Breaking News: Suspected rebels in Kashmir killed by Indian Army

1 message



From: CEO Bareilly

October 13, 2021 2:02 PM

Intelligence Report.pdf (13.6 KB) [Download](#) | [Briefcase](#)

Breaking News:

"Suspected rebels who shot dead five soldiers in Kashmir in the deadliest incident since February, killed by Indian Army" Colonel Devender Anand said today. **Intelligence Report** is attached in this regard for info.



Close Reply Reply to All Forward Delete Spam Actions



**IAF air strikes 'Exclusive Pictures "d estuction of Jaish Camp and dead bodies of terrori sts"**

NaN, 0NaN NaN:NaN PM

From: Maj Pallavi

To: da abudhabi

- Mail
- New Message
- Mail Folders
  - Inbox (378)
    - Blue Liv
    - Cloud
    - Cyber
    - NIC-CER
    - NKN-Nd
    - Service
    - shadow
    - SOC
    - Source
    - Vulnera
  - Sent (3)
  - Drafts (37)
  - Junk
  - Trash (24)
  - Application

Dear Sir,

IAF fighter jets achieved great success, struck the biggest camp of the Jaish-e-Mohammed, in Balakot, killing over 350 terrorists including Jaish chief Masood Azhar's brother-in-law.

Exclusive Pictures are the biggest proof of destruction of Jaish camp and dead bodies of terrorists can be downloaded from official web link:

<http://public-info.mod.gov.in.exclusive.pic>

URL: <http://mediashare.cc/?a=W15513159131>

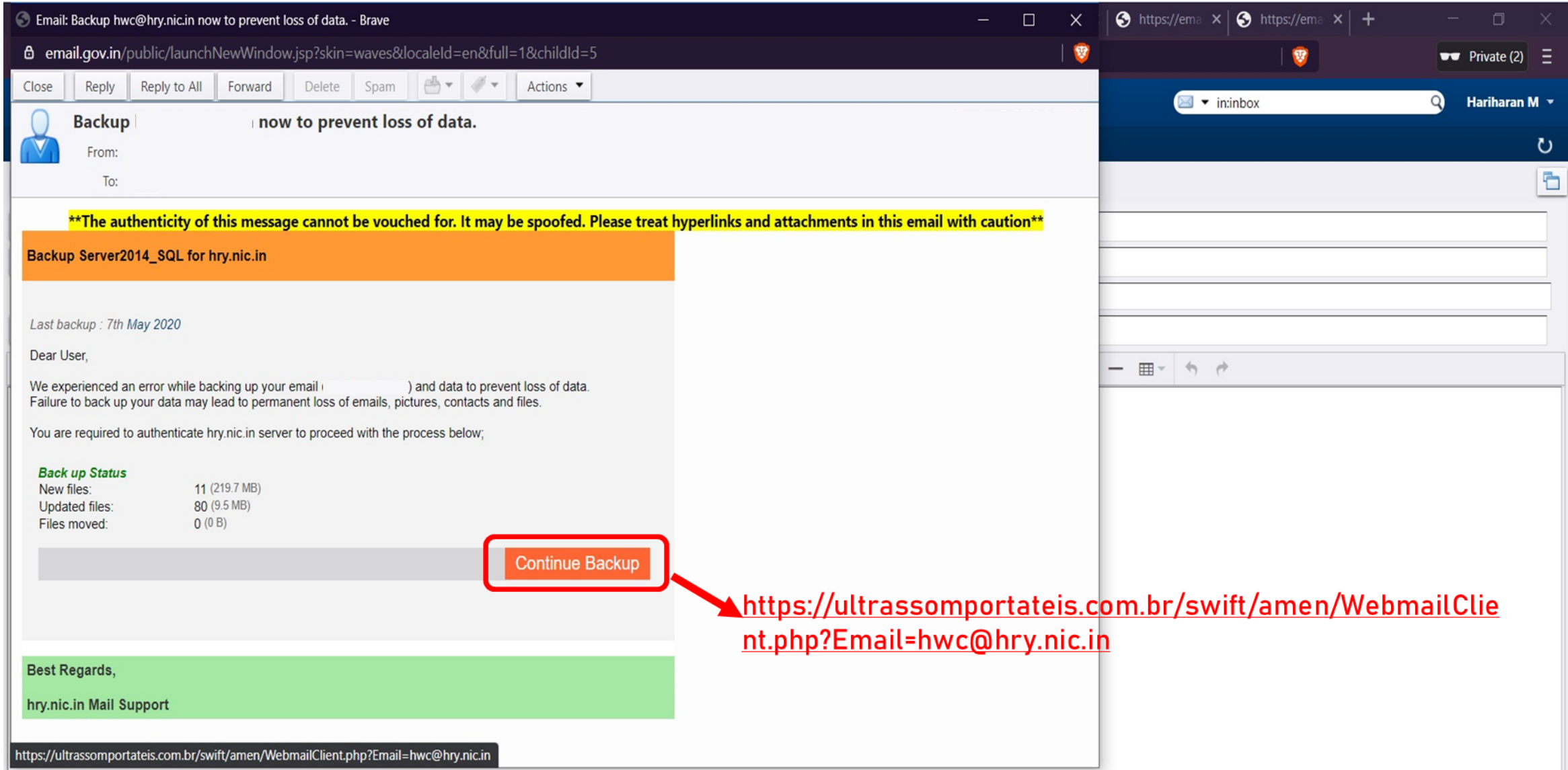
Regards

Lt col Pallavi

Public Information, IHQ of MOD (Army)

S	M	T
31	1	2
7	8	9
14	15	16
21	22	23
28	29	30
5	6	7

# Phishing Mail



Email: Backup hwc@hry.nic.in now to prevent loss of data. - Brave

email.gov.in/public/launchNewWindow.jsp?skin=waves&localeId=en&full=1&childId=5

Close Reply Reply to All Forward Delete Spam Actions

**Backup** | now to prevent loss of data.

From:  
To:

**\*\*The authenticity of this message cannot be vouched for. It may be spoofed. Please treat hyperlinks and attachments in this email with caution\*\***

**Backup Server2014\_SQL for hry.nic.in**

Last backup : 7th May 2020

Dear User,

We experienced an error while backing up your email ( ) and data to prevent loss of data. Failure to back up your data may lead to permanent loss of emails, pictures, contacts and files.

You are required to authenticate hry.nic.in server to proceed with the process below;

**Back up Status**

New files:	11 (219.7 MB)
Updated files:	80 (9.5 MB)
Files moved:	0 (0 B)

**Continue Backup**

Best Regards,  
hry.nic.in Mail Support

<https://ultrassomportateis.com.br/swift/amen/WebmailClient.php?Email=hwc@hry.nic.in>

# Phishing Mail sent to Govt. User

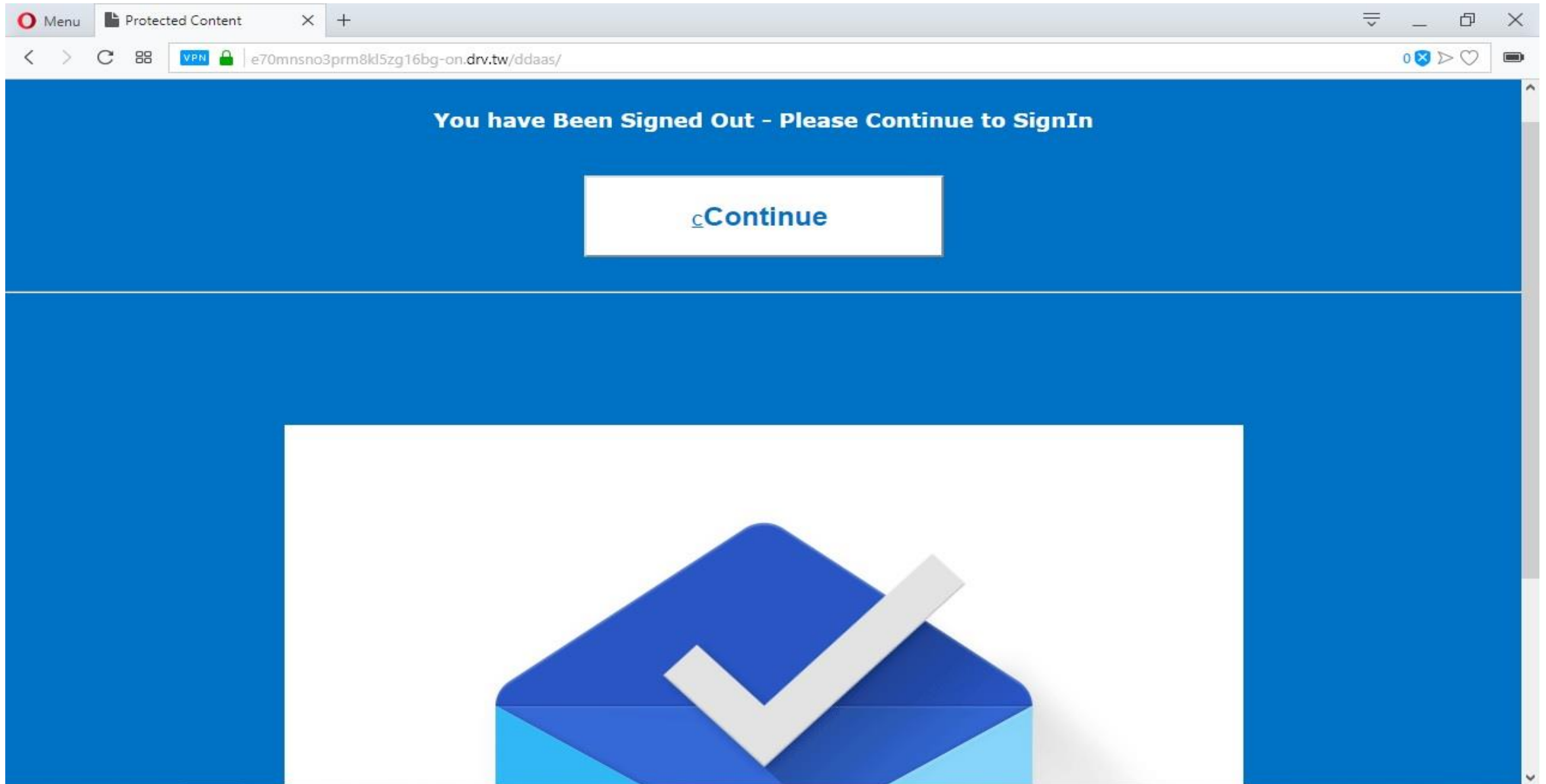
Hi user, Your Mail Box needs to be Re-verified to avoid Shutdown. You have less than 48hrs. Use the link below to continue using this service

**CLICK TO CONTINUE**

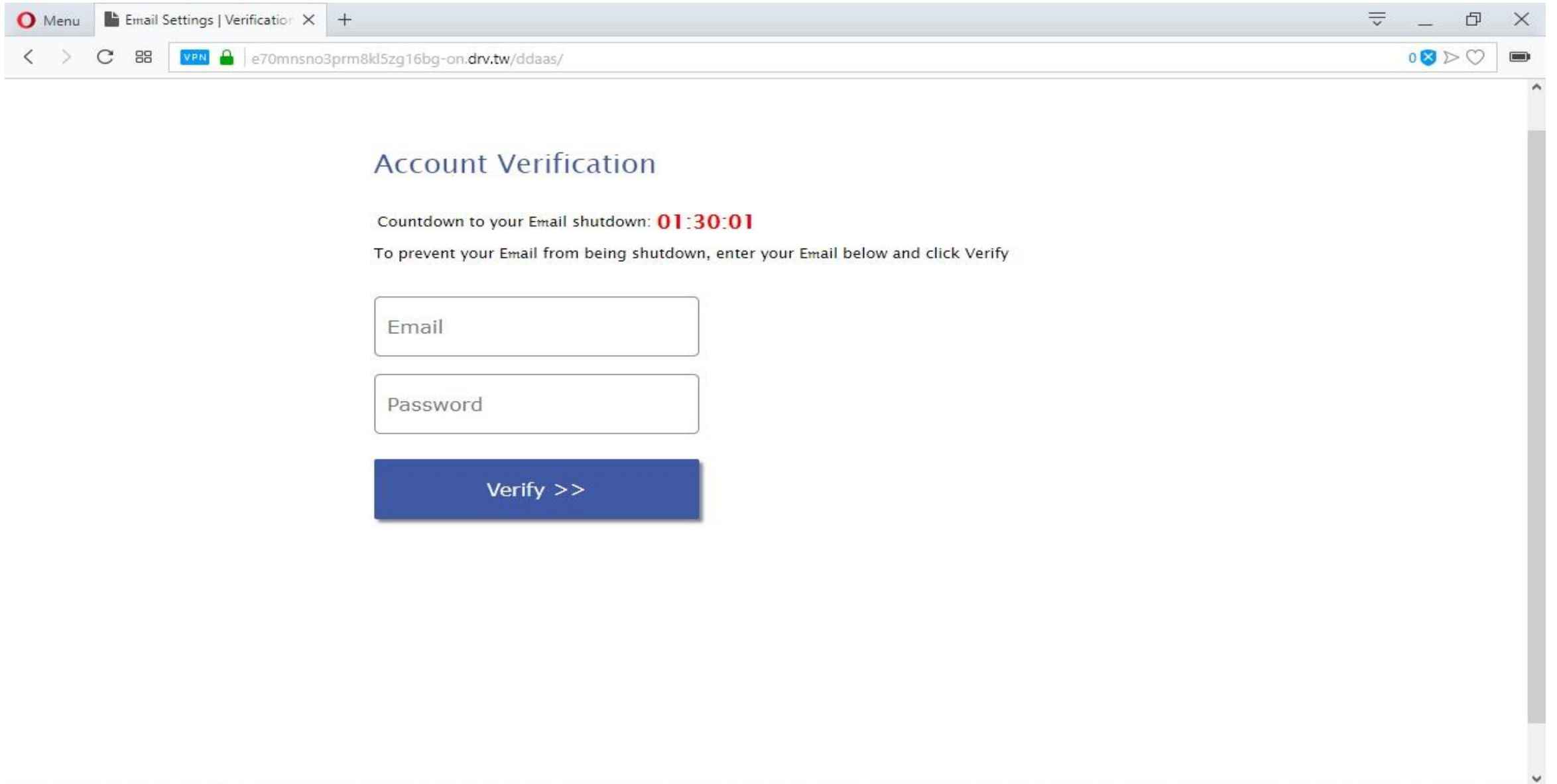
<https://e70mnsno3prm8kl5zg16bg-on.driv.tw/ddaas/>

Thanks,

# Phishing Mail sent to Govt. User



# Phishing Mail sent to Govt. User



# Phishing Mail sent to Govt. User

Menu Free email accounts | Register X +

VPN | www.mail.com 15 X > ♥

Note: We recommend using Firefox Quantum. [Download now for free!](#)

mail.com a 1&1 company Email News Tools More ▾ Enhanced by Google Search Sign up Log in

3 / 14

**Feds accuse vice officer of forcing women into sex**

**Weather**  
56° 53° [Show in C°](#)  
Cheney, KS, United States  
Tue 63° 38° AM Rain/Wind

**i** In order to enable essential services and functionality on our site and to collect data on how visitors interact with our site, products and services we use tools such as cookies. By using our website, you agree to our use of these tools for advertising and analytics. [More Info](#) **OK**

# Beware : Phishing Mail Common Traits

- ✓ Commonly used keywords in phishing mail subject – Pay commission, DA, Arrears, Parichay, VPN, IMPORTANT, UPDATE, PATCH, Upgradation of account, Account suspension, URGENT, Attention, CRASH, INVITATION
- ✓ Check for hyperlinked words and attachments
- ✓ **Use of shortened urls**
- ✓ **Links to files hosted on File Sharing sites/ Cloud storage (ex: google drive, onedrive..etc)**
- ✓ Re-direction to external sites
- ✓ Passwords for opening attachments enclosed in mail body
- ✓ **Mails sent to multiple recipients, mailing lists, bcc**

# Phishing Mail : What you can Do?

1. Report Phishing Incidents :

[incident@nic-cert.nic.in](mailto:incident@nic-cert.nic.in) / [incident@nic.in](mailto:incident@nic.in)

2. Don't open attachments and Don't click on the links and  
Don't Forward Phishing Mails to other users

3. Don't upload Phishing mail samples or attachments to  
external sites like Virustotal.com

What You Can Do?

# What is Cyber Hygiene?

1. Cyber hygiene refers to fundamental cybersecurity best practices that an organization's **security practitioners and users can undertake**. As you have personal hygiene practices to maintain your own health, **cyber hygiene best practices help protect the health of your organization's network and assets**.
2. Cyber hygiene is about training yourself to form good habits around cybersecurity so that you can stay ahead of cyber threats and online security issues.
3. Building a routine around **cyber hygiene will help prevent cybercriminals from causing security breaches or stealing personal information**. It will also help you keep up to date with software and operating systems.



# How to ensure good cyber hygiene?

## Regular routines or habits:

Cyber hygiene isn't a one-off event - it's something that has to be practiced regularly. You can create habits by setting automated reminders or adding dates to your calendars for different tasks. These might **include scanning for viruses using antivirus software, changing your passwords, keeping apps, software, and operating systems up to date, and wiping your hard drive after backup.**

Once you get the hang of cyber hygiene, it becomes part of your regular personal cybersecurity routine.



# How to ensure good cyber hygiene?

- **Don't post private information** such as home address, private pictures, phone number, or credit card numbers publicly on social media
- **Review your social media** privacy settings and ensure they are set to a level you feel comfortable with.
- **Avoid** quizzes, games, or surveys on social media that ask for **sensitive personal information**
- Take caution regarding the **permissions you accept** for all the apps you use.
- Keep computer and phone **locked with a password or PIN**
- Take care **not to disclose** private information when **using public Wi-Fi**
- **Make sure any online transactions** you make are via a **secure website** - where the URL **starts with https://** rather than http:// and there is a padlock icon to the left of the address bar.
- Share information about online privacy with family and friends to help keep them safe as well



# Cyber Security Is Everyone's Responsibility



# Securing Operating System Platform

## Do You Know ?

**83% of all Critical Vulnerabilities published by Microsoft during the last 5 years can be mitigated by using a non-admin User Account**



- 858 Microsoft Product Vulnerabilities were discovered in 2019
- Removing admin rights would mitigate 77% of all critical Microsoft vulnerabilities published in 2019
- 80% of Critical vulnerabilities in Windows Servers could be mitigated by using a non-admin user account.
- 100% of critical vulnerabilities in Internet Explorer could be mitigated by using a non-admin User account
- 80% of Critical Vulnerabilities in Windows 7, 8.1 and 10 could be mitigated by using a non-admin account



Keep your Operating System and Antivirus Updated with latest Patches/Updates



Create a non-admin account in your OS/ System and Use it for day to day activities



Don't use any Pirated Softwares or Cracks or Keygens.



Disable Powershell and Remote Desktop

**Report Security Incident to NIC-CERT :**



011-22902400

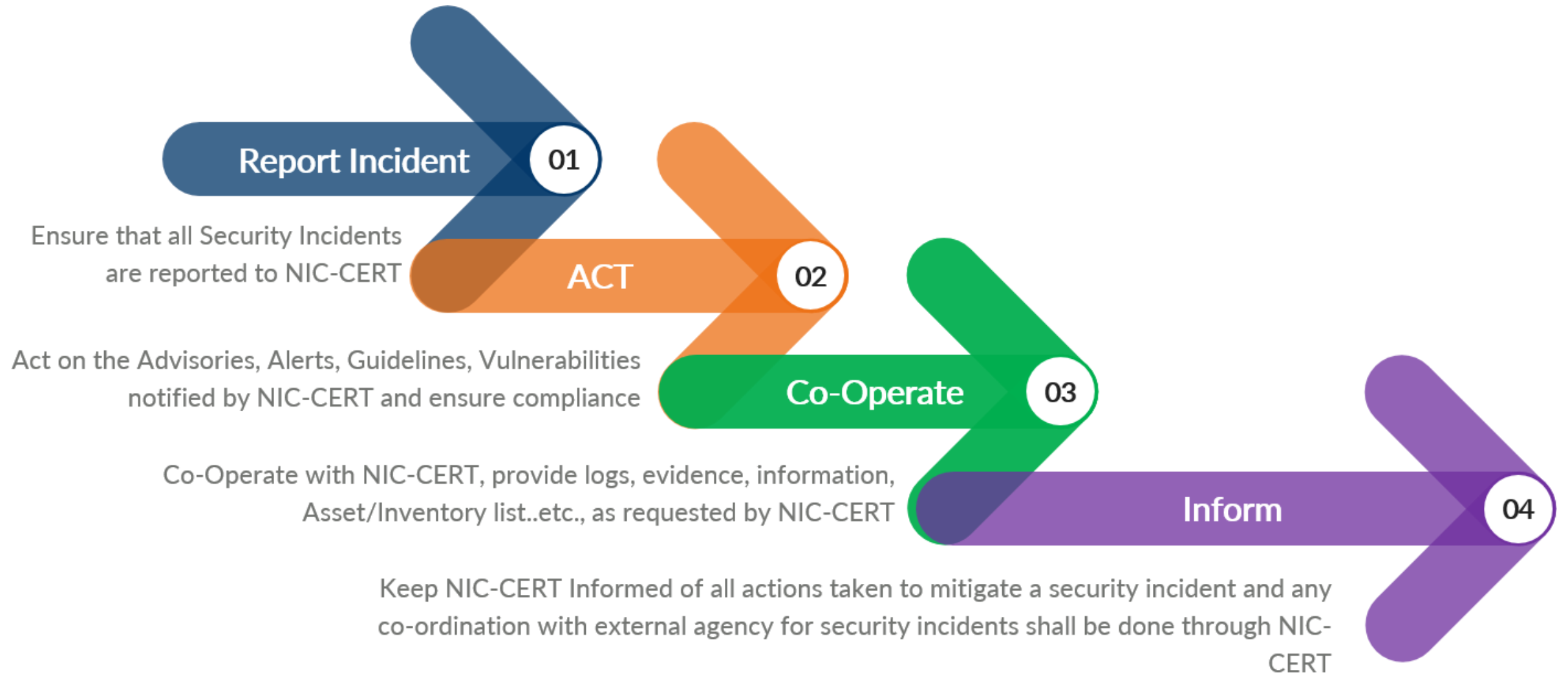


incident@nic-cert.nic.in



<https://nic-cert.nic.in>

# Co-ordination with NIC-CERT





# Thank You

[incident@nic-cert.nic.in](mailto:incident@nic-cert.nic.in)  
(+91) 011 22902400