Cybersecurity handbook: How attacks unfold and how to stop them

ZOHO

NIC National Informatics Centre

Did you know?

According to IBM[1], the global cost of a data breach is $4.4M.

Phishing

Modern phishing attacks rely on emails that use natural language, familiar branding, contextual cues, and personalization to appear trustworthy, tricking recipients into sharing credentials or clicking malicious links. Whether generated by humans, automated tools, or AI-assisted methods, these attacks are increasingly difficult to spot. Globally, only about 46% of employees were able to correctly identify AI-generated phishing emails.[2]

Ransomware

Ransomware attacks often start with a single click: when an employee opens a malicious attachment or link that installs malware inside the organization's network. Once inside, attackers spread to shared systems, encrypt critical servers and data, and disrupt business operations. These attacks are usually targeted towards businesses, government entities, and institutions that rely on continuous system availability and cannot afford prolonged downtime. In 2025, ransomware was involved in about 44% of reported breaches, up from roughly 32% in 2024, with an average impact of $5.08 million per incident.[3]

Insider threat

Insider threats involve people who already have legitimate access to company systems and data. These incidents can be intentional such as an employee misusing access to steal data or unintentional, caused by everyday actions like clicking a phishing link, using unapproved tools, or ignoring security procedures. Globally, 56% of organizations experienced at least one insider threat incident in the past year.[4]

Passwords

Passwords protect access to the systems and data that employees use every day. When they're weak, reused, or shared, attackers can log in as trusted users and operate unnoticed. In 2025, credential theft surged by ~160%, and stolen or exposed credentials now account for about one in five data breaches.[5]

Security breaches on physical infrastructures

2019

Kudankulam nuclear plant breach

The Dtrack malware infiltrated the IT network of India's nuclear power plant, exposing vulnerabilities in critical infrastructure.

2025

Cyber attack on Indian airports

Navigation systems at multiple Indian airports were affected by GPS spoofing, disrupting flights and highlighting vulnerabilities in in aviation systems.

Security breaches in 2025

In January 2025, a Pakistan-backed threat group[6] targeted researchers at the Defence Research and Development Organisation (DRDO) through a focused phishing campaign. The attackers sent emails containing PDF files that appeared legitimate but were embedded with malware, aiming to gain access to systems and extract sensitive defense-related information.

Meil Infrastructure Ltd., based in Hyderabad, lost approximately ₹5.5 crore in early 2025 after attackers impersonated trusted vendors and subtly altered email domains to manipulate payment instructions.[7]

In June 2025, a Pune-based auto-parts manufacturer[8] suffered a loss of ₹2.35 crore due to an invoice diversion attack, where criminals intercepted business communications and falsely claimed that a vendor's bank account was temporarily unavailable. The victim was persuaded to transfer funds to an alternate account controlled by the attackers, illustrating the effectiveness of "man-in-the-middle" style email deception in supply-chain fraud.

In February 2025, Mumbai-headquartered Alkem Laboratories disclosed a major business email compromise (BEC) incident that resulted in losses estimated at ₹22.31 crore.[9] In this case, fraudsters allegedly impersonated senior officials associated with Alkem's US subsidiary, using carefully crafted emails to authorize a series of high-value fund transfers to overseas bank accounts under their control.

How hackers target employees to attack government departments

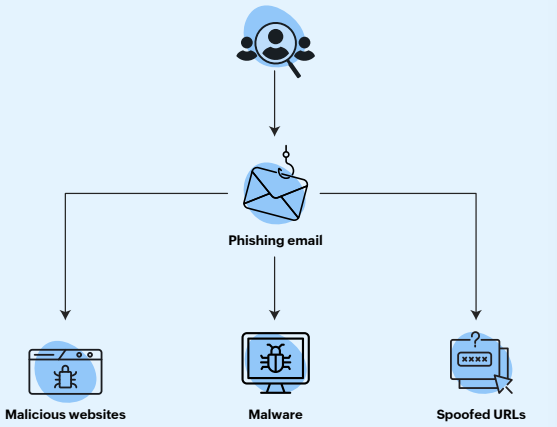
Cyberattacks are no longer just about hacking systems—they're about exploiting the human element within organisations. Employees often serve as both the first line of defence and the most targeted vulnerability. This playbook on how hackers target employees to attack government departments, uses the Cyber Kill Chain framework to break down the stages of an attack and highlight its progression.

Developed by Lockheed Martin, the Cyber Kill Chain is a framework designed to illustrate how cyberattacks unfold. By understanding this framework, employees can recognize the attacker's objectives, identify evolving threats at each stage, and take proactive measures to disrupt the attack.

Cyber Kill Chain

 **Reconnaissance**	The attacker collects information about the target.
 **Weaponisation**	Develops a malicious payload tailored to the target.
 **Delivery**	Transmits the malicious payload to the victim.
 **Exploitation**	Triggers and executes the malicious code.
 **Installation**	Installs malware on the target system.
 **Command and Control (C2)**	Establishes and maintains remote control over the compromised systems.
 **Actions on objectives**	Achieves the ultimate goals–data theft, disruption, or espionage.

PREPARATION



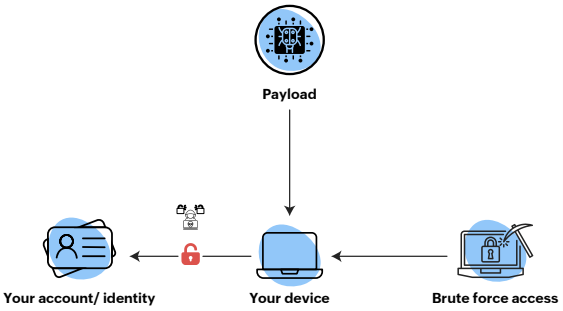
1. RECONNAISSANCE

Attackers gather information about their targets from government websites, public records, forums, and social media. They use this information to identify key individuals and craft highly targeted phishing emails.

2. WEAPONISATION

Attackers use phishing emails disguised as official government circulars, salary updates, or RTI requests. These emails often include malicious attachments like fake PDFs, policy documents, forms, or links to compromised websites resembling government portals to trick victims into downloading malware or sharing credentials.

INTRUSION



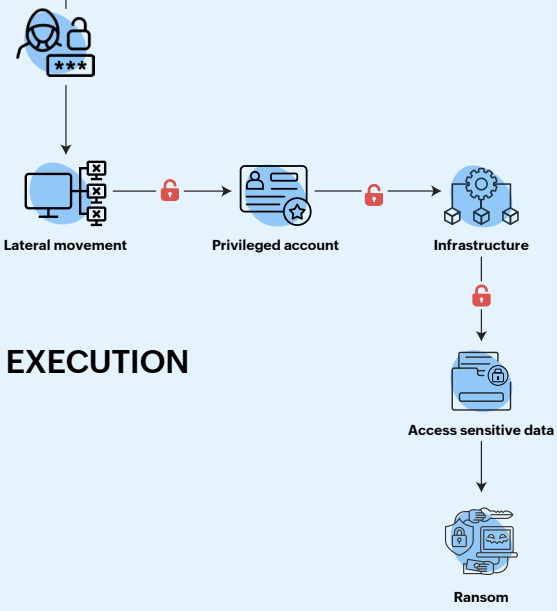
3. DELIVERY

Attackers proceed to deliver the malicious payload via phishing emails, exploiting vulnerabilities, brute-forcing passwords on government portals, or compromising weakly secured services such as email servers, VPNs, and internal dashboards.

4. EXPLOITATION

After delivering the payload onto the target device, attackers exploit vulnerabilities to gain unauthorised access to government accounts, official identities, or classified systems. They may compromise email credentials and access secure communication channels.

EXECUTION



5. COMMAND & CONTROL

Attackers control malware to spread across the network, targeting key systems like servers and domain controllers.

6. INSTALLATION

Using the compromised account, attackers send malicious emails or requests to unsuspecting colleagues, bosses, or officials. Attackers move deeper into others' devices and department systems, accessing sensitive government records/ files and high-level accounts. This process is known as lateral movement.

7. ACTIONS ON OBJECTIVES

Cybercriminals execute their goals by stealing sensitive government data, accessing classified files, disrupting critical services like e-governance portals, citizen databases, or demanding ransom to restore access.

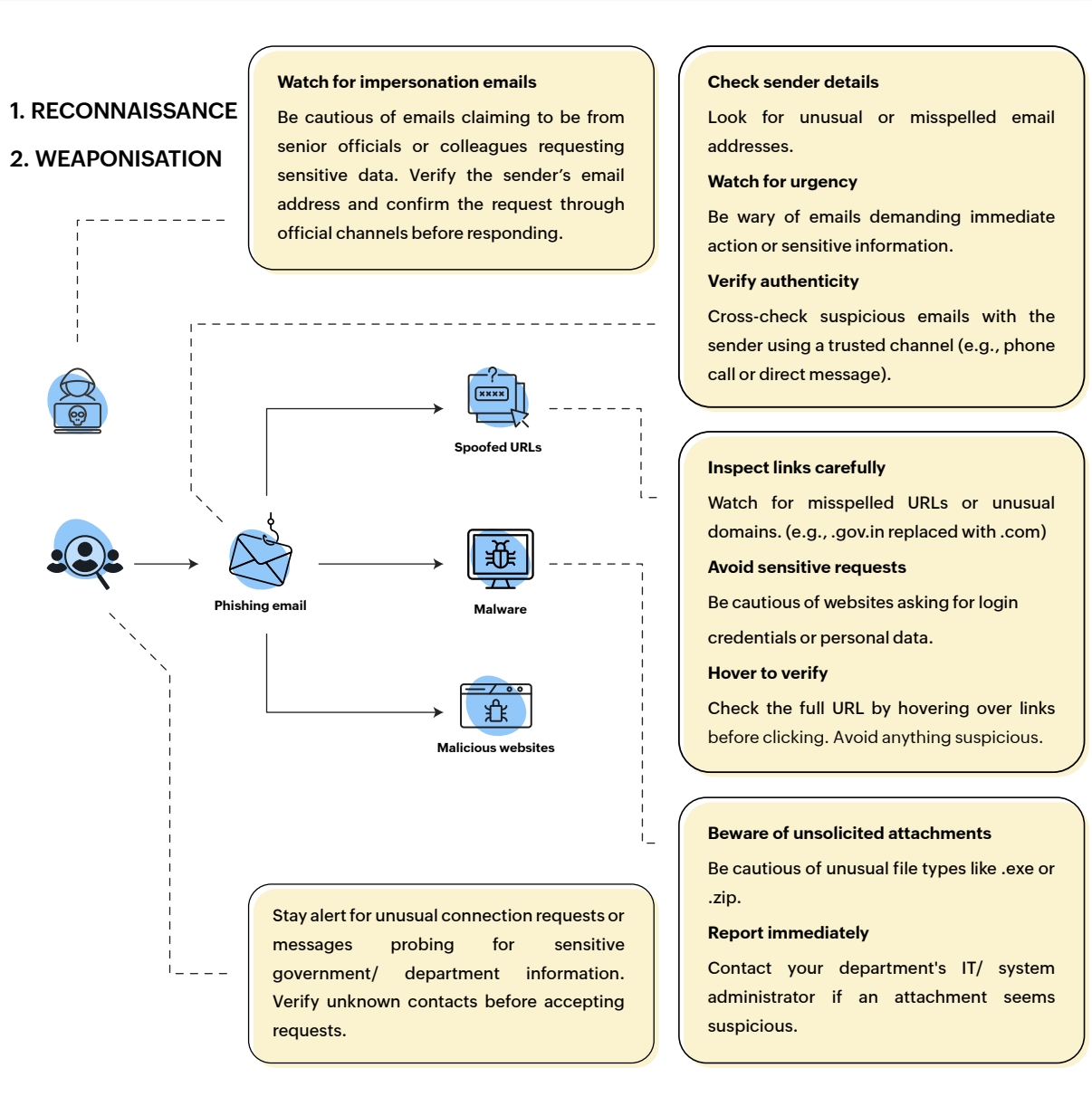
HOW HACKERS EXPLOIT EMPLOYEES IN CYBERATTACKS

The first line of defense

The preparation stage is a critical entry point for attackers and the best opportunity to intercept a potential breach. Research shows that 91% of cyberattacks start with a phishing email targeting unsuspecting employees.

Attackers exploit email's ability to create urgency and prompt action, tricking victims into clicking malicious links, downloading harmful attachments, or sharing sensitive information.

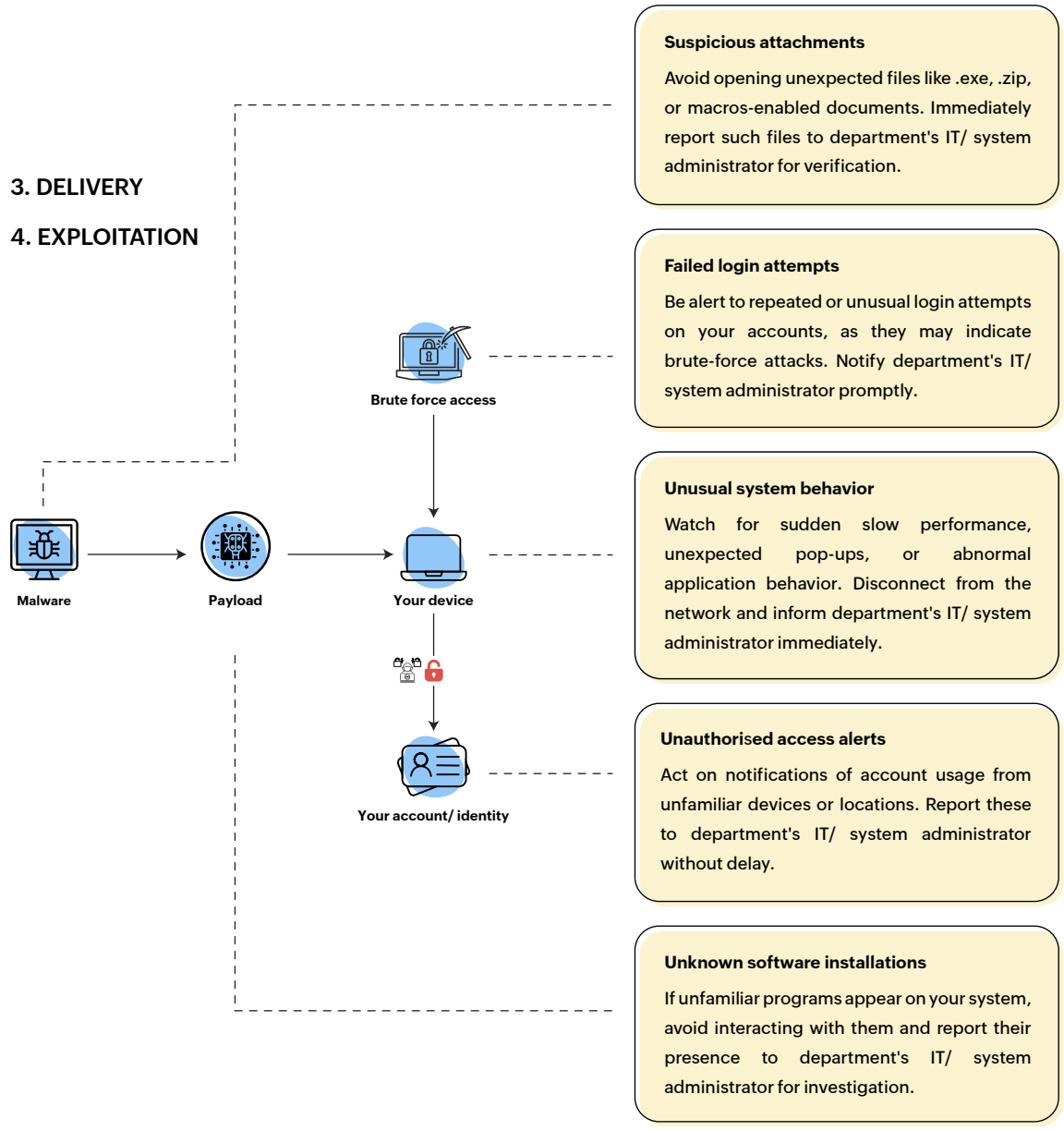
As the first line of defence, employees play a vital role in identifying and acting on early warning signs, preventing attackers from advancing and protecting the organisation from significant damage.



Detecting and responding to intrusions

In the intrusion stage, attackers deploy malicious payloads via phishing emails, exploit kits (automated tools for software vulnerabilities), or brute-force attacks (repeated password guessing). Once delivered, they exploit vulnerabilities to gain unauthorised access to accounts, systems, or identities.

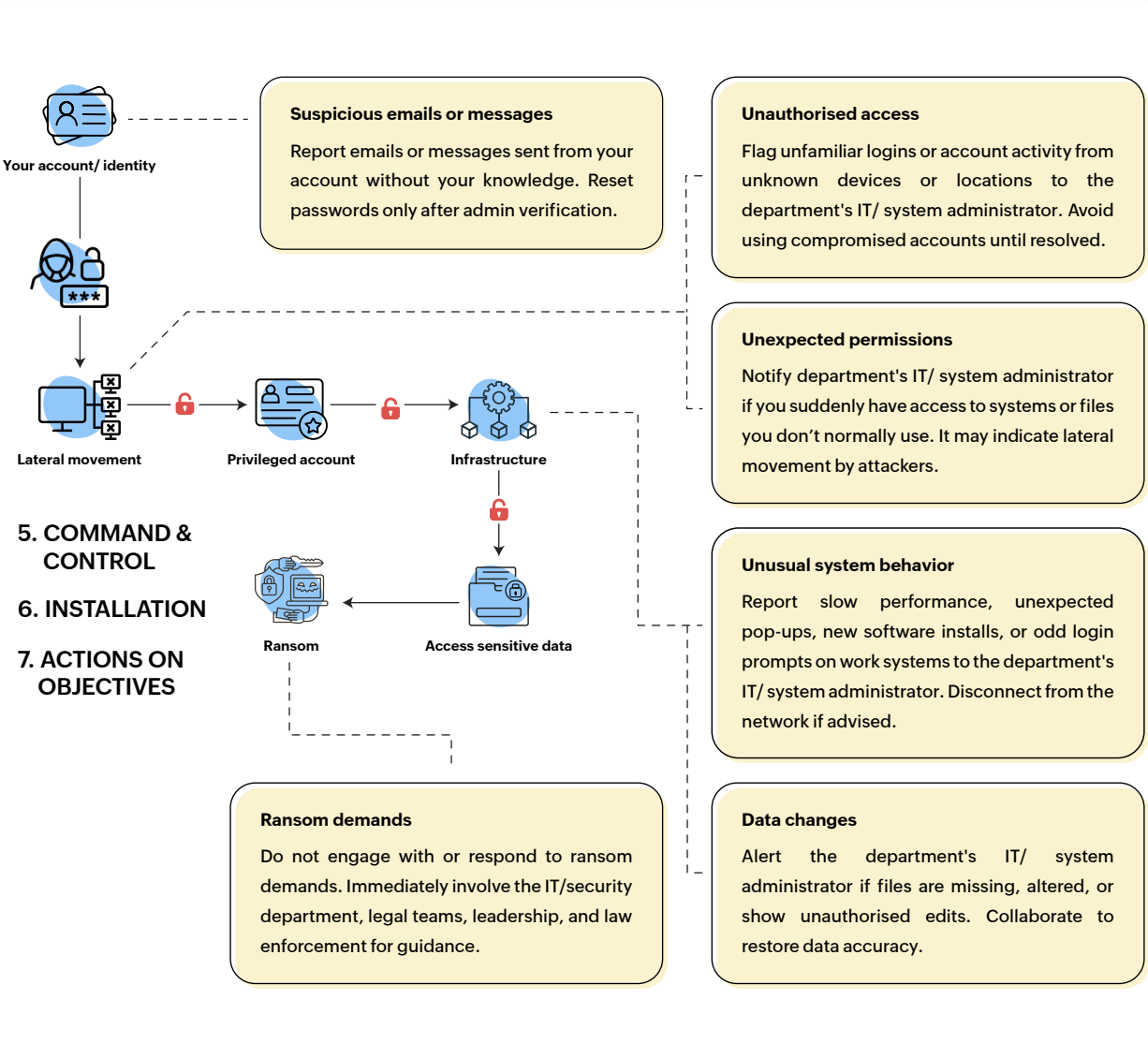
By this stage, attackers may have entered the system, exploited identities, and started lateral movement. Employees must watch for signs like unauthorised emails, login attempts, or unusual system behavior. Promptly reporting anomalies to IT or security department is vital to containing the threat and protecting the organisation.



Containing the breach

In this stage, attackers move from compromise to full exploitation, using compromised accounts and malware for deeper infiltration. They control malware to enable lateral movement, targeting high-value systems or privileged accounts. Once critical access is achieved, their objectives—such as data theft, operational disruption, or ransom demands—are executed.

This stage marks a turning point where a breach can cause significant damage. Employees must stay alert to unusual system activity (e.g., unexpected slowdowns, new software installations, or login prompts on work systems like computers, emails, or databases), unauthorised access, or changes in data integrity (e.g., missing, altered, or unauthorised edits in records). Prompt reporting and collaboration with IT and security department are key to limiting the attack's impact.



INDICATORS OF CYBERATTACK

By recognizing warning signs and responding swiftly, employees can prevent attacks from escalating, protect sensitive information, and strengthen organizational security.

How to report a cyber incident

Report Immediately: If you notice unusual activity, phishing attempts, or account compromise, inform your department's IT/ system administrator right away.

Report to CERT-In: Report the incident to CERT-In (Indian Computer Emergency Response Team), the national agency responsible for handling and preventing cyber incidents across government, at incident@cert-in.org.in.

Notify NIC-CERT: Simultaneously, report the issue to NIC-CERT, which specifically protects NIC systems and government networks, at incident@nic-cert.nic.in.

References

1. https://www.ibm.com/reports/data-breach
2. https://nypost.com/2025/10/03/tech/most-adults-couldnt-differentiate-between-authentic-ai-phishing-emails/
3. https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges
4. https://spycloud.com/resource/report/insider-threat-pulse-report-2025
5. https://www.itpro.com/security/cyber-attacks/credential-theft-has-surged-160-percent-in-2025
6. https://eventussecurity.com/cybersecurity/india/cyber-attacks/
7. https://timesofindia.indiatimes.com/city/hyderabad/infra-major-meil-loses-rs-5-5-cr-in-phishing-attack/articleshow/118258061.cms
8. https://cybersecuritynews.com/pune-auto-parts-firm-loses-%E2%82%B92-35-crore/
9. https://www.hindustantimes.com/cities/mumbai-news/alkem-labs-duped-of-22-cr-by-officials-of-its-us-arm-101738782831023.html

ZOHO

National Informatics Centre