Digital Forensics – FAFD Batch

(Forensic Accounting and Fraud Detection)

For businesses,
a cyber-attack is not a matter of
“IF”
but
“WHEN”

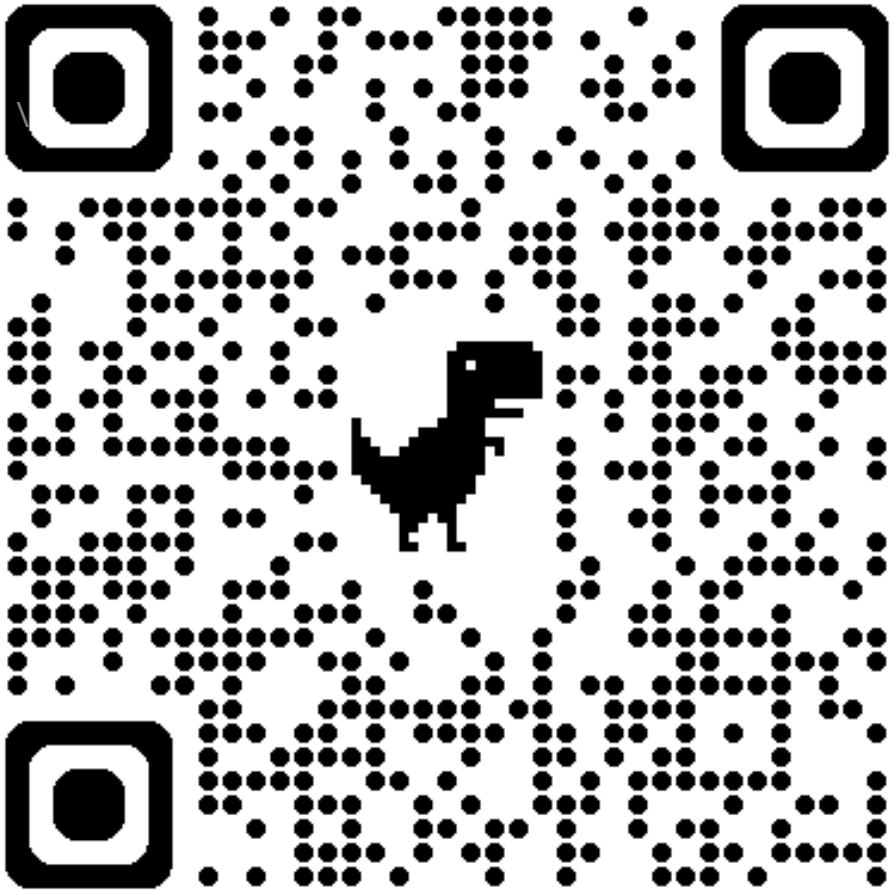
#	Session Agenda
1	Introduction to Digital Forensics
2	Cybersecurity & Forensics
3	Digital Forensics – Investigation Process
4	Notable Cybercrimes & their Modus Operandi (MO)
5	IT ACT 2000, Digital Personal Data Protection (DPDP) Act

Introduction

Digital Forensics in Today’s Context

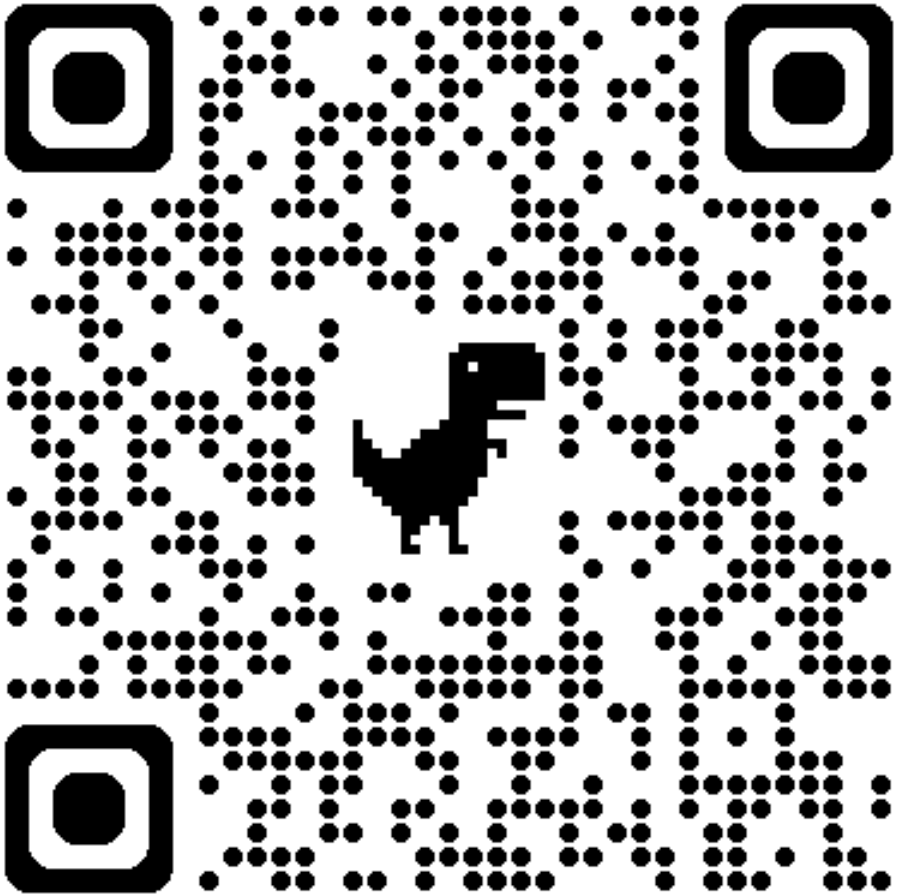
(1) PwC's Global Economic Crime Survey 2024

https://www.pwc.in/pwcs-global-economic-crime-survey-2024-india-outlook.html



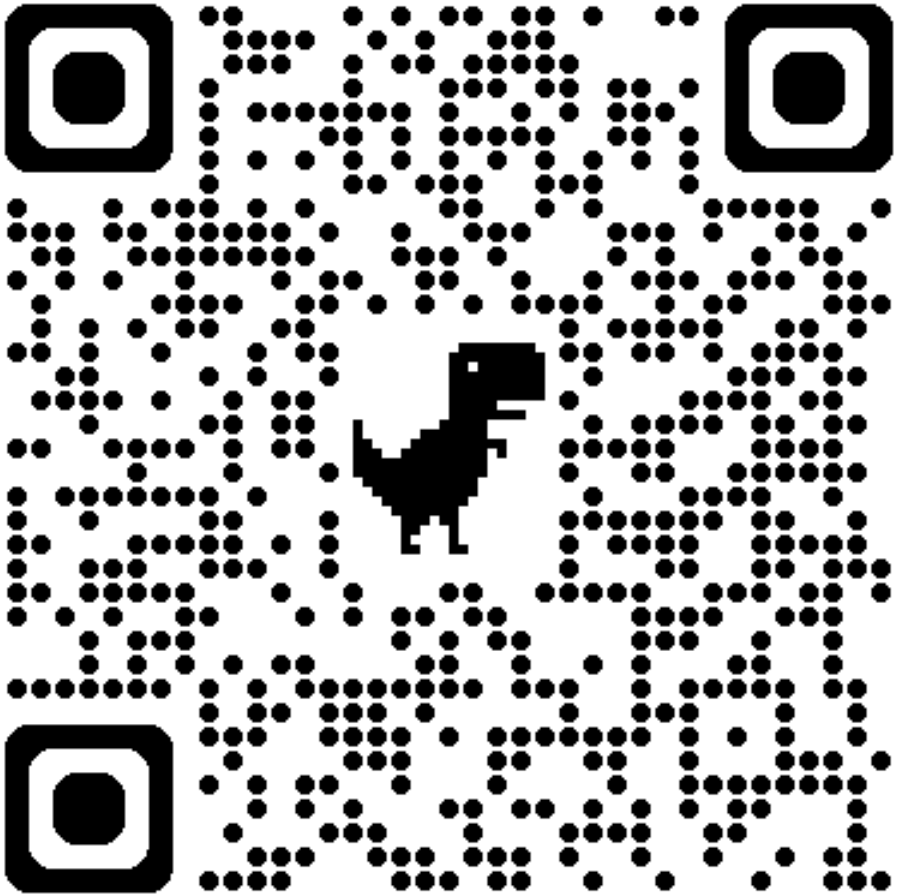
(2) Financial and Cyber Fraud Report 2024

https://www.grantthornton.in/insights/financial-and-cyber-fraud-report-2024/



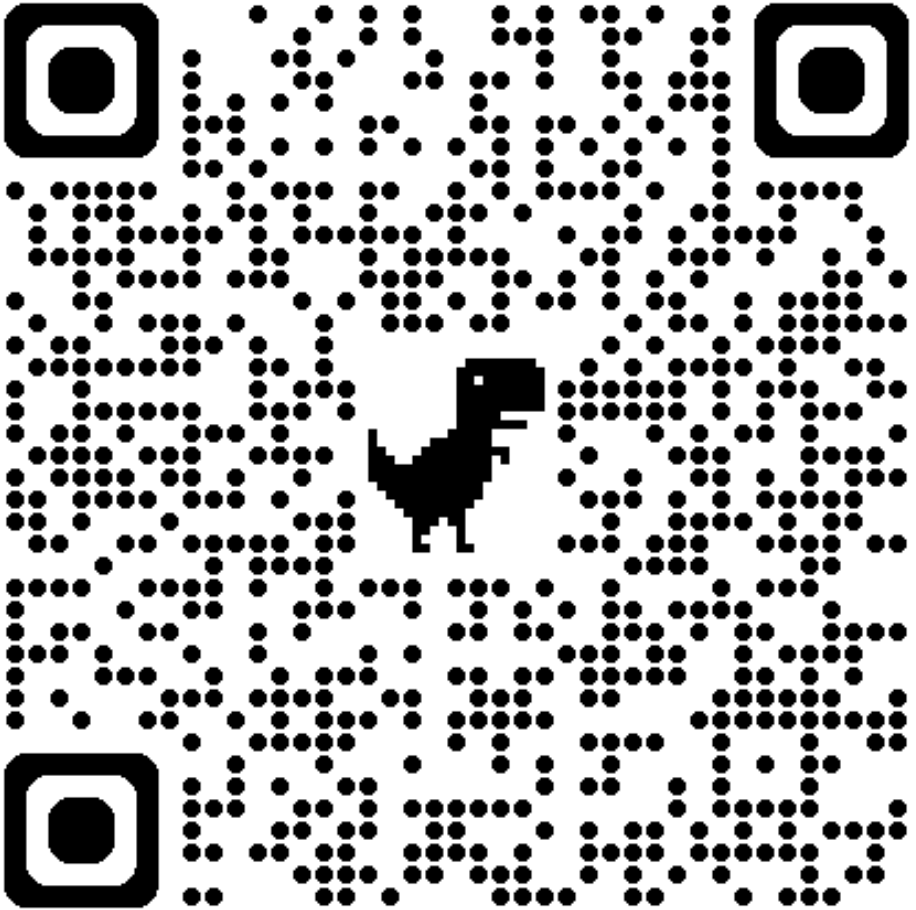
(3) How exposed do you believe your company will be to the following key threats in the next 12 months?

https://www.pwc.com/gx/en/ceo-survey/2025/28th-ceo-survey.pdf



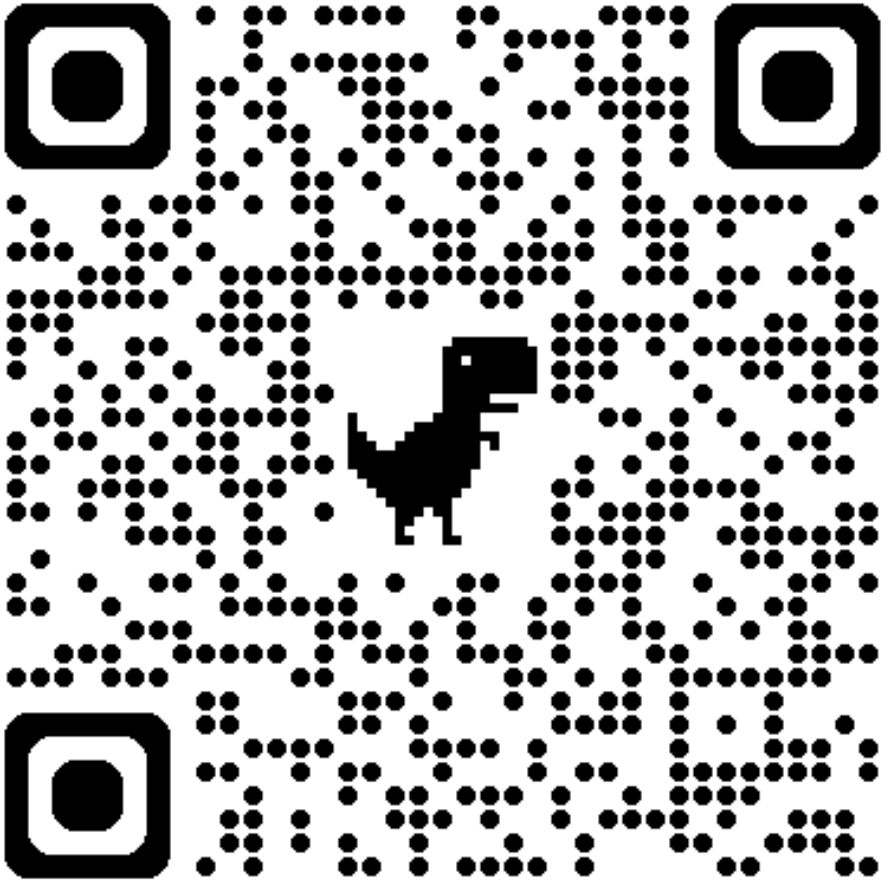
(4) Cost of a Data Breach Report 2024 (IBM)

https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf



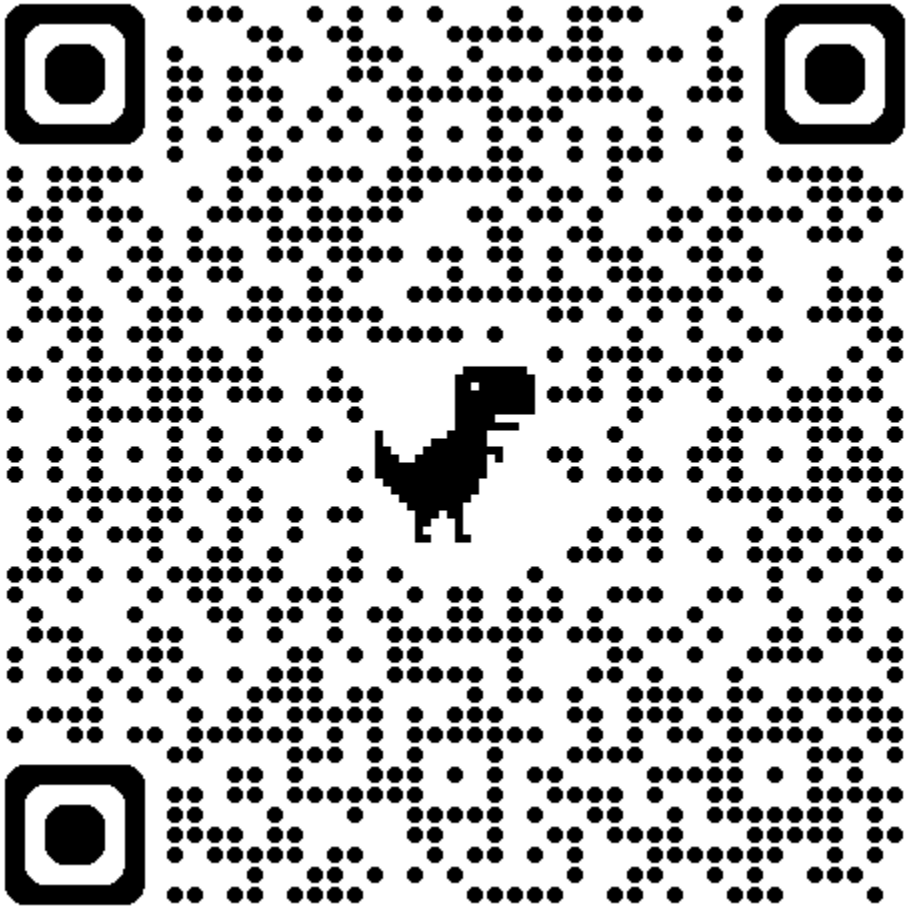
(5) Digital 2025

https://wearesocial.com/wp-content/uploads/2025/02/GDR-2025-v2.pdf



(6) Cybersecurity Trends: Resilience Through Transformation

https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends



Digital Forensics vis-à-vis Forensic Audit

Understanding the fitment of Digital Forensics in Audit

'Forensic Audit' is generally taken to refer to a comprehensive view of fraud investigation, including

- Forensic Accounting - The audit of accounting records and systems to prove or disprove fraud
- **Digital Forensics**
- Investigation
- Litigation Support

Issue	Financial Audits	Forensic Audits
Frequency	Recurring	Incidental & Nonrecurring
Objective	Compliance Advisory & Control	Culpability & Liability Investigation, Compliance
Scope	Generic & Broad – Random Sampling; Fair View	Specific Data Set; Exact & Precise
Relationship with Client	Non-adversarial	Adversarial
Methodology & Process	Accounting Standards	Accounting Standards, IT standards, Industry-Specific Standards
Presumption	Professional Skepticism	Evidence-based

Digital Forensics – What?

Understanding this field beyond just methods, procedures & techniques

Digital forensics deals with the process of finding evidence related to a digital crime to find the culprits and initiate legal action against them.

OBJECTIVES

- Identify, gather, and preserve the evidence of a cybercrime.
- Track and prosecute the perpetrators in a court of law.
- Interpret, document and present the evidence to be admissible during prosecution.
- Estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator.
- Find vulnerabilities and security loopholes that help attackers.
- Understand the techniques and methods used by attackers to avert prosecution and overcome them.
- Recover deleted files, hidden files, and temporary data that could be used as evidence.
- Perform incident response to prevent further loss of intellectual property, finances and reputation during an attack.

Digital Forensics – When?

When do organizations seek the help of computer forensics

- Prepare for incidents by securing and strengthening the defense mechanism as well as filling the holes in security
- Gain knowledge of the regulations and comply with them.
- Report the incidence of a breach of contract.
- Identify the actions needed as incident response.
- Act against copyright and intellectual property theft/misuse.
- Settle disputes among employees or between the employer and employees.
- Estimate and minimize the damage to resources.
- Set a security parameter and create the security norms for forensic readiness

Digital Forensics – Where?

Where do we apply the Forensics skills and techniques

Fundamental Principle

- Nulla poena sine lege (Latin for "no penalty without a law")

Elements for an act to become a cybercrime

- The conduct is *facilitated by information and communications technology*;
- The conduct is *motivated by intent to commit harm against a person or organization*;
- The perpetrated or intended harm encompasses conduct amounting to *interference or damage to either tangible or intangible* property owned by a person or organization;
- The conduct concerned is criminalized within either the jurisdiction of the victim or the jurisdiction of the accused.

Types of attack

- Internal attacks
- External attacks

Digital Forensics – Challenges

Cyber-crimes pose new challenges for investigators

- **Speed:** Advancement in technology has boosted the speed with which cyber crimes are committed, whereas investigators require authorization and warrants before starting legal procedure.
- **Anonymity:** Cyber criminals can easily hide their identity by masquerading as some other entity or by hiding their IP addresses using proxies
- **Volatile nature of evidence:** Most of the digital evidence can be easily lost as it is in the form of volatile data such as rotational logs, records, light pulses, radio signals or other means.
- **Evidence Size and Complexity:** Diversity and distributed nature of digital devices results in increased size of evidence data and complexity.
- **Anti-Digital Forensics (ADF):** Attackers are increasingly using encryption and data hiding techniques to hide digital evidence.
- **Global origin and difference in laws:** The perpetrators can initiate the crime from any part of the world, whereas the authorities have jurisdiction over domestic crimes only.
- **Limited legal understanding:** Many victims are unaware of the law violated during the incident and fail to defend their claim.

Digital Forensics – Rules

Certain rules to follow during a digital forensic examination

- Limited access and examination of the **original evidence**
- Record **changes** made to the evidence files
- Create a **chain of custody** document
- Set **standards** for investigating the evidence
- Comply with the **standards**
- Hire **professionals** for analysis of evidence
- Evidence should be strictly **related** to the incident
- The evidence should comply with the **jurisdiction** standards
- Document the **procedures** applied on the evidence
- Securely **store** the evidence
- Use recognized **tools** for analysis

Understanding Digital Evidence

Digital Evidence is any information of probative value that is either stored or transmitted in a digital form

Digital Information can be gathered while examining digital storage media, monitoring the network traffic, or making duplicate copies of digital data found during forensics investigation

Digital evidence is circumstantial and fragile in nature, which makes it difficult for a forensic investigator to trace criminal activities

Locard's Exchange Principle “anyone or anything, entering a crime scene - takes something of the scene with them, AND leave something of themselves behind when they leave.”

Types of Digital Evidence

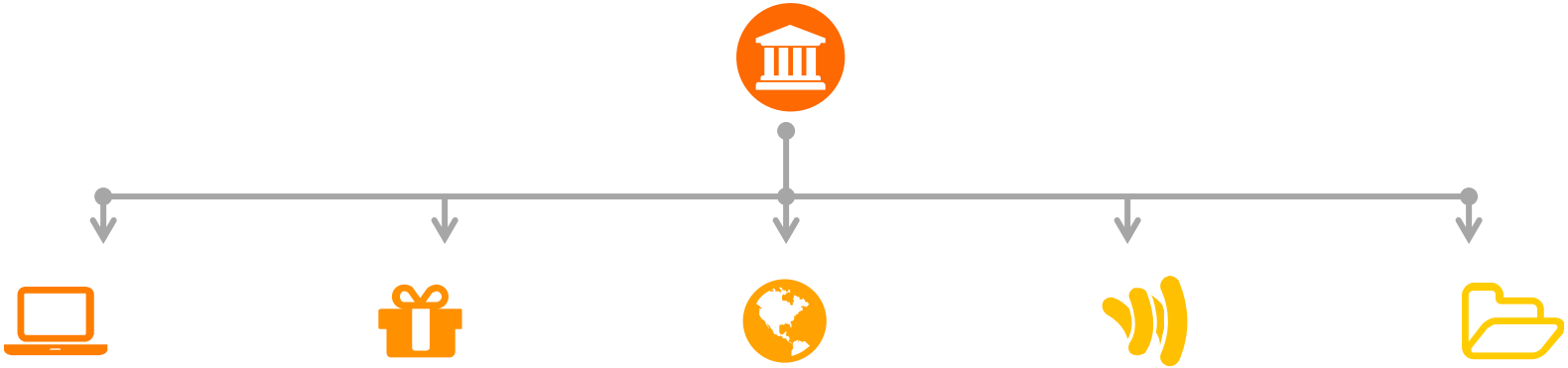
Volatile Data

Data that is lost as soon as the device is powered off. Examples include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.

Non-Volatile Data

Persistent data that is stored on secondary storage devices such as hard disks and memory cards. Examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, event logs, etc.

Characteristics of Digital Evidence



Admissible

Evidence must be real and related to the incident in a proper way

Authentic

Evidence must be authentic in nature & shouldn't be artificially

Complete

The evidence must prove the attacker's actions or his innocence

Reliable

There must be no doubt about the authenticity or veracity of the evidence

Believable

Evidence must be clear and understandable by the judges or authorities

Forensics Examiner – Profile

Tasks performed by a forensics investigator

- Evaluates the damages of a security breach
- Identifies and recovers data required for investigation
- Extracts the evidence in a forensically sound manner
- Ensures proper handling of the evidence
- Acts as a guide to the investigation team
- Creates reports and documents about the investigation required to present in a court of law
- Reconstructs the damaged storage devices and uncovers the information hidden on the computer
- Updates the organization about various methods of attack and data recovery techniques, and maintains a record of them (following a variant of methods to document) regularly
- Addresses the issue in a court of law and attempts to win the case by testifying in court

Soft Digital Forensics Investigative Skill Sets

Soft Skill	Competency
Communicative	Liaise with the public, other team members, court staff, lawyers, law enforcement personnel, and other interlocutors.
Rational	Swiftly assess a situation and make appropriate decisions.
Collaborative	Rapidly gain the confidence of others and sustain those relationships.
Intuitive	Instinctively differentiate between normal and abnormal events.
Coherent	Explain technical subject matter in plain language and make information accessible to diverse audiences.
Resilient	Prioritize and maintain composure whilst working under pressure.
Punctual	Meet deadlines and provide deliverables to specification.
Fastidious	Maintain focus with persistent attention to detail.
Disciplined	Restrained work ethic with strict observance to directives and mindfulness of personal and technical limitations.
Strategic	Formulate and ask probing questions to key stakeholders and devise plans, which bring value to an inquiry.

Hard Digital Forensics Investigative Skill Sets (1/2)

Tech Skill	Competency
Evidence Continuity	Strict compliance with established processes for demonstrating chain-of-custody when handling electronically stored information.
Forensic Imaging	Applied knowledge of data preservation techniques, which use both physical and logical methods to forensically acquire data and verify sources of information.
Networking Architecture	Practical understanding of the Open System Interconnection (OSI) model and the function of communication technologies in the storage and transmission of data, such as network protocols, media access control (MAC) addresses, firewalls, routers,
Hardware	Applied knowledge of components and peripherals connected to information systems, including hard disk drives, solid state drives (SSDs), random access memory (RAM), the basic input output system (BIOS), network interface cards (NICs), chipsets, and flash storage.
File Systems	Applied knowledge of diverse file system attributes such as FAT, FAT32, exFAT, NTFS, HFS+, XFS, Ext2, Ext3, Ext4, and UFS.

Hard Digital Forensics Investigative Skill Sets (2/2)

Tech Skill	Competency
Structured Data Analysis	Retrieval and interpretation of universally formatted information, such as fixed field entries inside records, as well as embedded information associated with operating systems, *relational databases, spreadsheets, registries, Internet history, security and system logs, and encrypted file systems*.
Unstructured Data Analysis	Interpretation of values associated with detached files stored across various file systems such as *digital photos, graphic images, videos, streaming data, webpages, PDF files, PowerPoint presentations, email data, blog entries, wikis, and word processing documents*.
Semi-structured Data Analysis	Extraction of tags, metadata, or other types of identity markers subsisting within detached files, including *information indicative of authorship, revision number, creator, sender, recipient, time and date particulars, GPS coordinates, keywords, and firmware version*. This activity also extends to analysis of relational data within files that are associated with detached files, such as *XML* and other markup languages.

Cybersecurity and Forensics

Protection against cybercrime

What is cybersecurity?

It is no longer just an IT challenge – it is a business imperative!

- ***Broader*** than just information technology and ***extends*** beyond the enterprise
- ***Increasingly vulnerable*** due to technology connectivity and dependency
- An 'outside-in view' of ***the threats*** *and* ***business impact*** facing an organization
- Shared responsibility that requires ***cross functional disciplines*** in order to plan, protect, defend, react and respond

Core Principles

The CIA Triad

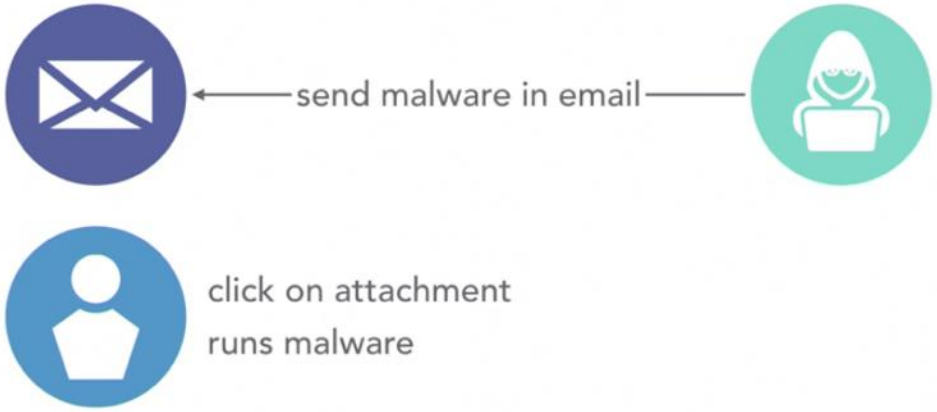
Confidentiality	Integrity	Availability	Authentication
- Encryption	- Hashing	- Backups	- MFA / 2FA

In a multi-factor authentication scheme, two or more of these are combined:

- something you know (e.g. password)
- something you are (e.g. Biometrics)
- something you have (e.g. OTP on phone)

Cyber Attacks

The Ones that break the Organizational Security

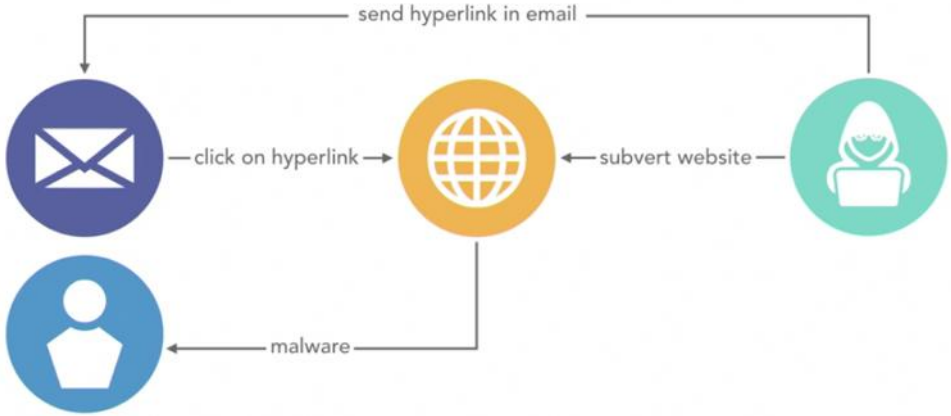


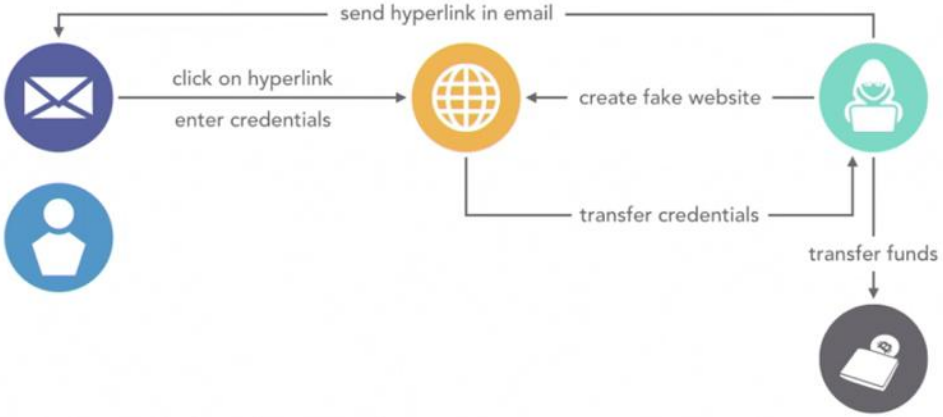
Email phishing

One of the most successful forms of attack

Malicious website

Hosting malware or a legitimate website which has been compromised by a hacker without the owner's knowledge.



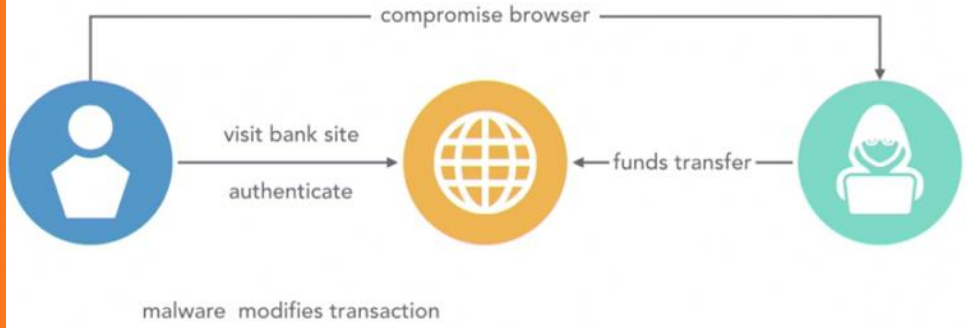


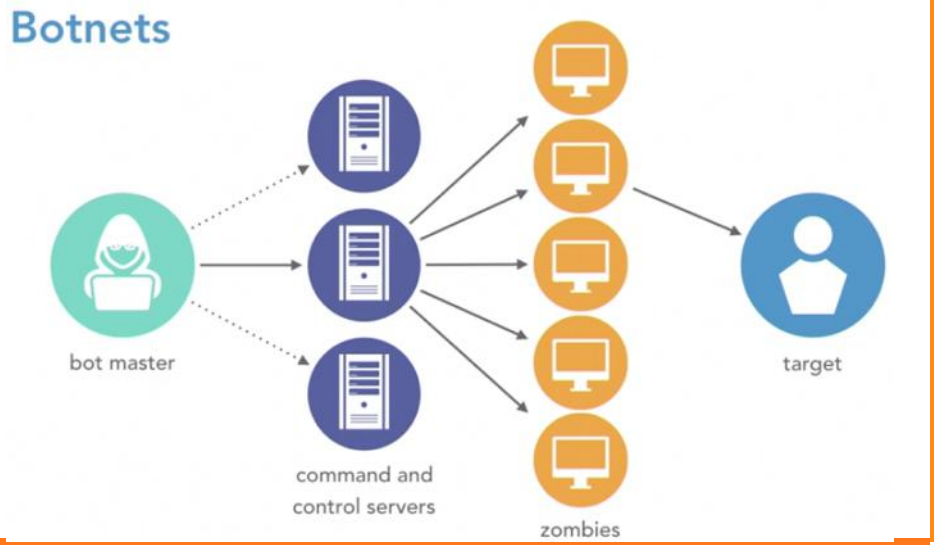
Fake Website

Site looks like a real website but is in fact run by the hacker

Hacker in the Middle

The malware will change the transactions to effect a funds transfer to the hacker's own account.



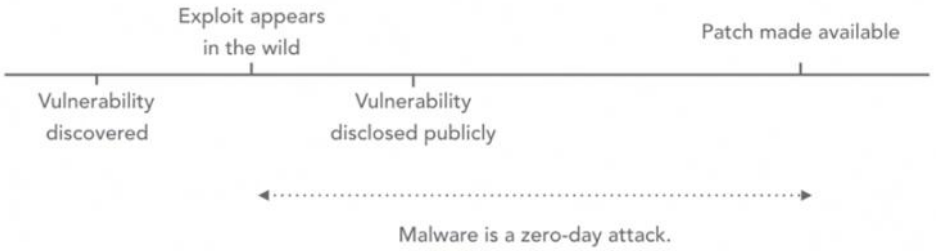


Botnet

Manage their command and control servers, which in turn are used to control a vast number of compromised computers, known as zombies, all around the world

Software flaws

Minimizing a system's exposure to the internet helps reduce the risk of the zero day being exploited



Protocol spoofing

Impersonates another entity on the network

IP Address Spoof

Spoofing an IP address will conceal the actual IP

ARP Spoofing

With ARP spoofing, a fake or spoofed MAC address is placed on the LAN

DNS spoofing

A spoof will modify the DNS server cache

Email Spoofing

makes an email look like it came from someone else

Insider Threat

It may not be what you think

Categories of Insider Threats

What is an Insider Threat and how it affects you

Compromised

Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.

Negligent

Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.

Malicious

Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

Insider Threat

How to protect yourself and your organization

Exploiting information via remote access software

Third-party threats

Careless use of wireless networks

Posting information to discussion boards and blogs

Leaking data via email and instant messaging

Insecure file sharing

Cyber Defense

Getting it Right

Email Phishing - Check

Three things to protect from phishing attacks

01

Check Sender & Message

- Is this really from your friend or an organization that you do business?
- Look at the message body. Are the text and graphics as authentic as others you've received from this sender before?
- Are you being asked to transfer money or sensitive data?
- Now hover your mouse over any links in the message. Does the URL match what you see in the message?

02

Move the message out

- If you find it suspicious then don't click on any links, don't open any email attachments
- Close the message
- Forward it to company IT Support.
- Mark it as SPAM and/or DELETE it

03

Stay protected

- Never say yes to an unexpected prompt to install or update software.
- Enable host firewall & anti-malware tool on your machine.
- Enable pop-up blocker on your browsers.

Email Phishing - Technical Countermeasures

Three things to protect from phishing attacks

01

Sender Policy Framework (SPF)

Sender policy framework authenticates by comparing records in the appropriate DNS record and helps prevent phishing emails and forgery *E.g. v=spf1 include:amazonses.com ~all*

02

Domain Keys Identified Mail (DKIM)

Senders sign the email with a digital signature to ensure authenticity, and then the receivers verify this.

03

Domain Message Authentication Reporting and Conformance (DMARC)

Email authentication policy that uses sender policy framework and/or DKIM, to establish the sender's identity. *E.g. v=DMARC1;p=quarantine;pct=100;fo=1*

Antimalware Protection

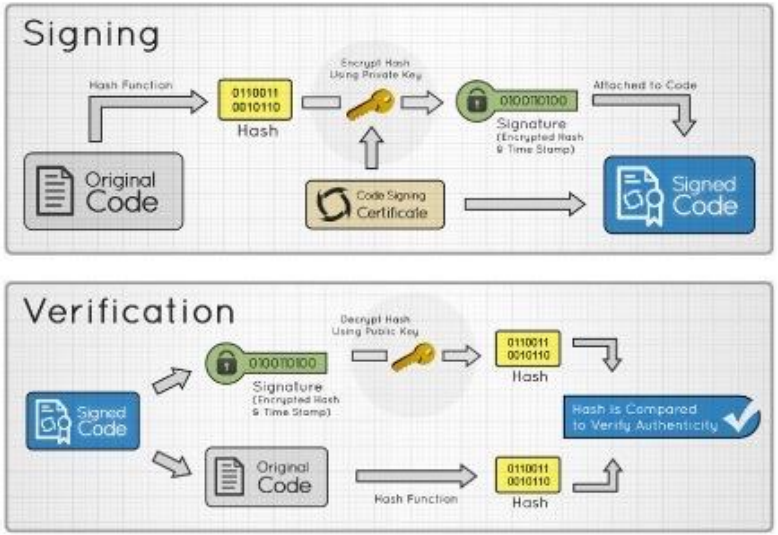
Adding to the Defence in Depth

01 Antivirus is signature based, a database of signatures that identify known malware like the unique file hash of a malicious binary or the file associated with an infection.

02 Binary whitelisting software operates off a white list. It's a list of known good and trusted software and only things that are on the list are permitted to run. Everything else is blocked.

03 Software signing or code signing, where a software vendor can cryptographically sign binaries, they distribute using a private key.

04 If the hash matches and the public key is trusted, then the software can be verified that it came from someone with the software vendor's code signing private key.



Full-disk encryption (FDE)

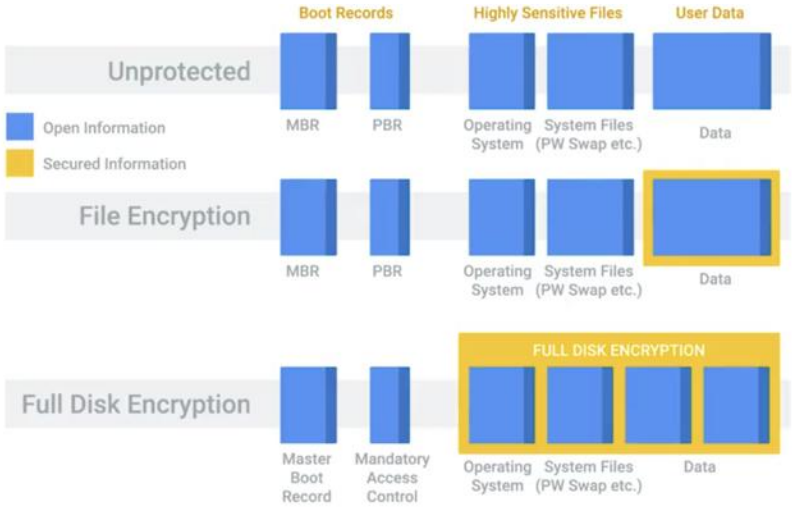
Adding to the Defence in Depth

01 Having the disk fully encrypted protects from data theft and unauthorized tampering even if an attacker has physical access to the disk

02 Bit Locker and FileVault 2, PGP, TrueCrypt, VeraCrypt are some examples

03 Full-disk encryption schemes rely on the secret key for actual encryption and decryption operations. In many cases, this might be the same as the user account password.

04 Home directory or file-based encryption only guarantees confidentiality and integrity of files protected by encryption. These setups usually don't encrypt system files.



Password Alert (by Google)

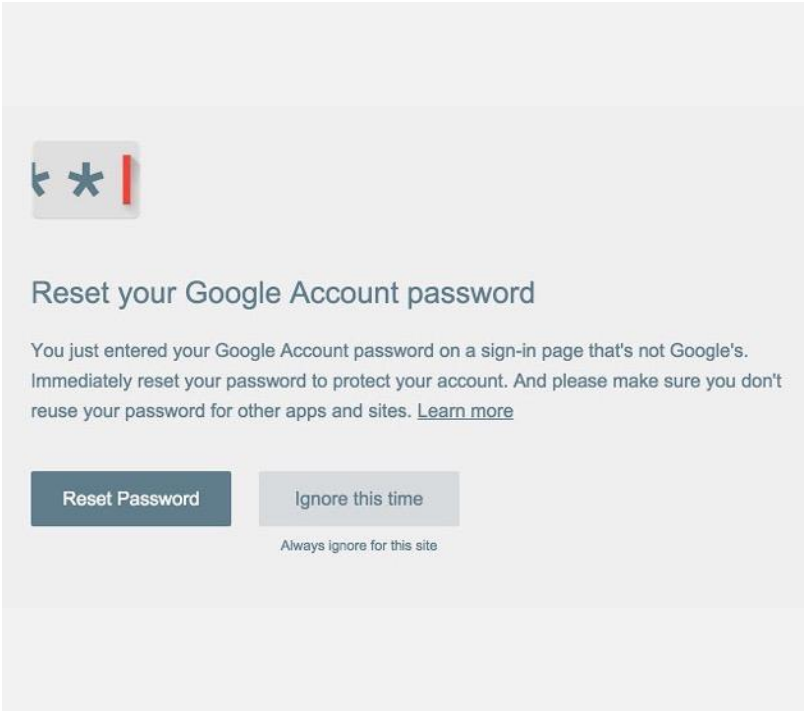
Password Alert helps keep your Google Account safe

01 Password Alert helps protect against phishing attacks.

02 Once you've turned Password Alert on, you'll get an alert any time your Google Account password is used to sign-in to a non-Google site.

03 Password Alert also checks each page you visit to see if it's impersonating Google's sign-in page and alerts you if so.

04 Password Alert doesn't store your password or keystrokes -- instead, it stores a secure thumbnail of your password, which it compares against a thumbnail of your most recent keystrokes within Chrome.



Firefox Monitor

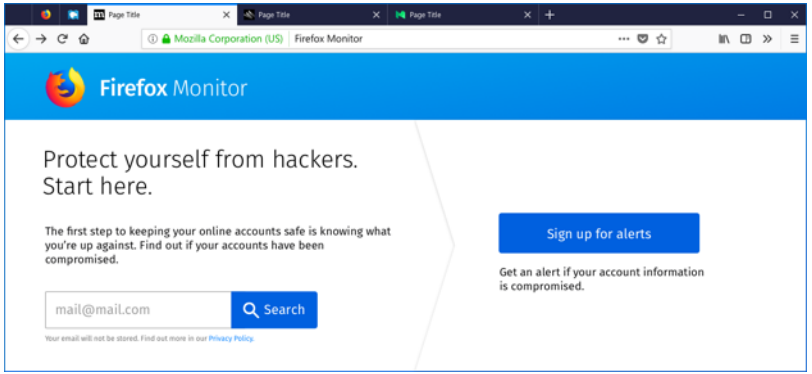
Get alerted if your email address appears in a new breach

01 Firefox Monitor warns you if your email address has been exposed in an online data breach.

02 Search for your email address in public data breaches going back to 2007.

03 Create a Firefox Account to monitor your email for ongoing breaches.

04 Receive a full report of past breaches, including sensitive breaches.



Keyword Alert

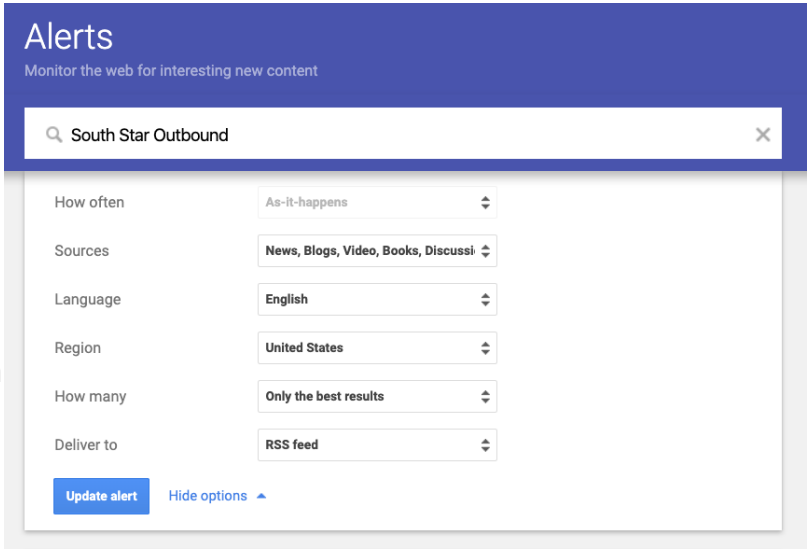
How to Set Up Google Alerts

01 Keep tabs on what others are saying online about your business

02 Set up an individual alert for each variation of your brand name. (Include potential misspellings. Common ones include inserting a space within a single compound word or adding an ‘s’ to a word.)

03 If you want to keep close tabs on Facebook or Yelp, you can use the site: operator by inserting one of the following search strings in the alert box: site:facebook.com SouthStar

04 You can also monitor your employees using the same techniques, just substituting their names for yours



Digital Forensics

Investigation Process

Phases in Digital Forensics

Phases Involved in the Computer Forensics Investigation Process

Pre-investigation

Planning the process, defining mission goals, and securing the case perimeter and devices involved

Investigation

Involves **acquisition**, **preservation**, and **analysis** of the evidentiary data to identify the source of crime and the culprit

Post-investigation

Deals with the **reporting** & **documentation** of all the actions undertaken and findings during an investigation

Digital Forensics – Checklist

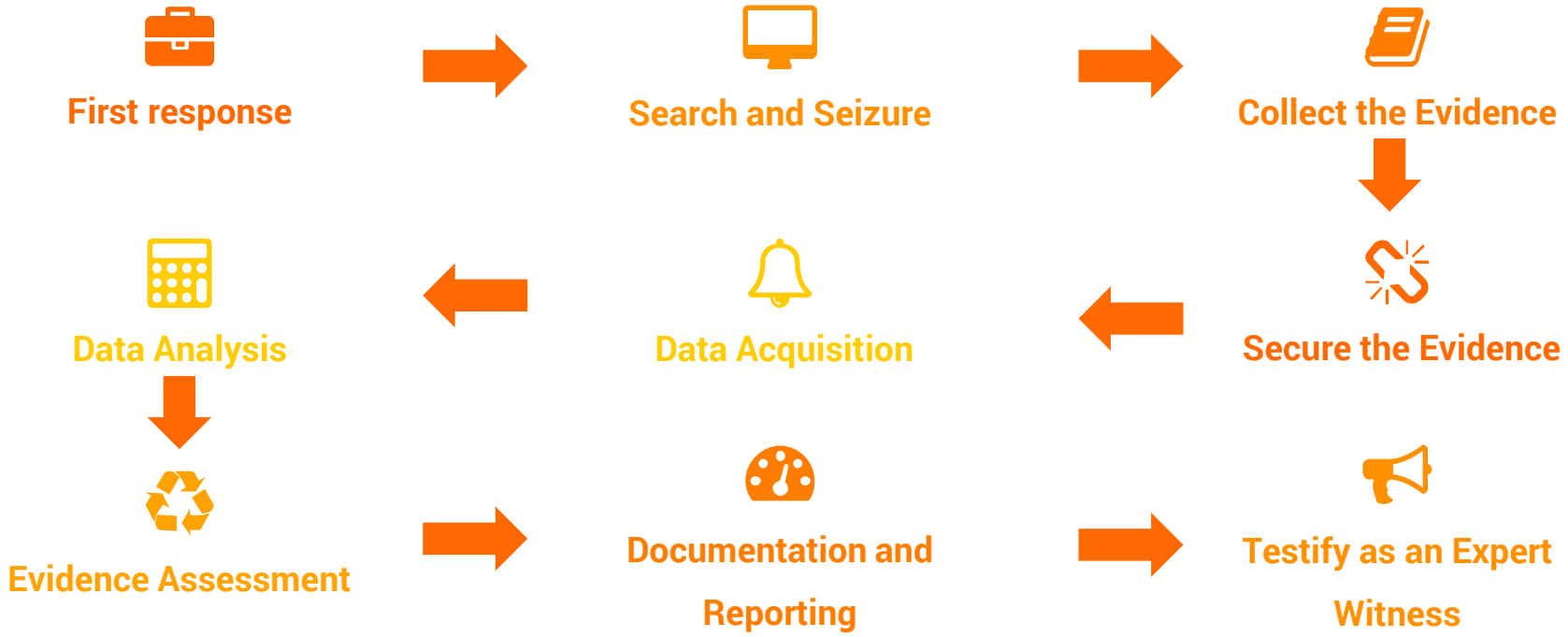
Checklist to Prepare for a Computer Forensics Investigation

1. Do not turn the computer off or on, run any programs, or attempt to access data on the computer. An expert should have the **appropriate tools** and experience to **prevent data overwriting**, damage from static electricity, or other concerns
2. **Secure** any relevant media including hard drives, cell phones, DVDs, USB drives, etc.
3. **Suspend** automated document destruction and recycling policies that may pertain to any relevant media or users at the time of the issue
4. Perform a **preliminary assessment** of the crime scene and identify the type of data you are seeking, the information you are looking for, and the urgency level of the examination
5. Once the machine is secured, **obtain information** about the machine, the peripherals, and the network to which it is connected
6. If possible, **obtain passwords** to access encrypted or password-protected
7. Compile a **list** of names, e-mail addresses, and other identifying information of those with whom the subject might have communicated
8. If the computer is **accessed** before the forensic expert is able to secure a mirror image, note the user(s) who accessed it, what files they accessed, and when the access occurred. If possible, find out why.
9. Maintain a **chain of custody** for each piece of original media, indicating where the media has been, whose possession it has been in, and the reason for that possession.
10. Create a list of **key words** or phrases to use when searching for relevant data

Chain of Custody - Sample

The item(s) described below were obtained as evidence by the undersigned during an official investigation of the : (name of school, district, or entity)		
Description of Item:		
Obtained from: (title, name, location, phone number)		
Printed name of investigator:	**Signature of Investigator:**	**Date Obtained:**
Case Number:		
Temporary disposition of item (s): (where stored)		
Released by: (printed name and signature)	Released to: (printed name and signature)	Date:
Temporary disposition of item (s): (where stored)		
Released by: (printed name and signature)	Released to: (printed name and signature)	Date:
Temporary disposition of item (s): (where stored)		
Released by:(printed name and signature)	Released to: (printed name and signature)	Date:
Temporary disposition of item (s): (where stored)		

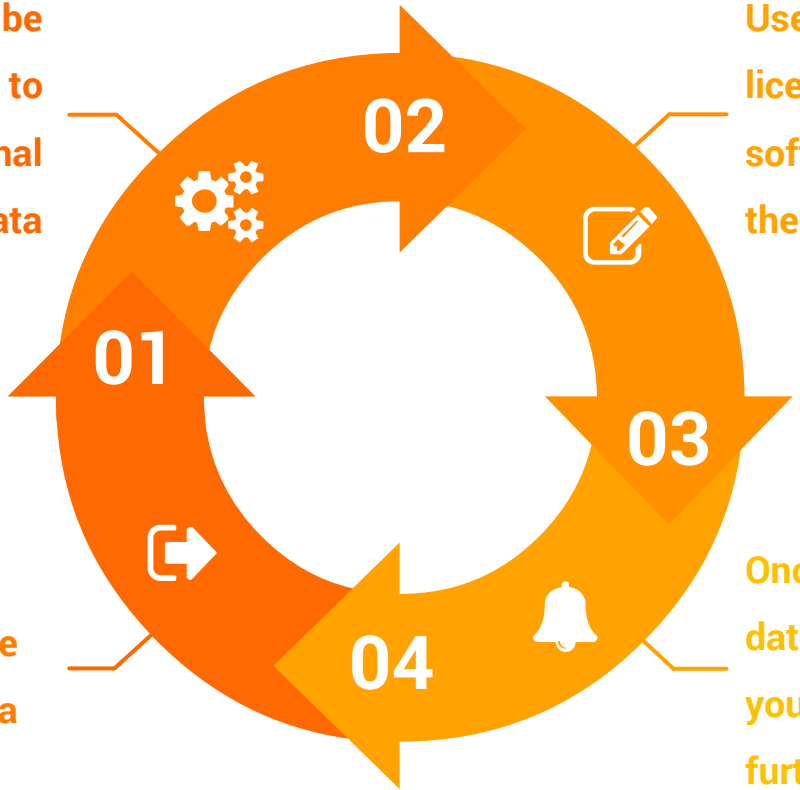
Digital Forensics - Methodology



Data Acquisition - Imaging

The data should be duplicated bit by bit to represent the same original data

Use industry standard or licensed hardware or software tools to duplicate the data



Make a duplicate of the collected data

Once a copy of the original data is made and verified, you can use the copy for further processing

Data Acquisition - Hashing

Verify Image Integrity

- Hash Function (File) results in unique string of Hexadecimal values
- H(F1) = A & H(F2) = B; then it can be derived that F1 <> F2
- H(F1) = C & H(F2) = C; then it can be derived that F1 == F2
- MD5, SHA-1, SHA-2, SHA-3 (**S**ecure **H**ash **A**lgorithm) are common algorithms.
  - Sample MD5: 8650f1d0ea13e99079e504369d0d6c5a (32 chars)
  - Sample SHA1: 961a77da52e0a1ba194dd06a49afb1b21a5cc502 (40 chars)
- **Collision** occurs when two inputs hash to a same value, so to avoid it we need to use a bigger hash value size such as SHA512 which has 64 bytes (128 chars) length.

Data Acquisition - Write blockers

Preserving the data integrity

- Preserving the data integrity is of utmost importance
- Don’t damage the evidence – Evidence Drive
- **Risk** – OS writing to the evidence drive
- **Countermeasure** – Write Blocker
- Two types –
  - Hardware (sits between evidence drive & forensic workstation)
  - Software (built into a computer forensic suite or OS configured)

Data Acquisition - Hardware Write blockers

Preserving the data integrity

- Purpose
  - To connect an evidence to a forensic workstation
  - To rely on in-built software for write blocking

1: SATA Connector
2: 3.5/5.25" IDE Connector
3: 2.5" IDE Connector
4: USB Connector

Data Analysis

- Thoroughly analyze the acquired data to draw conclusions related to the case.
- Data analysis techniques depend on the scope of the case or client's requirements, and the type of evidence.
- This phase includes:
  - Analyzing the file content for data usage
  - Analyzing the date and time of file creation and modification
  - Users associated with file creation, access, and file modification
  - Physical storage location of the file
  - Timeline generation
- Identify and categorize data in order of relevance to the case, such that the most relevant data serves as the most important evidence to the case
- Forensics tools help in sorting and analysis of a large volume of data to draw meaningful conclusions.
- Examples of data analysis tools:
  - AccessData's Forensic Toolkit (FTK)
  - Guidance Software's EnCase Forensic
  - The Sleuth Kit (TSK)

Writing the Investigation Report (1/2)

- **Purpose of Report:** Explain the objective of the report, the target audience, and the reason for preparing the report clearly. Mention how the evidence supports or denies the claims and provide sufficient backup to the statements.
- **Author of Report:** Include a list of all the authors and co-authors of the report, including their positions, responsibilities during the investigation, and their contact details.
- **Incident Summary:** Introduce the incident and explain its impact; the summary should explain clearly what the incident was and how it occurred.
- **Evidence:** Provide descriptions of the evidence acquired during the investigation, location, status during extraction, extraction procedure, analysis process, tools used, etc. Mention each detail clearly and in such a way that the process is explicable to the people with less or no technical knowledge.

Writing the Investigation Report (2/2)

- **Details**
  - Provide a detailed description of what evidence was analyzed and the analysis methods that were used and also explain the findings of the analysis.
  - List the procedures that were followed during the investigation and any analysis techniques that were used.
  - Include proof of your findings, such as utility reports and log entries.
- **Conclusion**
  - Summarize the outcome of the investigation.
  - Cite specific evidence to prove the conclusion.
  - The conclusion should be clear and unambiguous.
- **Supporting Documents**
  - Include any background information referred to throughout the report, such as network diagrams, documents that describe the computer investigation procedures used, and overviews of technologies that are involved in the investigation.
  - It is important that supporting documents provide enough information for the reader to understand the incident as completely as possible.

Cloud Forensics

Up & above

Cloud - deployment models

1. **private cloud** - the services and infrastructure are provided for a single organization on a private network,
2. **community cloud** - the services and infrastructure are provided between several organizations from a specific community with common concerns,
3. **public cloud** - the services and infrastructure are provided off-site over a network that is open for public use, and
4. **hybrid cloud** - cloud includes a variety of two or more clouds from different service providers

Cloud - services models (1/2)

Cloud services are of three types based on the services provided

- Infrastructure-as-a-Service (IaaS)

Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API

E.g. Amazon EC2, Azure, Oracle Cloud

- Platform-as-a-Service (PaaS)

Offers development tools, configuration, management, and deployment platforms on-demand that can be used by subscribers to develop custom applications

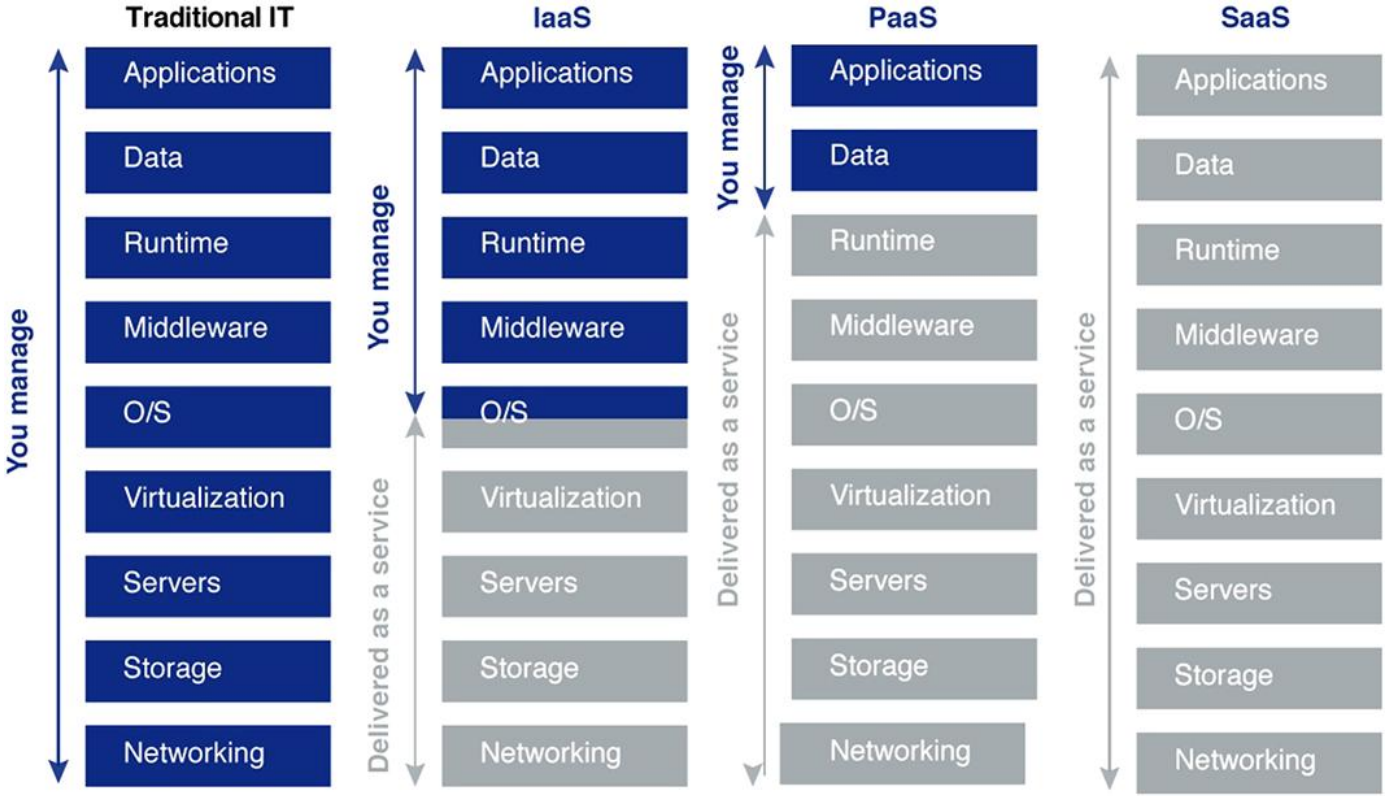
E.g. Intel MashMaker, Google Cloud, Microsoft Azure, etc.

- Software-as-a-Service (SaaS)

Offers software to subscribers on-demand over the Internet
E.g. web-based office applications like Google Docs or Mail, Salesforce CRM, etc

Cloud - services models (2/2)

Comparison between traditional IT and cloud computing



Source: Microsoft

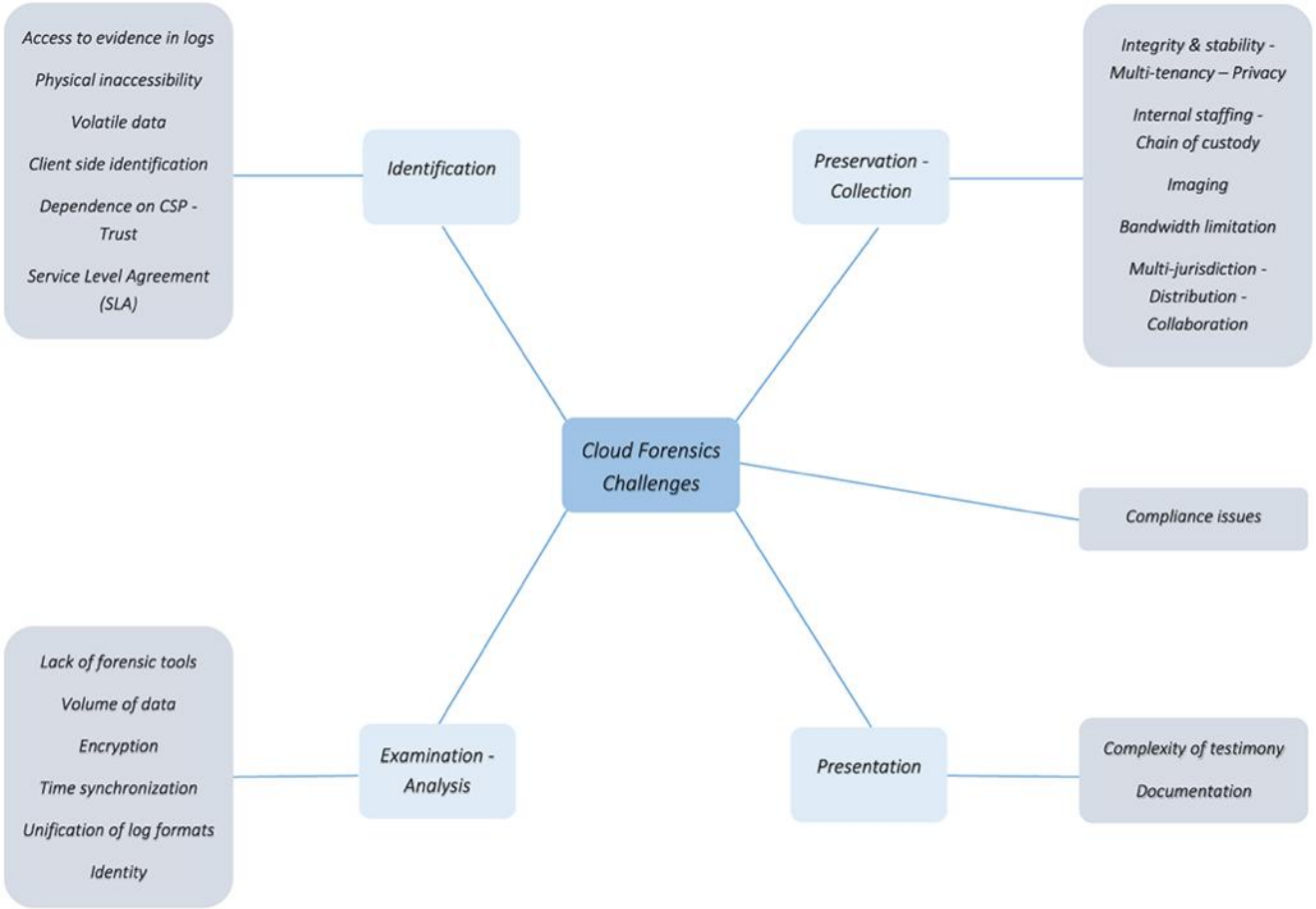
Cloud Forensics Challenges: Architecture and Identification

Challenge	Description
Deletion in the cloud	• The total volume of data and users operating regularly in a cloud ecosystem confines the amount of backups the CSP will retain • CSPs may not implement necessary methods to retrieve information on deleted data in an IaaS or PaaS delivery model
Recovering overwritten data	• It is very difficult to recover data marked as deleted, as it may get overwritten by another user sharing the same cloud • Also, a snapshot might not be taken in time (ex: backup) that contains data duplicate before it was overwritten
Interoperability issues among CSP	• Collection and preservation of forensic evidence is challenging as there is lack of interoperability among CSPs and lack of control from the consumer's end into the proprietary architecture and/or the technology used
Single points of failure	• Cloud ecosystem has single points of failure, which may have adverse impact on the evidence acquisition process
No single point of failure for criminals	• Collection and analysis of evidentiary data from distributed and disparate sources is highly difficult as criminals may choose one CSP to store their data, second CSP to obtain computing services, and third CSP to route all their communications

Cloud Forensics Challenges: Architecture and Identification

Challenge	Description
Detection of the malicious ac	• It is tough for an investigator to detect a malicious act by identifying a series of small changes made across many systems and applications as a result of attacks launched by perpetrator to penetrate a cloud
Criminals access to low cost computing power	• Cloud computing provides computing power that would otherwise be not available to criminals at a low budget, thus letting unpredictable attacks that would be unfeasible outside a cloud environment
Real-time investigation intelligence processes not possible	• Investigating real-time incidents in the cloud is very difficult as it requires intelligence process, which is often not possible while working along with the CSPs or other actors and a special legal means is to be applied in many cases to collect data
Malicious code may circumvent VM isolation methods	• Vulnerabilities in server virtualization allow malicious code to evade VM isolation methods and interfere with either other guest VMs or the hypervisor itself
Multiple venues and geo-locations	• Managing the scope of data collection is challenging as distributed data collection and chain of custody from multiple venues or geo-location unknowns can cause various jurisdictional issues

Cloud forensics - Challenges



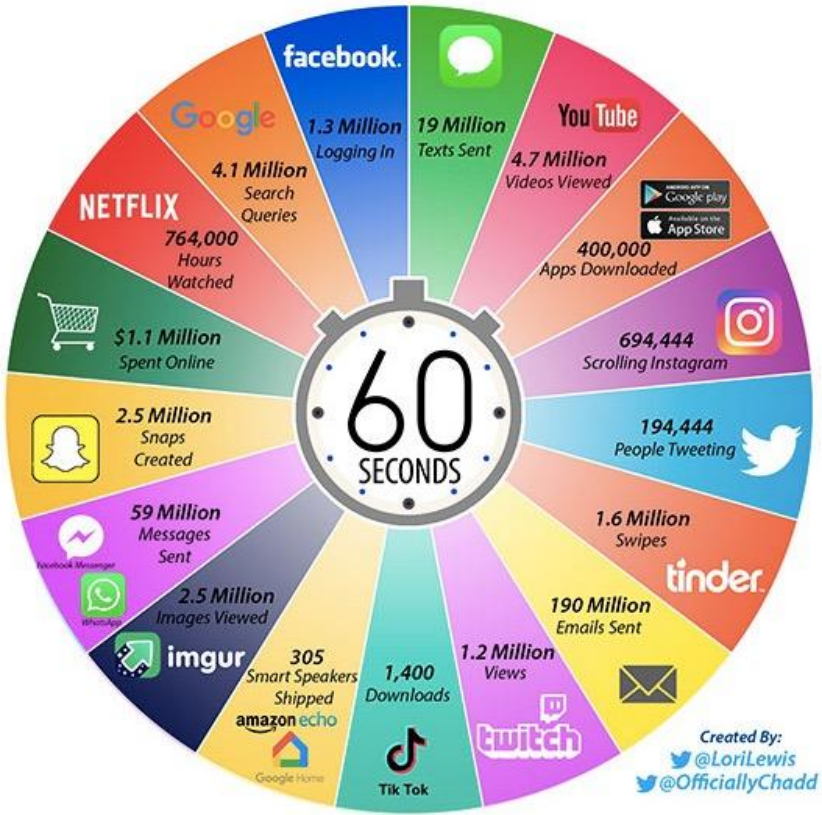
Cloud forensics - Options

- In service models like PaaS and SaaS, for example, consumers do not have the control of the hardware, and they depend on the CSP for the logs,
- whereas in IaaS consumers have the ability to make an image of the instance and acquire the logs.
- As for the deployment models, in public, cloud consumers do not have the physical access and the privacy compared with the ones in private cloud.
- Private cloud model is closer to traditional local access networks used in the past with the added advantage of virtualization.
- When the private cloud is hosted on premises (internally), forensic investigation is almost identical with the traditional forensic investigation.
- On the other hand, if the private cloud is hosted off premises (externally), forensic investigation depends on the CSPs and the signed contracts.

Ethical Hacking

Wearing the right hat

What Happens Online in 60 Seconds in 2020



7 Main phases of a cyber attack

Ethical Hacking - Principles

Reasons behind Un-ethical Hacking

Ethical Hacking - Opportunities

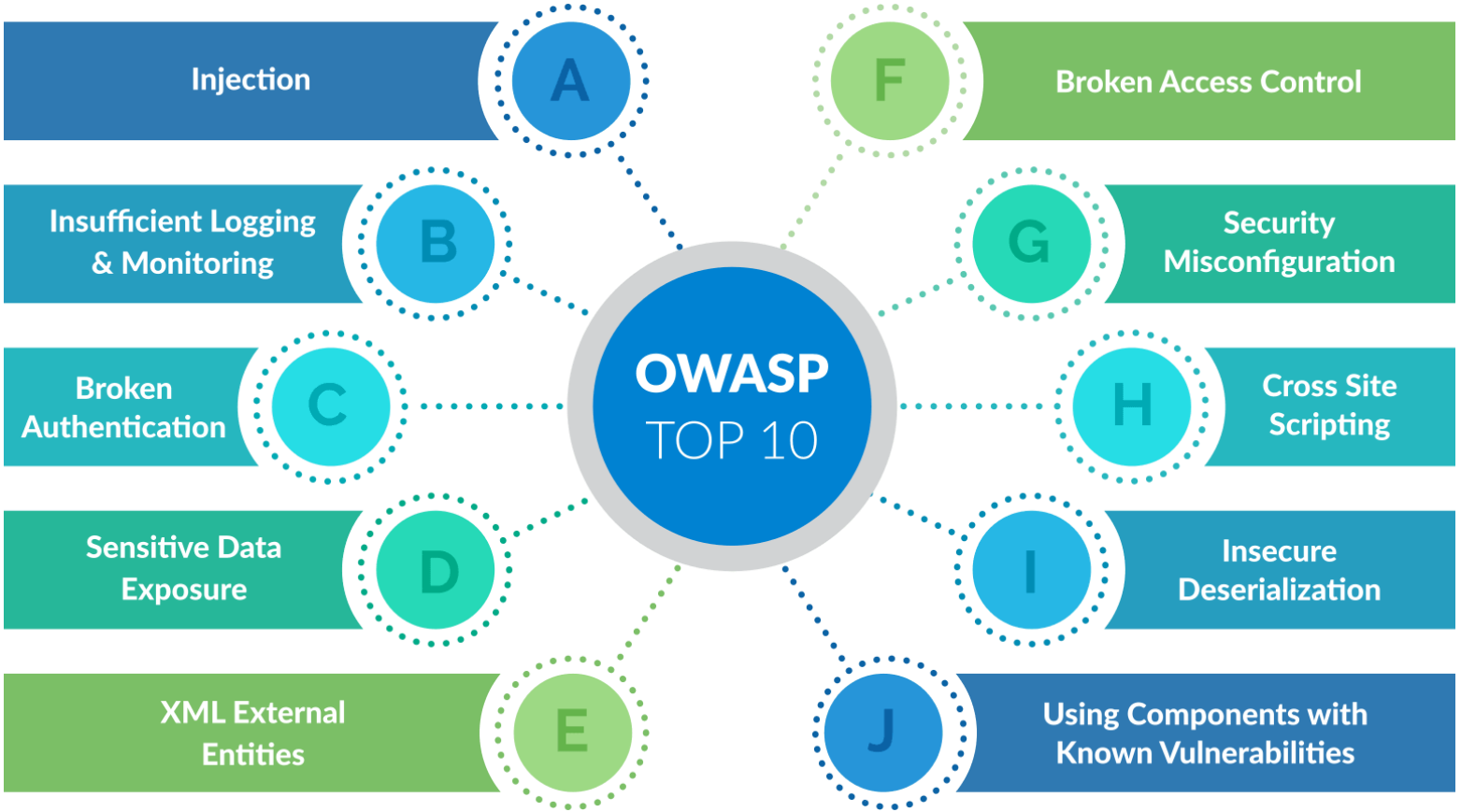
Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to organization’s information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard customer’s data available in business transactions
- To enhance security awareness at all levels in a business

SQL Injection

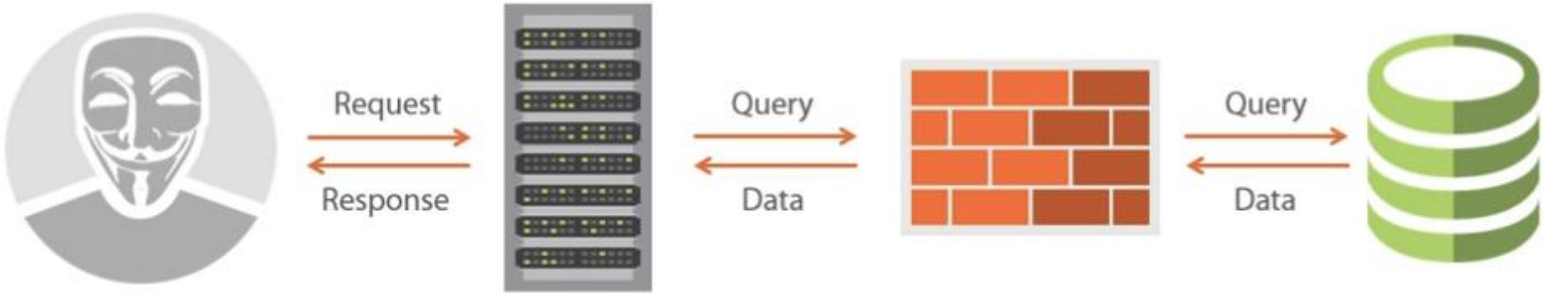
The #1 Attack Vector

Top 10 Most Critical Web Application Security Risks



SQL Injection – How it works

- SQL injection is a technique used to take advantage of un-sanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database
- SQL injection is a basic attack used to either gain unauthorized access to a database or retrieve information directly from the database
- It is a flaw in web applications and not a database or web server issue



Caller ID Spoofing

Faking the caller

Caller ID Spoofing

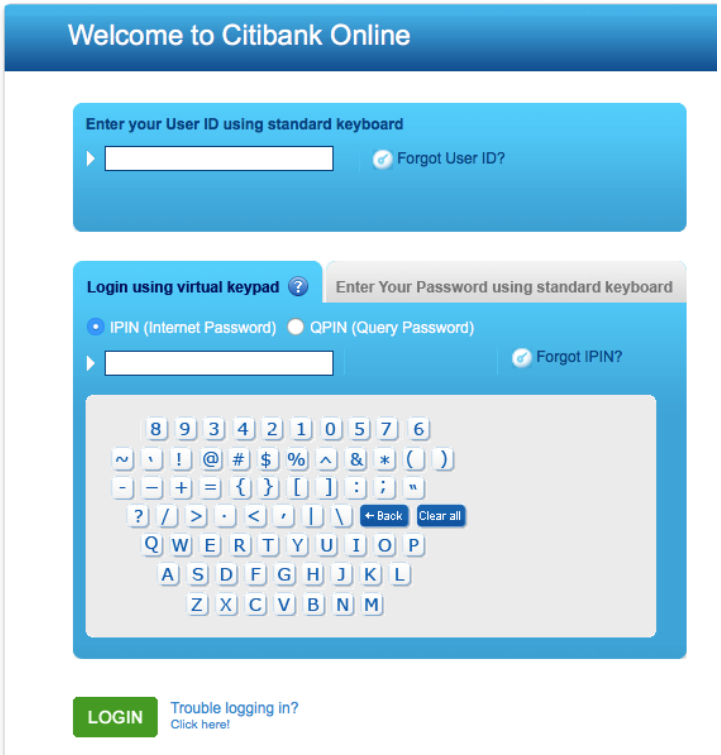
- Caller ID spoofing is the process of changing the caller ID to any number other than the calling number.
- The call-back method - If the number is busy or you reached the company they said they are calling from then they are potentially telling the truth.
- Phone with the company in question - you could ask whether or not the person is calling on behalf of the company.
- Enter the number in question in a search engine

KeyLogger

Finding the Keystrokes

KeyLogger

- Keyloggers are applications that monitor a user's keystrokes and then send this information back to the malicious user.
- Keyloggers can be one of three types:
  - **Hardware Keyloggers.**
  - **Software using a hooking mechanism**
  - **Kernel/driver keyloggers**
- Signature based anti-keylogger
- Hook based anti-keyloggers

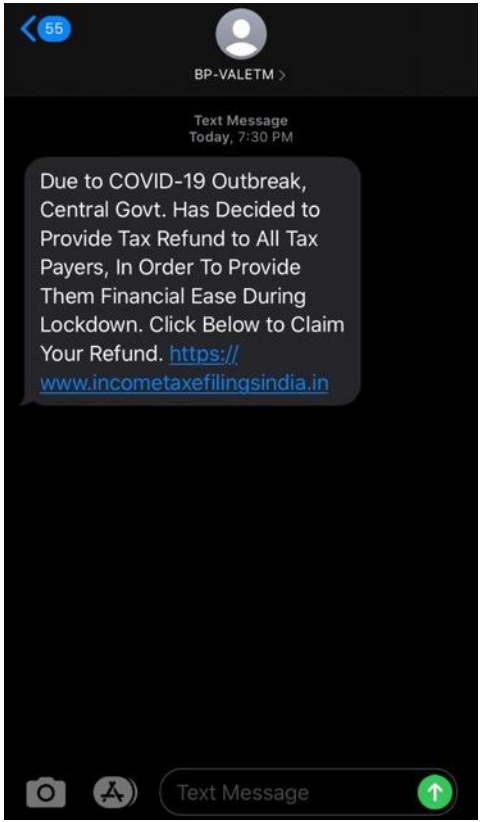


Social Engineering

Manipulating the Human

Social Engineering - Phishing

- A malicious entity contacts you, masquerading as a legitimate business and asks for information, directs you to a false website that tries to obtain your information, or otherwise tries to exploit you.
- Check the URL! URLs are unique, so no two websites can have the same URL.
- www.google.com and www.goog1e.com can look a lot alike, especially at a glance.
- If the URL is shortened, check the original URL
- Check whether the website is using HTTPS or HTTP. Most websites that involve secure transactions or your personal information will use HTTPS.



01

Phishing scams: Imposters claiming to be members of reputed domestic and international health authorities, such as the US Centre for Disease Control and Prevention (CDC) or the World Health Organisation (WHO), target victims with emails including malicious attachments, links, or redirects to 'updates' regarding the spread of COVID-19, new containment measures, maps of the outbreak or ways to protect their victims from exposure. Once opened, such attachments or links infect the computer/phone device with malware or expose sensitive personal data, credit card, etc., and this can transmit the data to the hacker

02

COVID-19 fraudulent websites: There has already been a significant rise in new fraud risk typologies, particularly relating to the registration of large numbers of "COVID" internet domains. These fake websites look like genuine websites of the organisation but carry the malware to infect the computers/phone devices

03

Business email compromise: The increase in remote working, accompanied with organisation-wide updates regarding COVID-19, has opened the avenue for fraudsters to target businesses and their employees. Using emails disguised as COVID-19 updates, fraudsters attempt to trick employees to hand over their credentials by requesting they login to a fake company's "COVID-19" portal. Once an employee has entered their credentials, the fraudster can have unfettered access to the employee's organisation's business accounts and network

04

Ransomware attacks: Government institutions and commercial organisations are seeing a new spike in ransomware attacks. In this type of attack, the critical servers and end points are first compromised and then encrypted. Ransomware attack locks the operating system and end-user files rendering them un-accessible until some ransom is paid (usually through bitcoins) to the attacker. As remote access to computers is becoming a norm for "work from home" due to the government-imposed curfews/self-imposed lockdowns, we expect a spike in ransomware attacks to cripple the organisations' IT infrastructure to collect the ransom

05

Other mobile app scams: Fraudsters are developing or manipulating mobile phone applications which outwardly look as if they track the spread of COVID-19. However, once installed the application infects the user's device with malware which can be used to obtain personal information, sensitive data, or bank account/card details.

Social Engineering – Spear Phishing (1/4)

From: **Amit More** <privmd@india.com>
Date: Tue, Jan 22, 2019 at 11:00 AM
Subject: RTGS transfer
To: <apoorv@finzy.com>

Apoorv,

Are you available? I am tied up in a meeting and I will need you to help me process RTGS of RS 4,80,100? into the beneficiary's account details that I will send you shortly. I was supposed to make the payment this morning before leaving for a meeting, but I forgot and I have just received an email reminder of the payment, I would very much appreciate if you could help.

The payment is a personal payment that should be referenced in my name and the payment will be refunded as soon as I finish with meetings. My meeting has just started and I can't take a phone call but I will call you after finishing, Please kindly email me back and let me know the details needed to process the RTGS?

Regards,

Amit More

Sent from my iPhone

Social Engineering – Spear Phishing (2/4)

Important - Don't get locked out of your Finzy Gmail account. Act Now Spam ×

admin@finzv.com
to me

9:30 PM (0 minutes ago)

This message seems dangerous

Many people marked similar messages as phishing scams, so this might contain unsafe content. Avoid clicking links, downloading attachments, or replying with personal information.

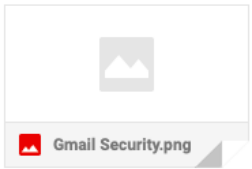
Hello,

We detected an unauthorised sign-in to your account. Please secure your account by clicking resetting your password of your Google account. **Link expires in 24 hours!** Here is the link >> http://192.168.0

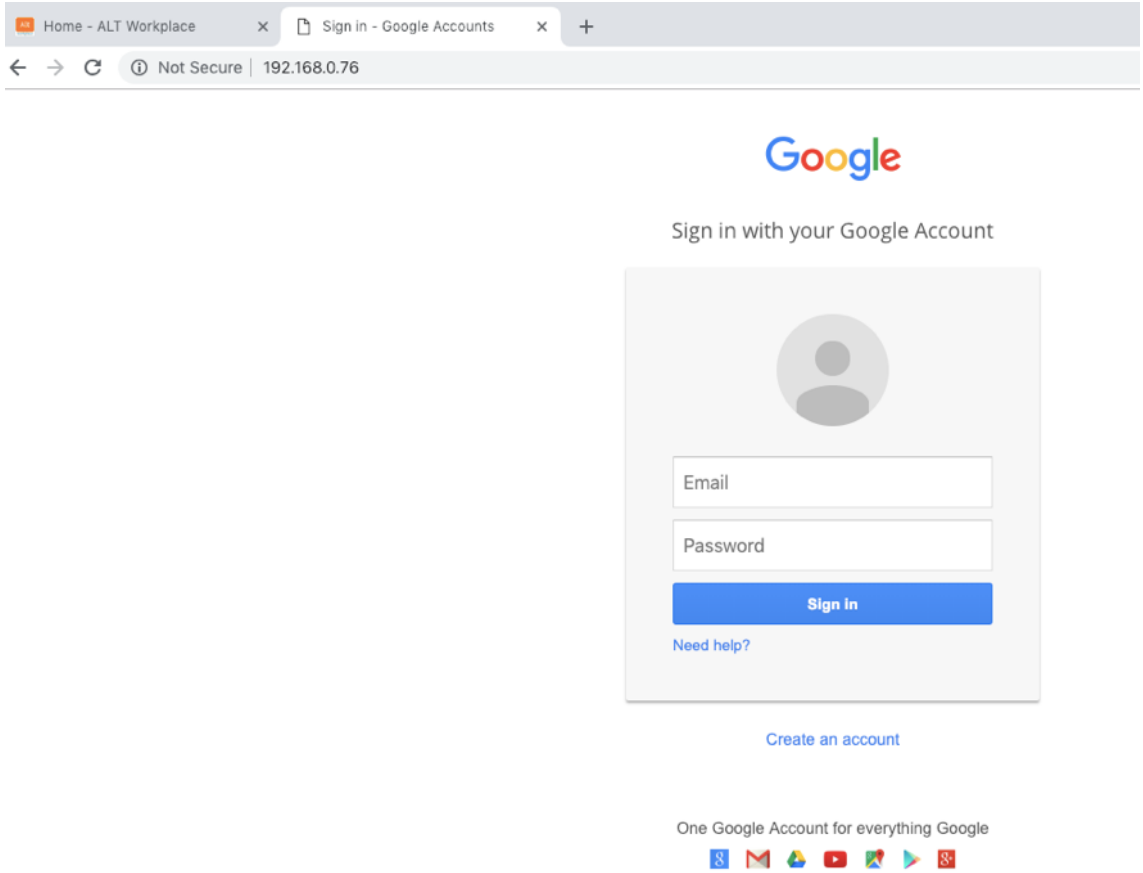
Thank you for verifying your Google account. Never share your password with anyone. For any queries, contact the IT team.

Thanks & Regards,
Finzy IT Admin Team

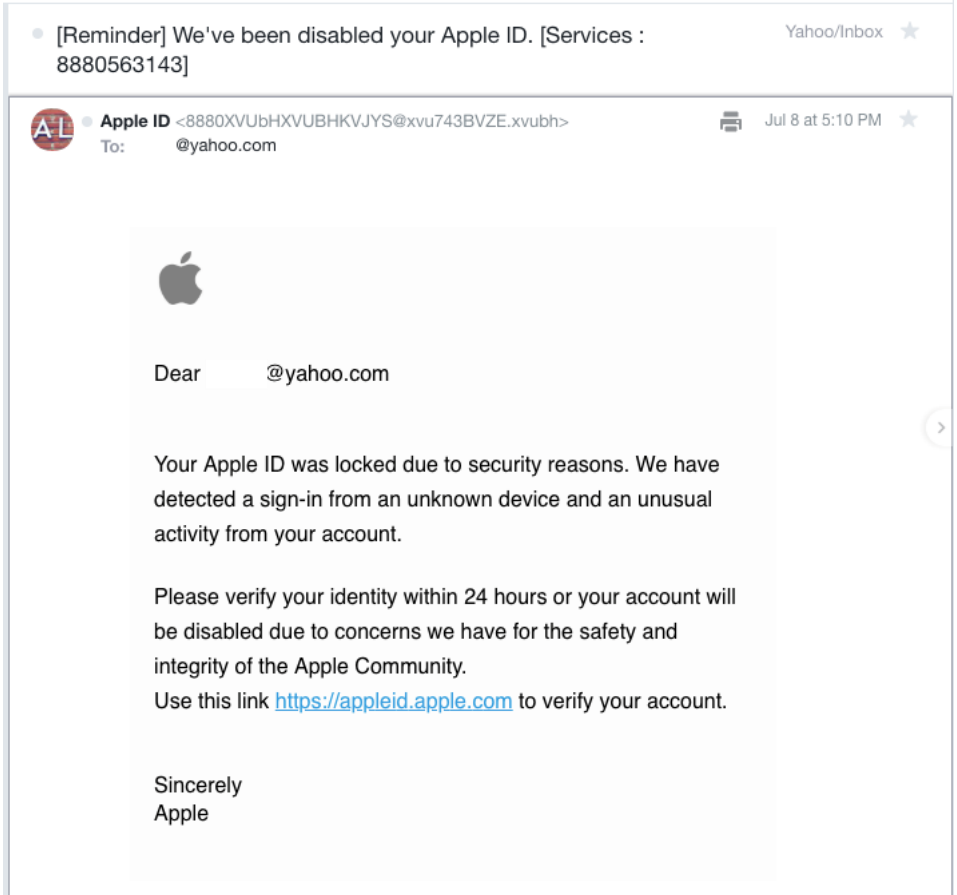
Downloading this attachment is disabled. This email has been identified as phishing. If you want to download it and you trust this message, click "Not spam" in the banner above.



Social Engineering – Spear Phishing (3/4)



Social Engineering – Spear Phishing (4/4)



[Reminder] We've been disabled your Apple ID. [Services : 8880563143]

Yahoo/Inbox

Apple ID <8880XVUbHXVUBHKVJYS@xvu743BVZE.xvubh>
To: @yahoo.com

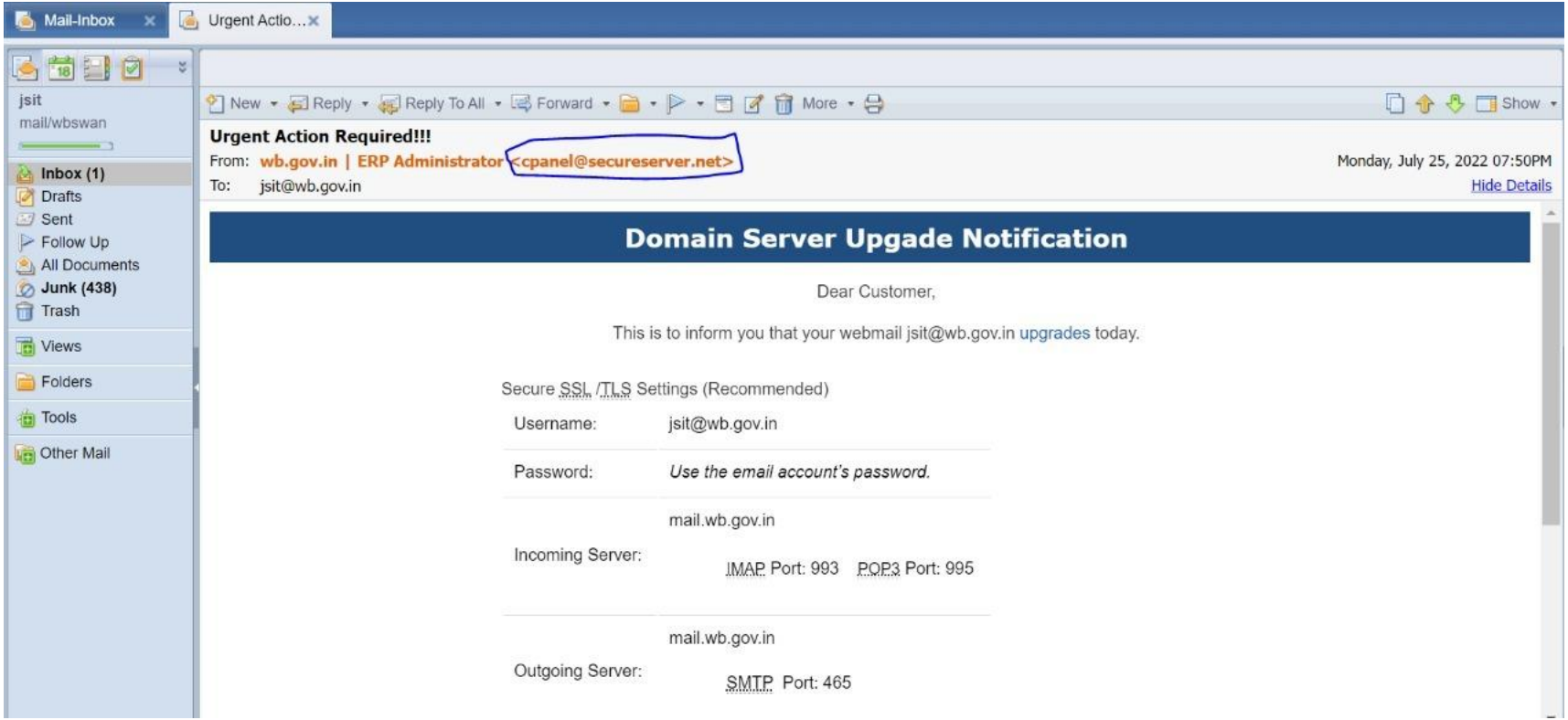
Jul 8 at 5:10 PM

Dear @yahoo.com

Your Apple ID was locked due to security reasons. We have detected a sign-in from an unknown device and an unusual activity from your account.

Please verify your identity within 24 hours or your account will be disabled due to concerns we have for the safety and integrity of the Apple Community.
Use this link https://appleid.apple.com to verify your account.

Sincerely
Apple


Mail-Inbox
Urgent Actio...
jsit
mail/wbswan
Inbox (1)
Drafts
Sent
Follow Up
All Documents
Junk (438)
Trash
Views
Folders
Tools
Other Mail
New
Reply
Reply To All
Forward
More
Show
Urgent Action Required!!!
From: wb.gov.in | ERP Administrator <cpanel@secureserver.net>
To: jsit@wb.gov.in
Monday, July 25, 2022 07:50PM
Hide Details
Domain Server Upgade Notification
Dear Customer,
This is to inform you that your webmail jsit@wb.gov.in upgrades today.
Secure SSL /TLS Settings (Recommended)
Username: jsit@wb.gov.in
Password: Use the email account's password.
Incoming Server: mail.wb.gov.in
IMAP Port: 993 POP3 Port: 995
Outgoing Server: mail.wb.gov.in
SMTP Port: 465

Dark Web

Know the Web

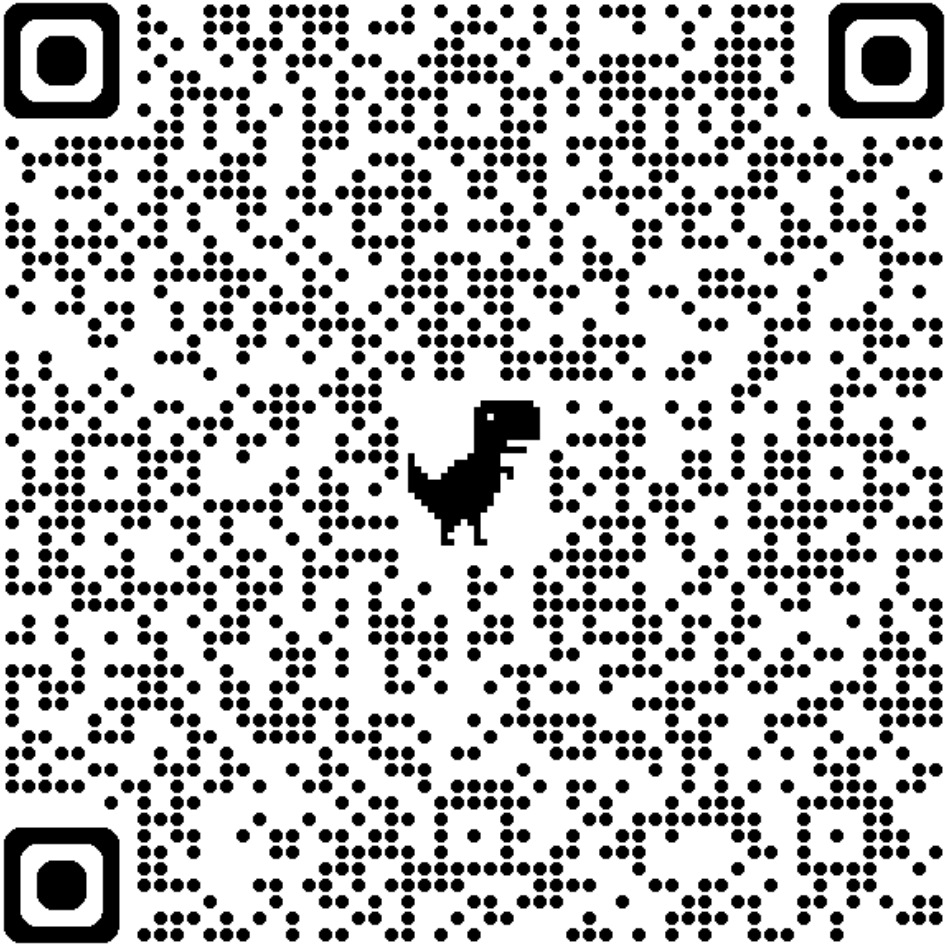
Image Credits: elixirofknowledge

Notable Cyber-Stories

Recent mentions in the news (and some more)

(1) New e-Zero FIR: Govt launches pilot project for swift action against cybercrimes

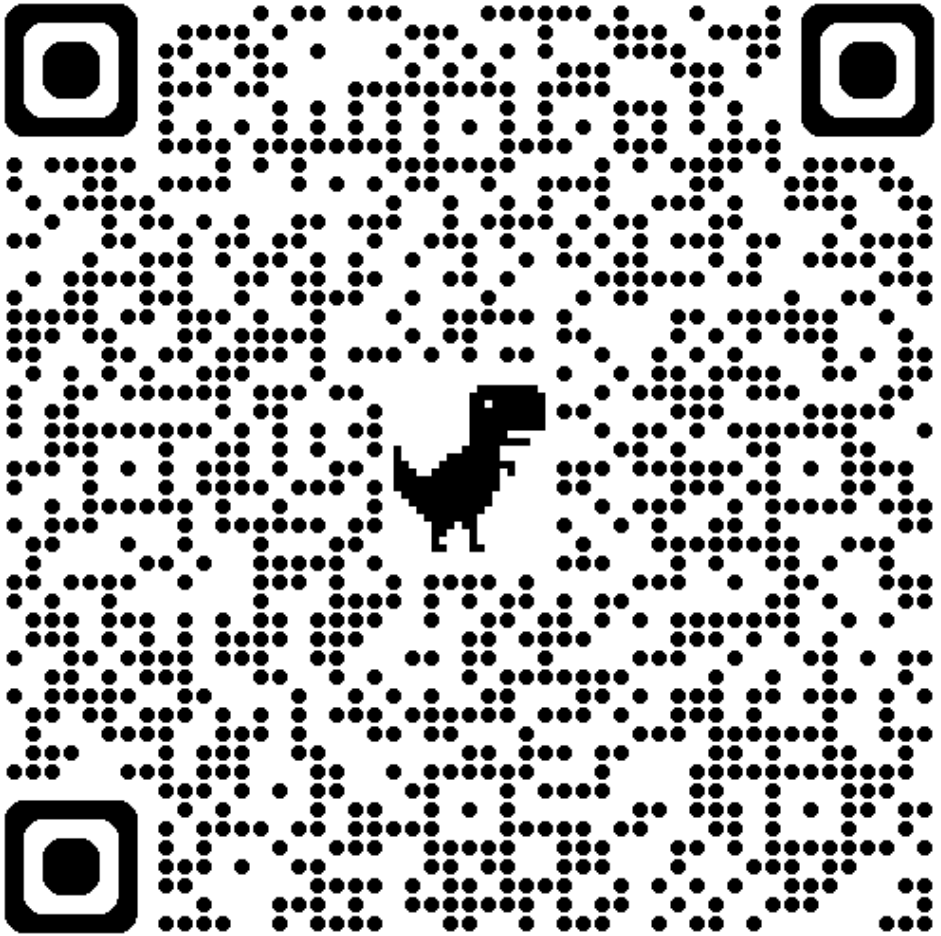
https://economictimes.indiatimes.com/wealth/save/new-e-zero-fir-govt-launches-pilot-for-swift-action-against-cybercrimes-how-it-can-help-you/articleshow/121314437.cms



May 22, 2025

(2) ‘Cop’ threatening on call?

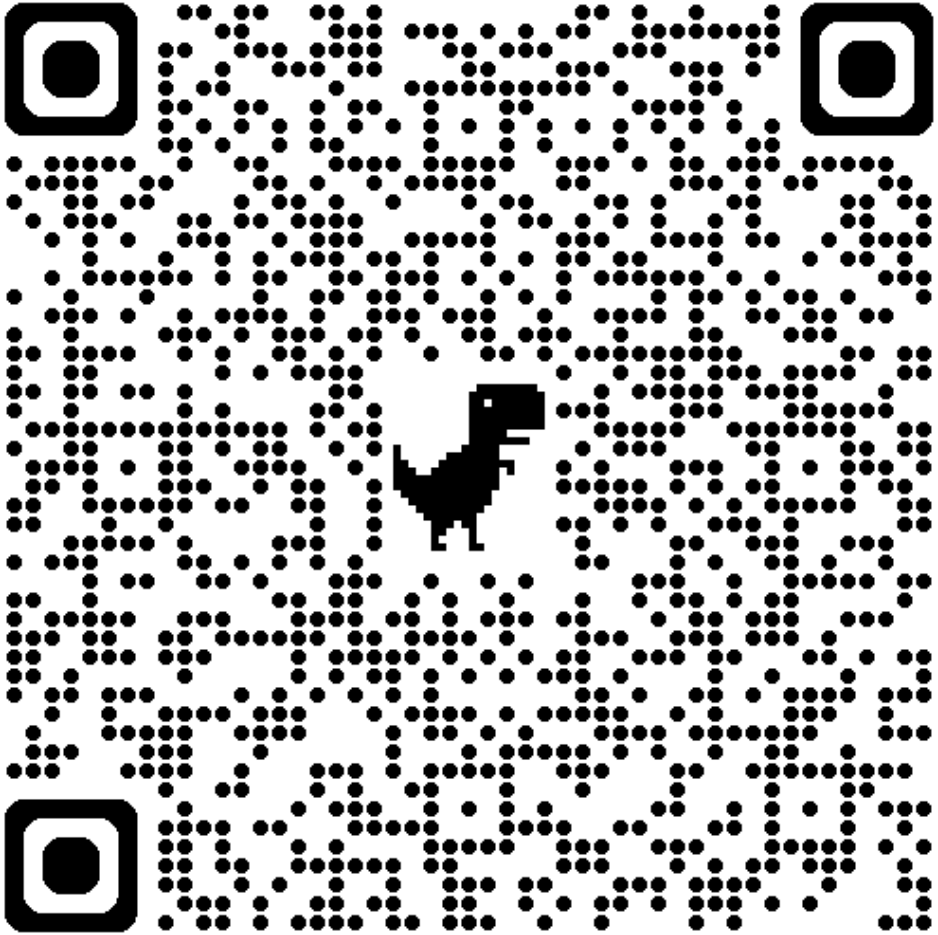
https://timesofindia.indiatimes.com/city/mumbai/cop-threatening-on-call-soon-check-id-on-app/articleshow/121503805.cms



May 30, 2025

(3) City police launches Zonal Cyber Cells to combat cybercrime

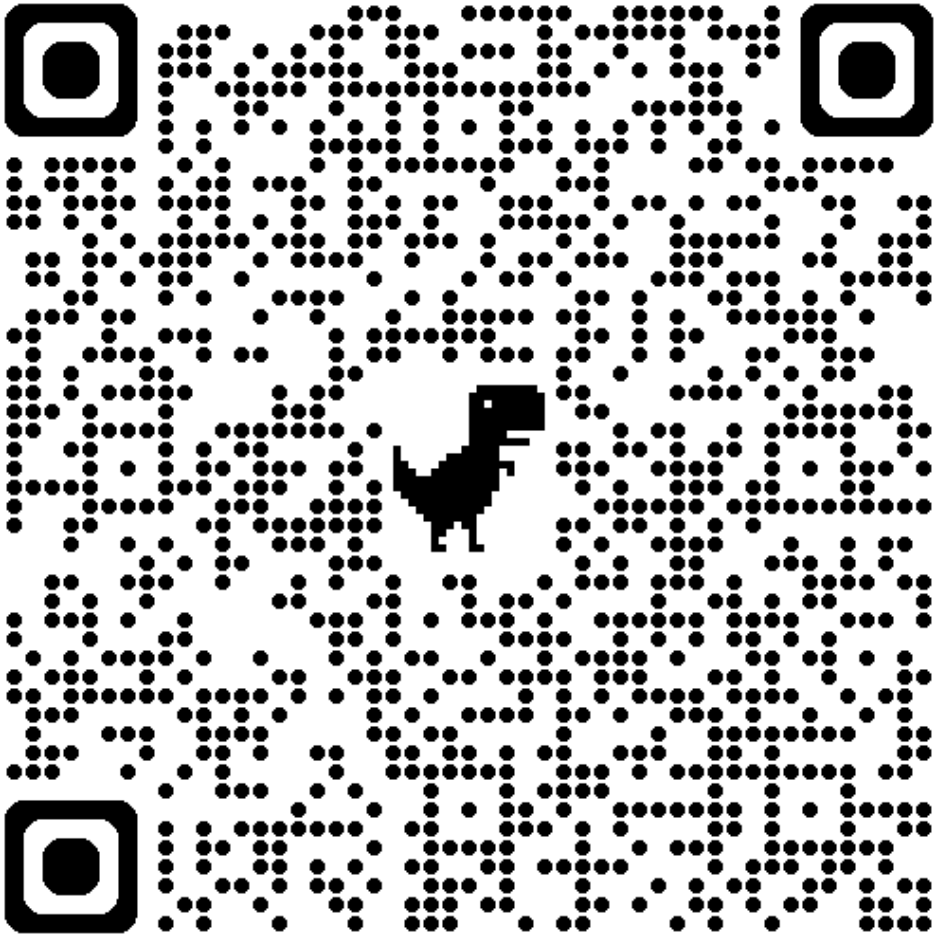
https://timesofindia.indiatimes.com/city/hyderabad/city-police-launches-zonal-cyber-cells-to-combat-cybercrime/articleshow/121504209.cms



May 30, 2025

(4) India's alarm over Chinese spying rocks the surveillance industry

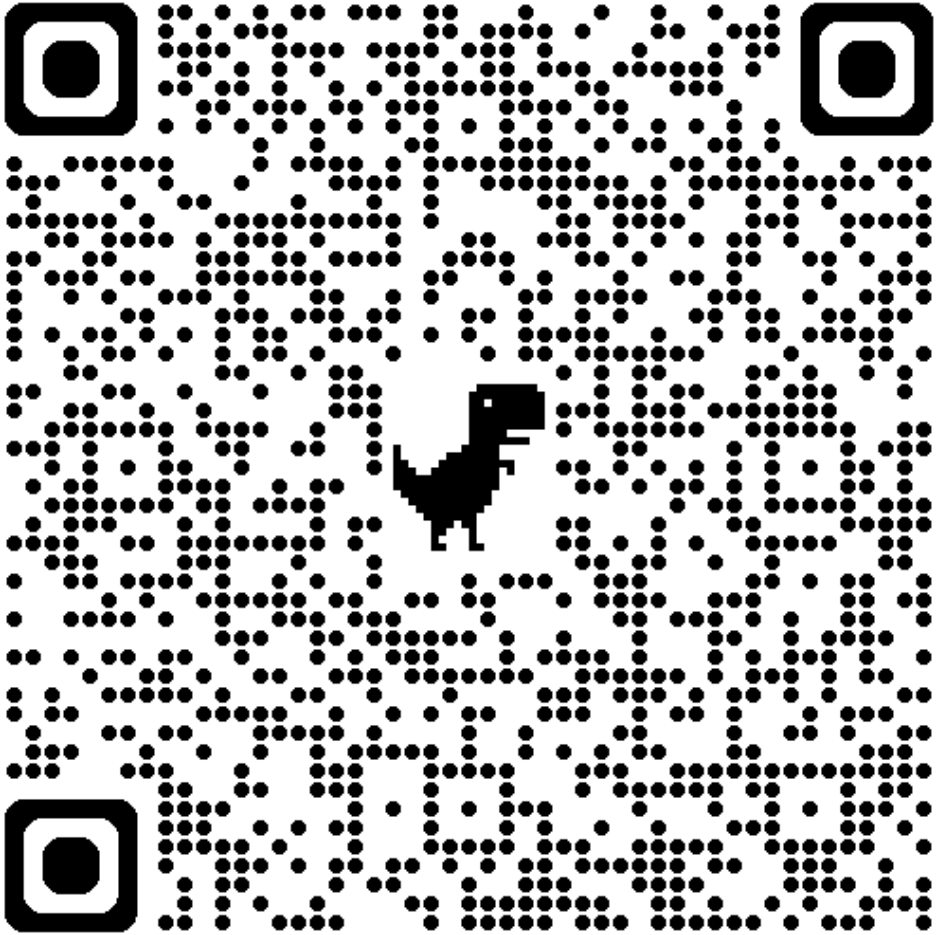
https://www.reuters.com/world/china/indias-alarm-over-chinese-spying-rocks-surveillance-industry-2025-05-28



May 29, 2025

(5) CIAL to unveil Rs 200-cr tech upgrade

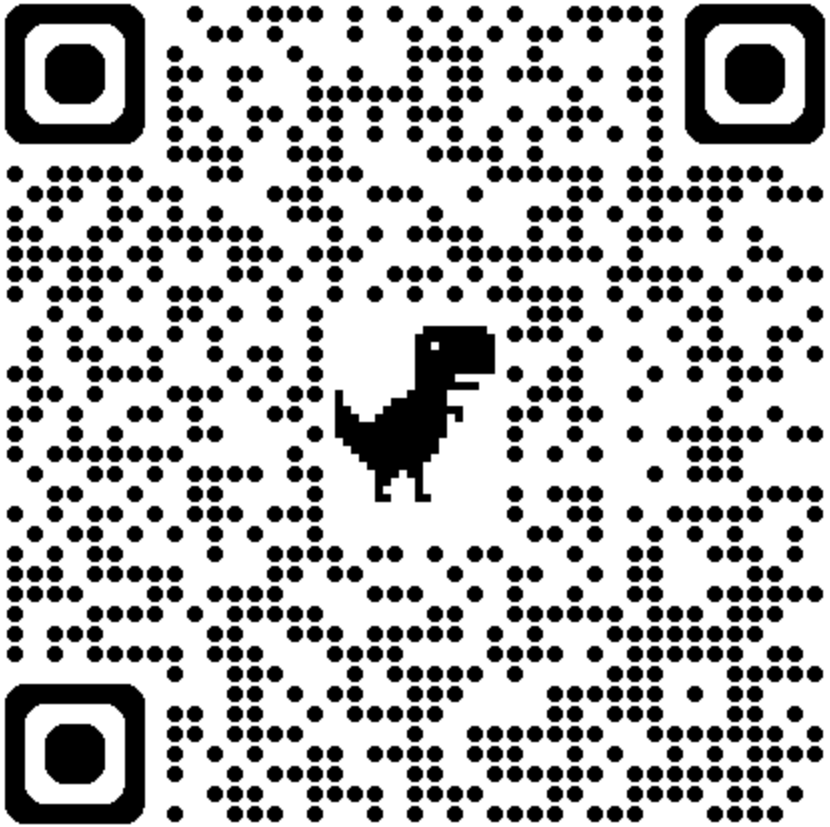
https://timesofindia.indiatimes.com/city/kochi/cial-to-unveil-rs-200-cr-tech-upgrade/articleshow/121169929.cms



May 14, 2025

(6) Do-It-Yourself Cyberattack Tools Are Booming

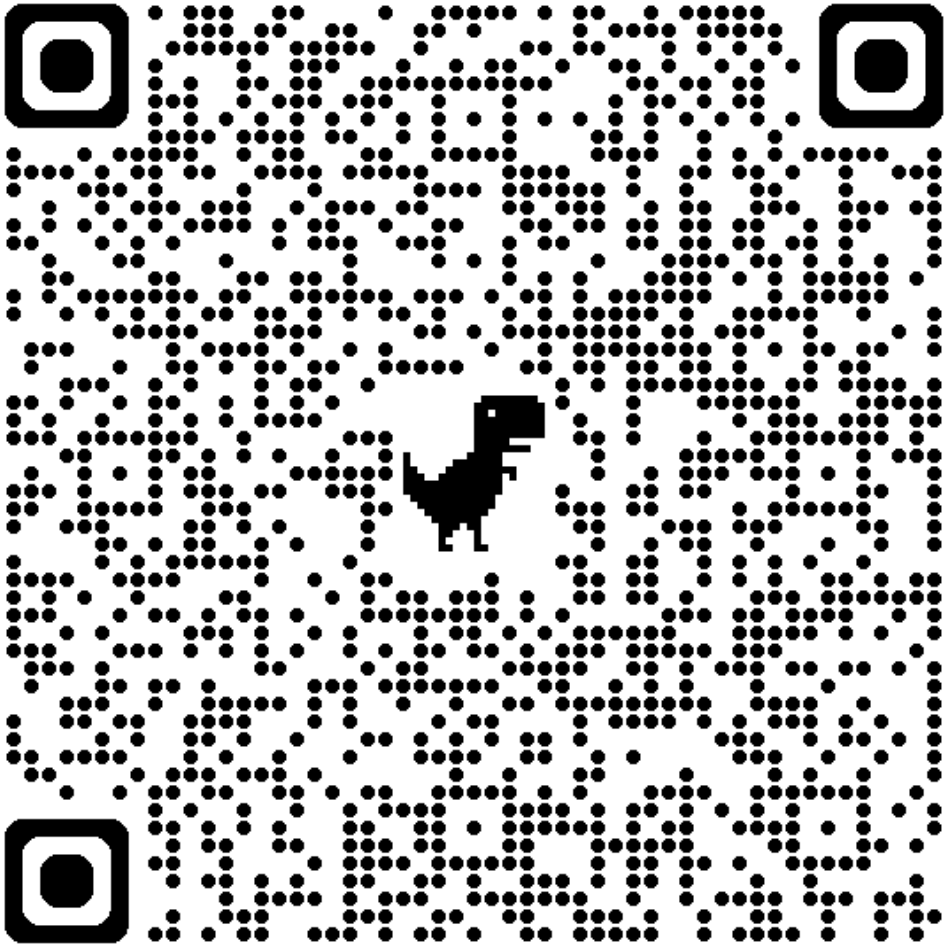
https://www.wsj.com/articles/do-it-yourself-cyberattack-tools-are-booming-7ce1445d



May 29, 2025

(7) M&S hack may have been caused by security issues at Indian IT giant Tata Consultancy Services (TCS)

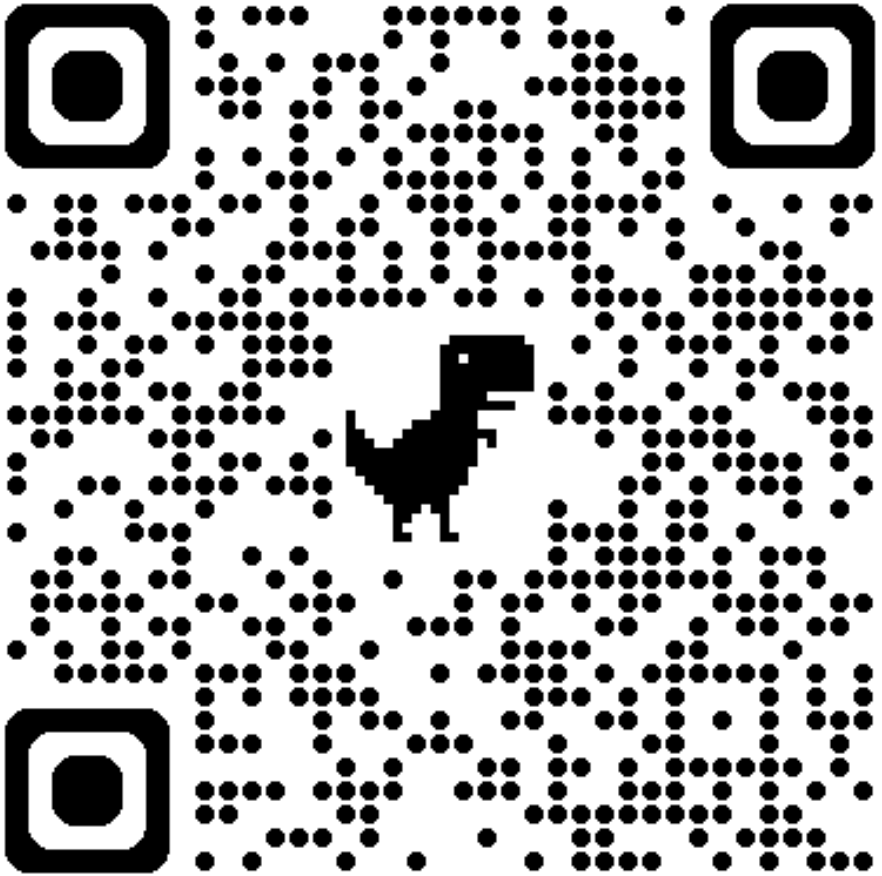
https://www.techradar.com/pro/security/m-and-s-hack-may-have-been-caused-by-security-issues-at-indian-it-giant-tata-consultancy-services



May 26, 2025

(8) CrowdStrike 2025 Global Threat Report

https://www.crowdstrike.com/en-us/global-threat-report/?utm_source=chatgpt.com

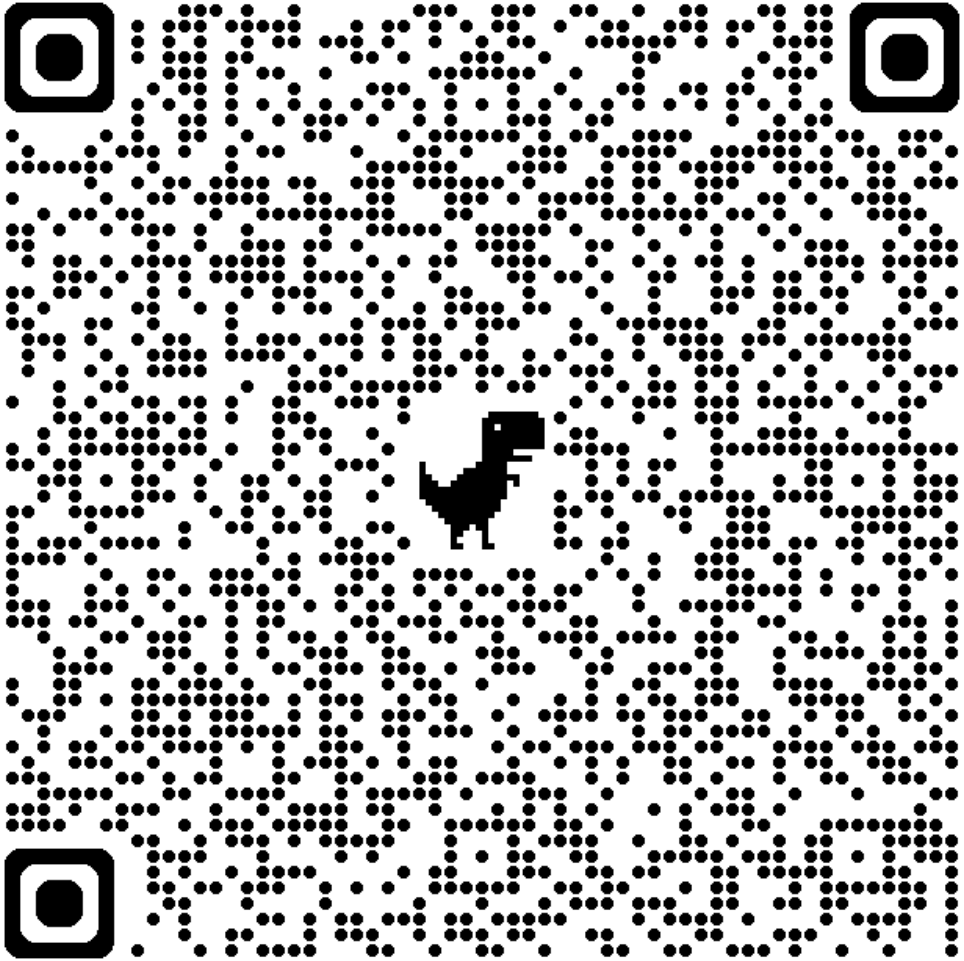


2025

(9) Rising Demand for Cyber Security Professionals, Over 3.5 Million Positions Unfilled Globally

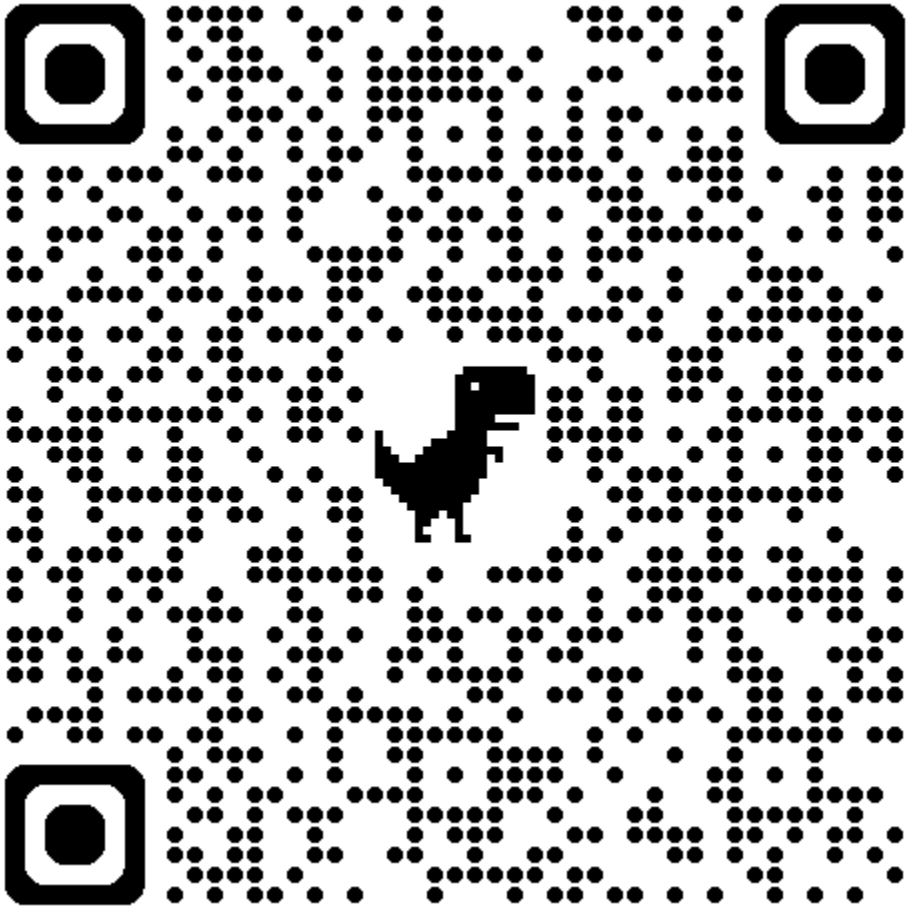
https://www.businesswire.com/news/home/20250530656246/en/Cyber-Security-Market-Industry-Report-2025-Rising-Demand-for-Cyber-Security-Professionals-Over-3.5-Million-Positions-Unfilled-Globally---ResearchAndMarkets.com

May 30, 2025



(10) Bank fraud amount jumps by three times to Rs 36,014 crore in FY25: RBI

https://indianexpress.com/article/business/bank-fraud-amount-jumps-by-three-times-to-rs-36014-crore-in-fy25-rbi-10036075/#



May 29, 2025

https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?year=2025

May 29, 2025

Table VI.2: Fraud Cases - Bank Group-wise

(Amount in ₹ crore)

Bank Group/Institution	2022-23		2023-24		2024-25	
	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved
1	2	3	4	5	6	7
Public Sector Banks	3,331	12,557	7,460	9,254	6,935	25,667
	(24.7)	(66.2)	(20.7)	(75.6)	(29.0)	(71.3)
Private Sector Banks	8,971	5,206	24,207	2,722	14,233	10,088
	(66.4)	(27.4)	(67.2)	(22.3)	(59.4)	(28.0)
Foreign Banks	804	292	2,899	154	1,448	181
	(6.0)	(1.5)	(8.0)	(1.3)	(6.0)	(0.5)
Financial Institutions	9	888	1	1	2	13
	(0.1)	(4.7)	-	-	-	-
Small Finance Banks	311	31	1,019	64	1,217	58
	(2.3)	(0.2)	(2.8)	(0.5)	(5.1)	(0.2)
Payments Banks	68	7	472	35	113	6
	(0.5)	-	(1.3)	(0.3)	(0.5)	-
Local Area Banks	0	0	2	0	5	1
	-	-	-	-	-	-
Total	**13,494**	**18,981**	**36,060**	**12,230**	**23,953**	**36,014**
	(100.0)	**(100.0)**	**(100.0)**	**(100.0)**	**(100.0)**	**(100.0)**

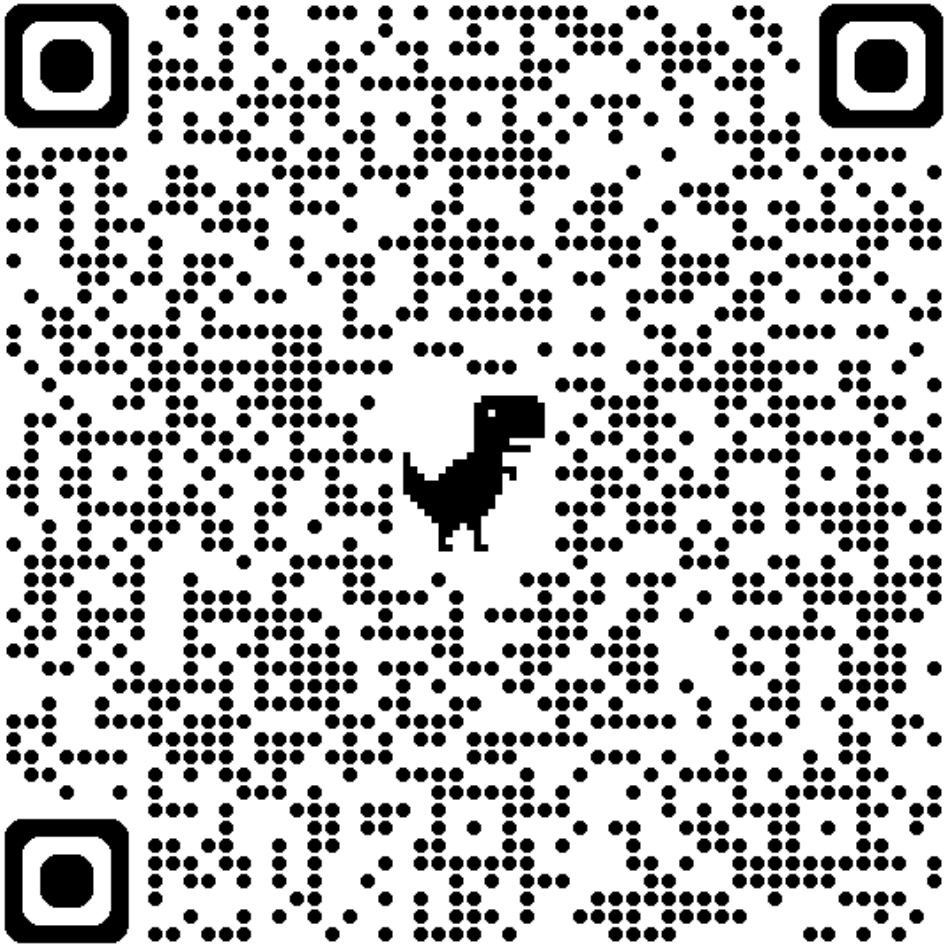
-: Nil/Negligible.

Note:
1. Figures in parentheses represent the percentage share of the total.
2. Data are in respect of frauds of ₹1 lakh and above reported during the period.
3. The figures reported by banks and FIs are subject to changes based on revisions filed by them.
4. Frauds reported in a year could have occurred several years prior to year of reporting.
5. Amounts involved reported do not reflect the amount of loss incurred. Depending on recoveries, the loss incurred gets reduced. Further, the entire amount involved is not necessarily diverted.
6. As on March 31, 2025, 783 frauds amounting to ₹1,12,911 crore were withdrawn by banks due to non-compliance with the principles of natural justice as per the judgment of the Hon'ble Supreme Court dated March 27, 2023.
7. Data pertaining to 2024-25 includes fraud classification in 122 cases amounting to ₹18,674 crore, pertaining to previous financial years, reported afresh during the current financial year after re-examination and ensuring compliance with the judgement of the Hon'ble Supreme Court, dated March 27, 2023.

Source: RBI Supervisory Returns.

(11) RBI's cloud storage facility to help localise data

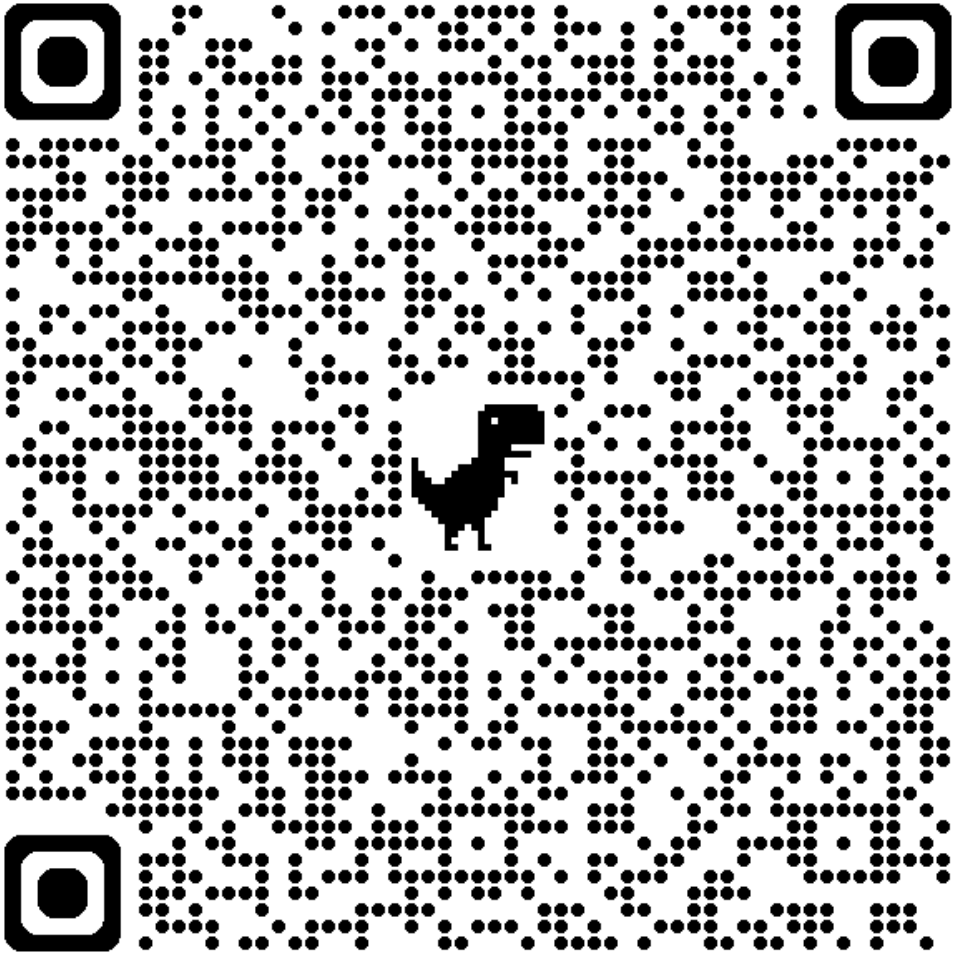
https://timesofindia.indiatimes.com/business/india-business/rbis-cloud-storage-facility-to-help-localise-data/articleshow/121494651.cms



May 29, 2025

(12) BSE issues cybersecurity advisory amid rising Pakistan-linked threats to Indian BFSI Sector

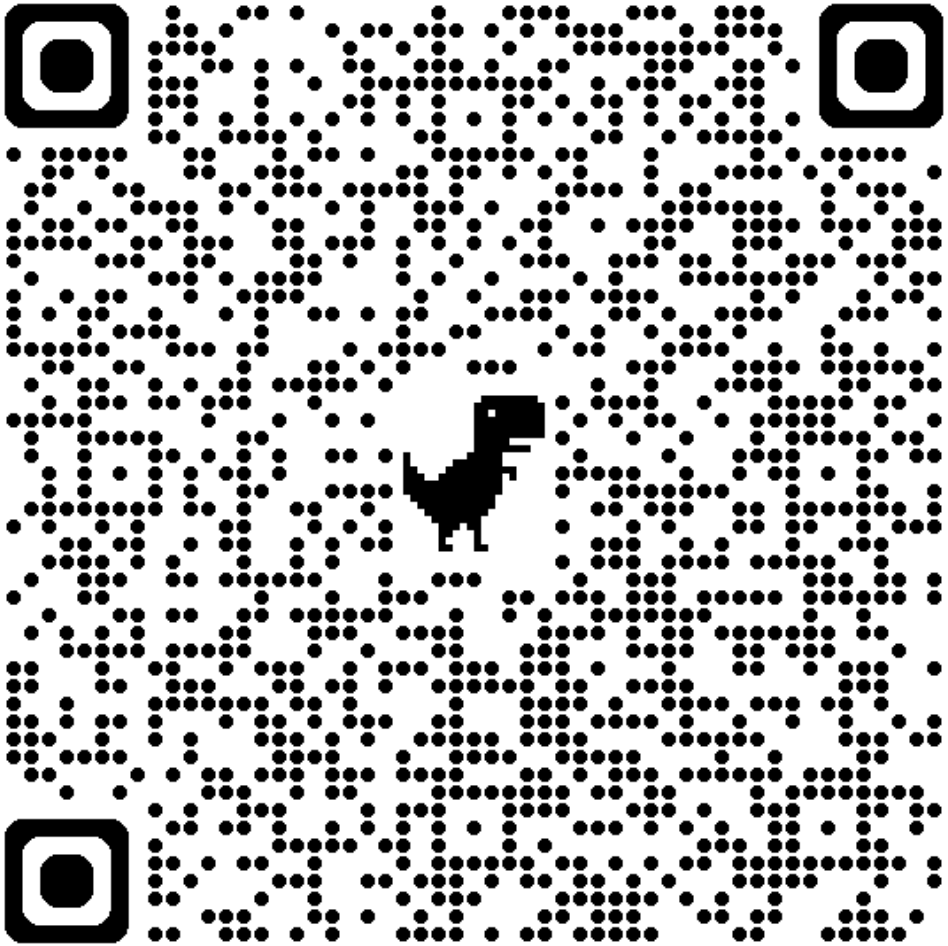
https://economictimes.indiatimes.com/markets/stocks/news/bse-issues-cybersecurity-advisory-amid-rising-pakistan-linked-threats-to-indian-bfsi-sector/articleshow/120987424.cms



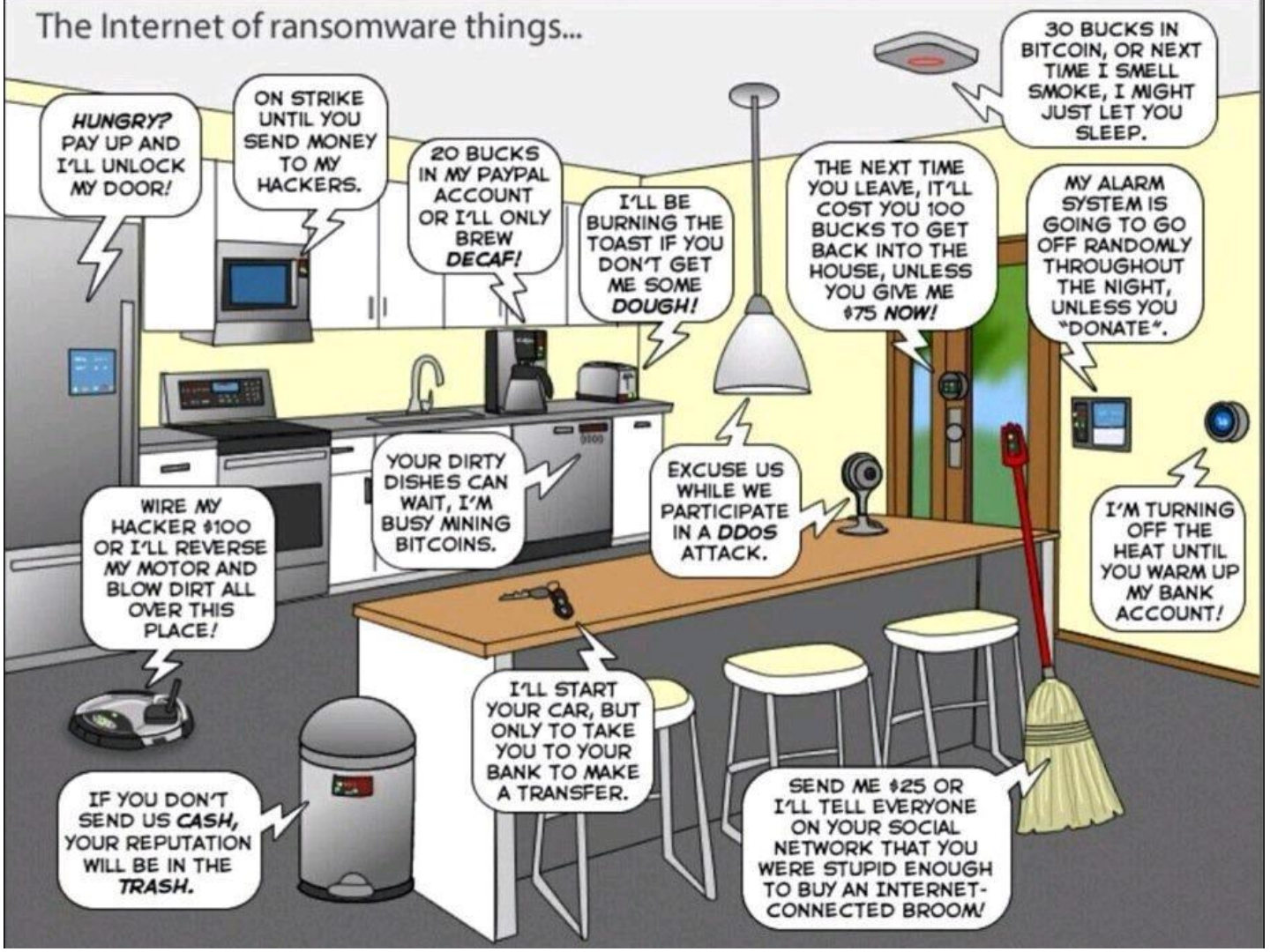
May 08, 2025

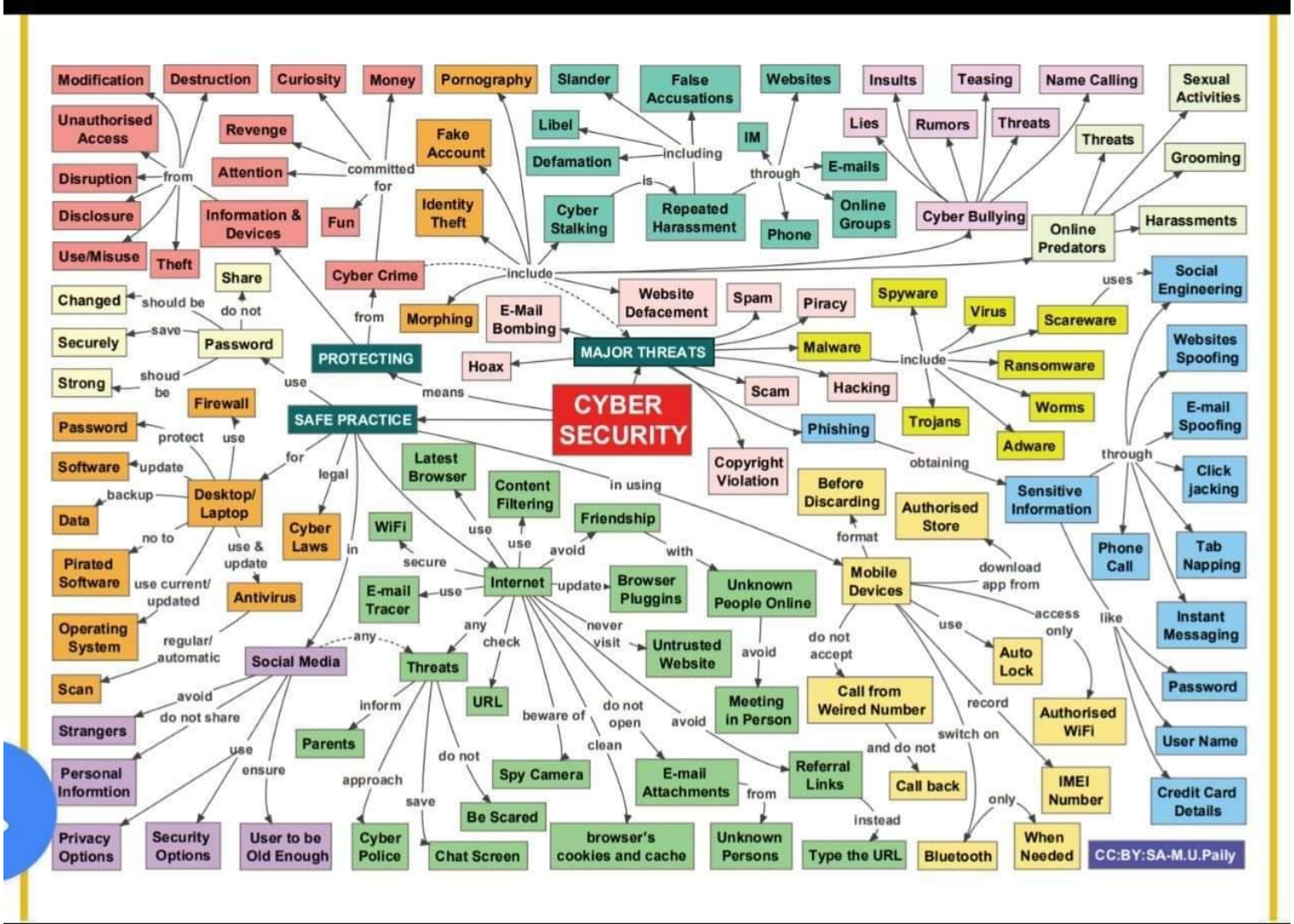
(13) BFSI not ready to tackle Quantum Computing threats, says study

https://timesofindia.indiatimes.com/city/hyderabad/bfsi-not-ready-to-tackle-quantum-computing-threats-says-study/articleshow/121170313.cms



May 15, 2025


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!


CYBER SECURITY
PROTECTING
MAJOR THREATS
SAFE PRACTICE
Modification
Destruction
Curiosity
Money
Pornography
Slander
False Accusations
Websites
Insults
Teasing
Name Calling
Sexual Activities
Unauthorised Access
Revenge
Fake Account
Libel
IM
Lies
Rumors
Threats
Threats
Grooming
Disruption
Attention
committed for
Defamation
including
through
E-mails
Disclosure
from
Information & Devices
Fun
Identity Theft
Cyber Stalking
is
Repeated Harassment
Phone
Online Groups
Cyber Bullying
Online Predators
Harassments
Use/Misuse
Theft
Share
Cyber Crime
include
Social Engineering
uses
Changed
should be
do not
Morphing
E-Mail Bombing
Website Defacement
Spam
Piracy
Spyware
Virus
Scareware
Securely
save
Password
from
Hoax
Malware
include
Ransomware
Websites Spoofing
Strong
shoud be
use
means
Scam
Hacking
Worms
Firewall
Trojans
E-mail Spoofing
Password
protect
use
Phishing
Adware
Software
update
for
Latest Browser
Content Filtering
Copyright Violation
obtaining
through
Click jacking
backup
Desktop/ Laptop
legal
in using
Before Discarding
Authorised Store
Sensitive Information
Data
Cyber Laws
WiFi
Friendship
format
Phone Call
Tab Napping
no to
use
use
avoid
with
Pirated Software
use & update
in
secure
Internet
update
Browser Pluggins
Unknown People Online
Mobile Devices
download app from
use current/ updated
E-mail Tracer
use
Antivirus
Instant Messaging
Operating System
regular/ automatic
any
check
never visit
Untrusted Website
avoid
do not accept
access only
like
Auto Lock
Social Media
Threats
Password
Scan
avoid
URL
Meeting in Person
Call from Weired Number
record
Authorised WiFi
Strangers
do not share
inform
beware of
do not open
avoid
switch on
User Name
Parents
clean
and do not
Personal Informtion
use
ensure
do not
Spy Camera
E-mail Attachments
Referral Links
Call back
IMEI Number
Credit Card Details
approach
save
Be Scared
from
only
Privacy Options
Security Options
User to be Old Enough
Cyber Police
Chat Screen
browser's cookies and cache
Unknown Persons
instead
Type the URL
Bluetooth
When Needed
CC:BY:SA-M.U.Paily

IT Act 2000

Overview

The Information Technology Act, 2000

- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill.
- The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000

Unauthorised Access - Section 43

“If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network.”
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.”
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network “

Damaging Computer – Section 43

“If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network”
(e) disrupts or causes disruption of any computer, computer system or computer network”
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means”

Facilitating Access – Section 43

“If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder”.
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.”
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.”

Tampering with Computer Source Documents - Section 65

“Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any **computer source code used for a computer, computer programming, computer system or computer network**, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable

- with imprisonment up to three years, or
- with fine which may extend up to two lakh rupees, or
- with both. “

Hacking, Copying, Downloading etc. with Dishonest & Fraudulent Intention – Section 66

“If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable

- with imprisonment for a term which may extend to three years or
- with fine which may extend to five lakh rupees or
- with both. “

Punishment for Sending Offensive Messages through Communication Service etc. – Section 66A

“Any person who sends, by means of a computer resource or a communication device,-
a) any information that is grossly **offensive** or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing **annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will**, persistently makes by making use of such computer resource or a communication device,
c) any electronic mail or electronic mail message for the purpose of causing **annoyance or inconvenience or to deceive or to mislead** the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine. “

Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device - Section 66B

“Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished

- with imprisonment of either description for a term which may extend to three years or
- with fine which may extend to rupees one lakh or
- with both. “

Punishment for Identity theft - Section 66C

“Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with

- imprisonment of either description for a term which may extend to three years and
- shall also be liable to fine which may extend to rupees one lakh “

Punishment for Cheating by Personation by using Computer Resource - Section 66D

“Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with

- imprisonment of either description for a term which may extend to three years and
- shall also be liable to fine which may extend to one lakh rupees “

Punishment for Violation of Privacy - Section 66E

“Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be

- punished with imprisonment which may extend to three years or
- with fine not exceeding two lakh rupees, or
- with both “

Punishment for Cyber Terrorism - Section 66F

Section 66F deals with Cyber Terrorism i.e. one who causes denial of access to computer resources, or has unauthorized access to a computer resource, or introduces a virus, with the **intent to threaten the unity, integrity, security or sovereignty of India** or to strike terror in any section of the people is deemed to be committing cyber terrorism.

Punishment for Publishing or Transmitting Obscene Material in Electronic Form - Section 67

As per Section 67, a material is obscene, if it is lascivious, appeals to prurient interest of a person and has the tendency to deprave and corrupt all those who are likely to read, see or hear the material via the net

Punishment for Transmission of Material Containing Sexually Explicit Act etc. in Electronic Form - Section 67A

This Section covers "Sexually Explicit Content" transmitted in electronic form. The term "sexually explicit act or conduct" has not been defined.

Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc. in Electronic Form - Section 67B

- For the purposes of this section, “children” means a person who has not completed the age of 18 years.”
- The section 67B deals with child pornography. This section makes even the recording in electronic form of any sexually explicit act with children shall be punishable under this section. Even if one is found to be engaged in online relationship with sexual overtone that may offend a reasonable adult on the computer resource

Offences with Three Years Imprisonment to be Cognizable - Section 77B

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of upto three years shall be bailable.

Offence	Cognizable or Non cognizable	Bailable or Non- bailable
Imprisonment less than 3 years	Non Cognizable	Bailable
Imp. of three years	Cognizable	Bailable
Imp. of more than 3 years	Cognizable	Non-Bailable

* Cognizable offence/case means a case in which, a police officer may arrest without warrant, as per the First Schedule of the Criminal Procedure Code, 1973 or under any other law for the time being in force.

Niraj Agarwal

We would love to hear from you

Built in the City of Joy with Security First

Kolkata, India

+91 9051 234 233

info@cyberyog.com

www.cyberyog.com