Welcome To The User Awareness Training

Of

Information security management (ISMS)

GEMINI SOLUTIONS
VISUALIZE SUCCESS

'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected'

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INFORMATION LIFECYCLE

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INFORMATION TYPES

- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronics means
- Shown on corporate videos
- Displayed/published on web
- Verbal-spoken in conversation

'...Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected'

GEMINI SOLUTIONS
VISUALIZE SUCCESS

WHAT IS INFORMATION SECURITY ?

- **Information Security** is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one

GEMINI SOLUTIONS
VISUALIZE SUCCESS

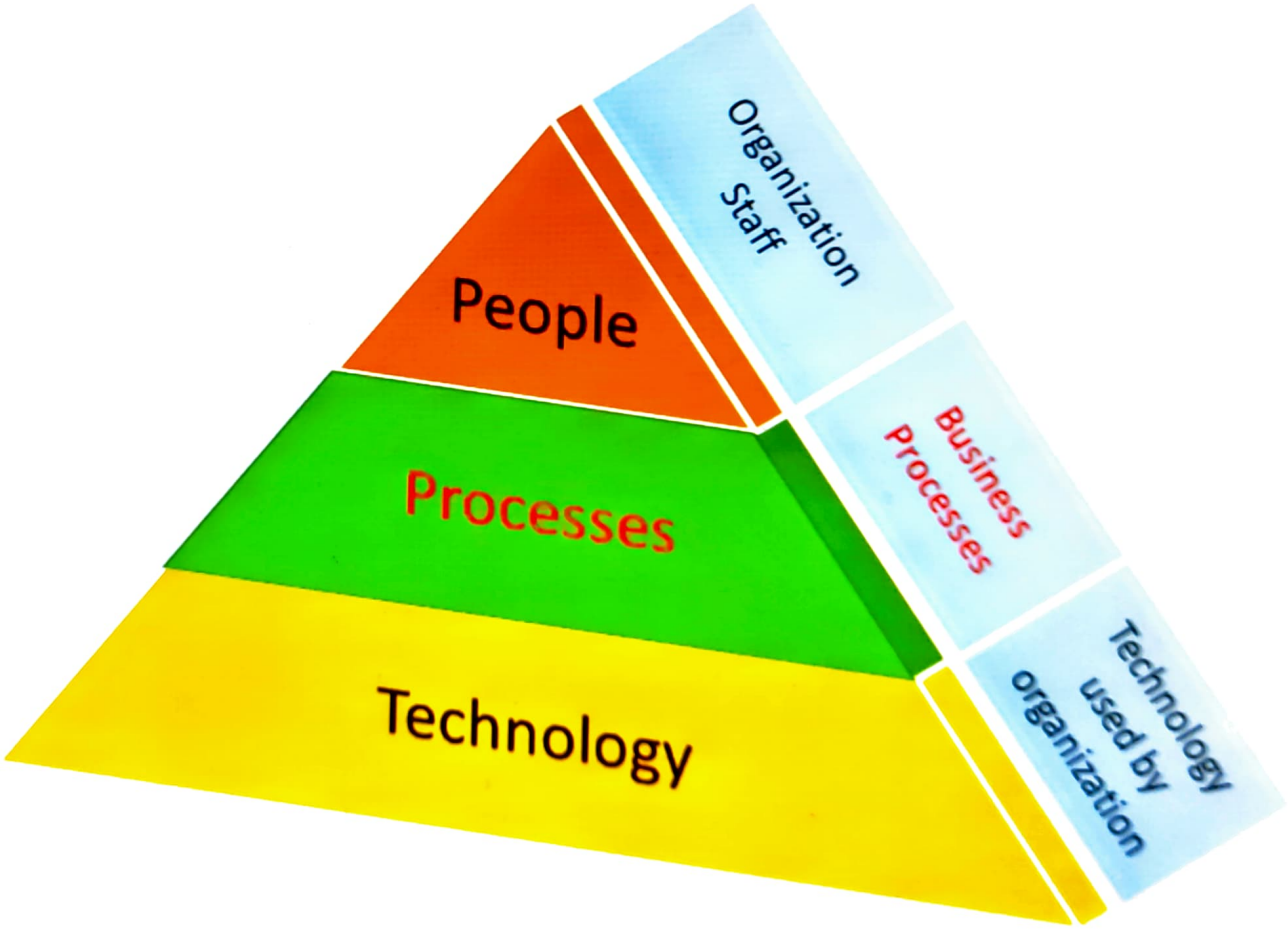
INFORMATION SECURITY

1. Protects information from a range of threats
2. Ensures business continuity
3. Minimizes financial loss
4. Optimizes return on investments
5. Increases business opportunities

Business survival depends on information security

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INFOSEC COMPONENTS



GEMINI SOLUTIONS
VISUALIZE SUCCESS

PEOPLE "WHO WE ARE"

People who use or interact with the Information include:

- Share Holders / Owners
- Management
- Employees
- Business Partners
- Service providers
- Contractors
- Customers / Clients
- Regulators etc.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

PROCESS "WHAT WE DO"

The processes refer to "work practices" or workflow. Processes are the repeatable steps to accomplish business objectives. Typical process in our IT Infrastructure could include:

- Helpdesk / Service management
- Incident Reporting and Management
- Change Requests process
- Request fulfilment
- Access management
- Identity management
- Service Level / Third-party Services Management
- IT procurement process etc...

GEMINI SOLUTIONS
VISUALIZE SUCCESS

TECHNOLOGY "WHAT WE USE TO IMPROVE WHAT WE DO"

Network Infrastructure:

- Cabling, Data/Voice Networks and equipment
- Telecommunications services (PABX), including VoIP services , ISDN , Video Conferencing
- Server computers and associated storage devices
- Operating software for server computers
- Communications equipment and related hardware.
- Intranet and Internet connections
- VPNs and Virtual environments
- Remote access services
- Wireless connectivity

GEMINI SOLUTIONS
VISUALIZE SUCCESS

TECHNOLOGY "WHAT WE USE TO IMPROVE WHAT WE DO"

Application software:

- Finance and assets systems, including Accounting packages, Inventory management, HR systems, Assessment and reporting systems
- Software as a service (Sass) - instead of software as a packaged or custom-made product. Etc..

Physical Security components:

- CCTV Cameras
- Clock in systems / Biometrics
- Environmental management Systems: Humidity Control, Ventilation , Air Conditioning, Fire Control systems
- Electricity / Power backup

Access devices:

- Desktop computers
- Laptops, ultra-mobile laptops and PDAs
- Thin client computing.
- Digital cameras, Printers, Scanners, Photocopier etc.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INFORMATION ATTRIBUTES: ISO defines Information Security as the preservation of

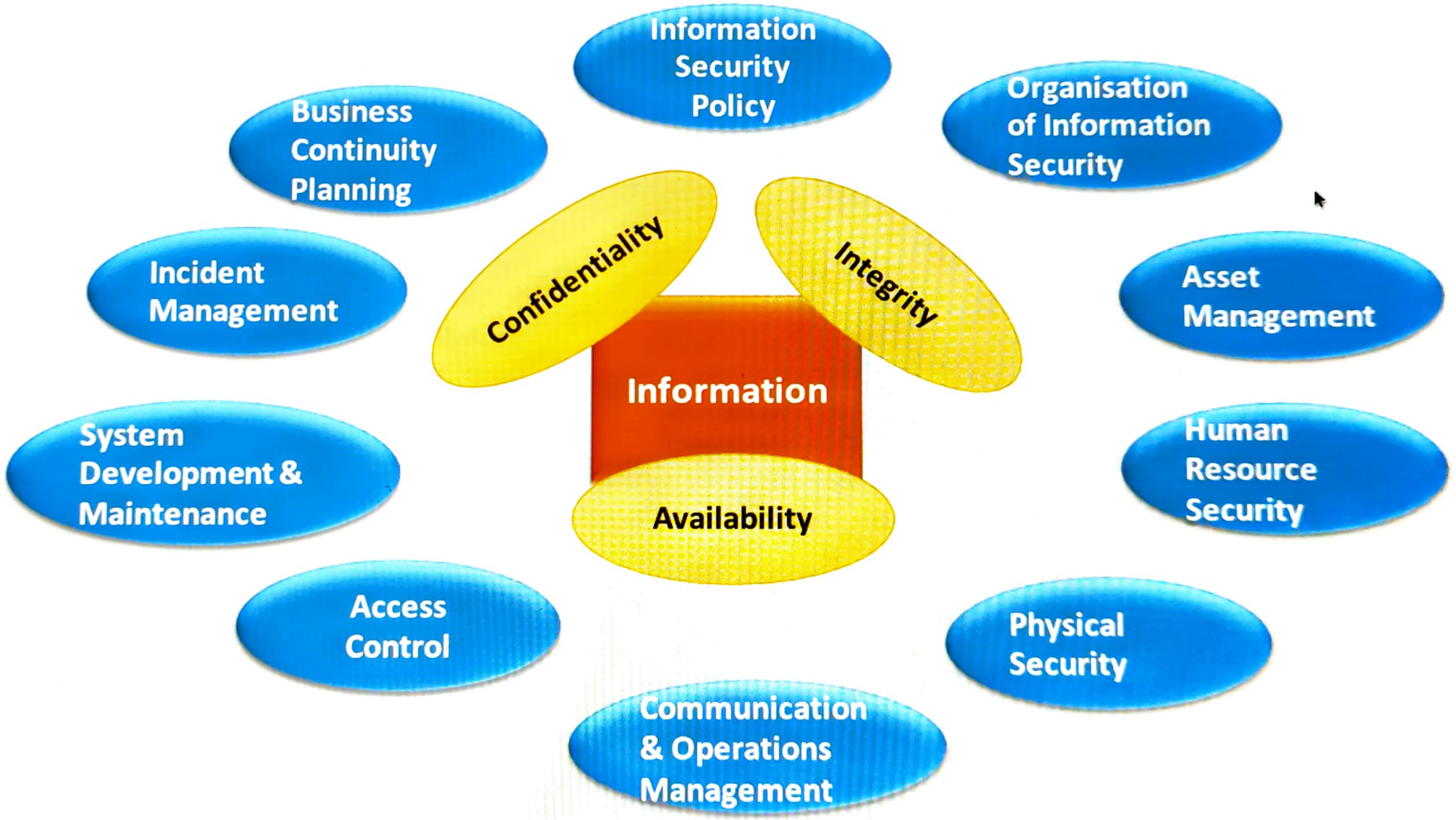
Security breaches leads to...

- Reputation loss
- Financial loss
- Intellectual property loss
- Legislative Breaches leading to legal actions (Cyber Law)
- Loss of customer confidence
- Business interruption costs

LOSS OF GOODWILL

GEMINI SOLUTIONS

CONTROL CLAUSES



GEMINI SOLUTIONS
VISUALIZE SUCCESS

CONTROL CLAUSES

- **Information Security Policy** - To provide management direction and support for Information security.
- **Organisation Of Information Security** - Management framework for implementation
- **Asset Management** - To ensure the security of valuable organisational IT and its related assets
- **Human Resources Security** - To reduce the risks of human error, theft, fraud or misuse of facilities.
- **Physical & Environmental Security** -To prevent unauthorised access, theft, compromise , damage, information and information processing facilities.
- **Communications & Operations Management** - To ensure the correct and secure operation of information processing facilities.
- **Access Control** - To control access to information and information processing facilities on 'need to know' and 'need to do' basis.
- **Information Systems Acquisition, Development & Maintenance** - To ensure security built into information systems

GEMINI SOLUTIONS

CONTROL CLAUSES (CONT..)

- **Information Security Incident Management** - To ensure information security events and weaknesses associated with information systems are communicated.
- **Business Continuity Management** - To reduce disruption caused by disasters and security failures to an acceptable level.
- **Compliance** - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INFORMATION ASSET CLASSIFICATION

- **CONFIDENTIAL:** If this information is leaked outside Organisation, it will result in major financial and/or image loss. Compromise of this information will result in statutory, legal non-compliance. Access to this information must be restricted based on the concept of need-to-know. Disclosure requires the information owner's approval. In case information needs to be disclosed to third parties a signed confidentiality agreement is also required. Examples include Customer contracts, rate tables, process documents and new product development plans.

- **INTERNAL USE ONLY:** If this information is leaked outside Organisation, it will result in Negligible financial loss and/or embarrassment. Disclosure of this information shall not cause serious harm to Organisation, and access is provided freely to all internal users. Examples include circulars, policies, training materials etc.

- **PUBLIC:** Non availability will have no effect. If this information is leaked outside Organisation, it will result in no loss. This information must be explicitly approved by the Corporate Communications Department or Marketing Department in case of marketing related information, as suitable for public dissemination. Examples include marketing brochures, press releases.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CONFIDENTIALITY - INFORMATION ASSET

- Confidentiality of information refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing organization security to the disclosure of private data of employees. Following table provides guideline to determine Confidentiality requirements:

CONFIDENTIALITY REQUIREMENT	EXPLANATION
Low	Non-sensitive information available for public disclosure. The impact of unauthorized disclosure of such information shall not harm Organisation anyway. E.g. Press releases, Company's News letters e.g. Information published on company's website
Medium	Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a limited harm to the organization. e.g. Organization Charts, Internal Telephone Directory.
High	Information which is very sensitive or private, of highest value to the organization and intended to use by named individuals only. The unauthorized disclosure of such information can cause severe harm (e.g. Legal or financial liability, adverse competitive impact, loss of brand name). E.g. Client's pricing information, Merger and Acquisition related Information, Marketing strategy

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INTEGRITY - INFORMATION ASSET

- Integrity refers to the completeness and accuracy of Information. Integrity is lost if unauthorized changes are made to data or IT system by either intentional or accidental acts. If integrity of data is not restored back, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions. Integrity criteria of information can be determined with guideline established in the following Table:

INTEGRITY REQUIREMENT	EXPLANATION
Low	There is minimal impact on business if the accuracy and completeness of data is degraded.
Medium	There is significant impact on business if the asset if the accuracy and completeness of data is degraded.
High	The Integrity degradation is unacceptable.

GEMINI SOLUTIONS

AVAILABILITY - INFORMATION ASSET

- Availability indicates how soon the information is required, in case the same is lost. If critical information is unavailable to its end users, the organization's mission may be affected. Following Table provides guideline to determine availability criteria of information assets.

AVAILABILITY REQUIREMENT	EXPLANATION
Low	There is minimal impact on business if the asset / information is not Available for up to 7 days
Medium	There is significant impact on business if the asset / information is not Available for up to 48 hours
High	The Asset / information is required on 24x7 basis

GEMINI SOLUTIONS
VISUALIZE SUCCESS

NON-INFORMATION ASSETS [PHYSICAL]

- Information is processed with the help of technology. The assets, which are helpful in creating, processing, output generation and storage. Such assets need to be identified and valued for the purpose of their criticality in business process.

- Asset valuation of non information / physical Assets like software, Hardware, Services is carried out based on different criteria applicable to the specific group of physical assets involved in organization's business processes.

GEMINI SOLUTIONS

CONFIDENTIALITY - NON-INFORMATION ASSET

- Confidentiality factor is to be determined by the services rendered by the particular asset in specific business process and the confidentiality requirement of the information / data processed or stored by the asset. This table provides a guideline to identify the Confidentiality requirements and its link to Classification label.

CONFIDENTIALITY REQUIREMENT	EXPLANATION
Low	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as LOW.
Medium	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as Medium.
High	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as HIGH.

GEMINI SOLUTIONS

INTEGRITY - NON INFORMATION ASSET

Integrity factor is to be determined by the reliability and dependability of the particular asset in specific business process and the Integrity requirement of the information / data processed or stored by the asset. This table provides a guideline to identify the Integrity requirements and its link to Classification label.

INTEGRITY REQUIREMENT	EXPLANATION
Low	Dependency and reliability of the services rendered by the particular asset in a business process is LOW. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as LOW.
Medium	Dependency and reliability of the services rendered by the particular asset in a business process is Medium. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as Medium.
High	Dependency and reliability of the services rendered by the particular asset in a business process is HIGH. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as High.

GEMINI SOLUTIONS

AVAILABILITY - NON-INFORMATION ASSET

Availability factor is to be determined on the basis of impact of non availability of the asset on the business process. This table provides a guideline to identify the Availability requirements and its link to Classification label.

INTEGRITY REQUIREMENT	EXPLANATION
Low	Impact of non availability of an asset in a business process is LOW. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as LOW.
Medium	Impact of non availability of an asset in a business process is Medium. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as MEDIUM.
High	Impact of non availability of an asset in a business process is HIGH. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as HIGH.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

PEOPLE ASSETS

Information is accessed or handled by the people from within the organization as well as the people related to organization for business requirements.

It becomes necessary to identify such people from within the organization as well as outside the organization who handle the organization's information assets.

The analysis such people, who has access rights to the assets of the organization, is to be done by Business Process Owner i.e. process / function head.

The people assets shall include roles handled by

- Employees
- Contract Employees
- Contractors & his employees

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CONFIDENTIALITY - PEOPLE ASSETS

CONFIDENTIALITY REQUIREMENT	EXPLANATION
Low	The role or third party identified has access limited to information assets classified as 'Public'. Security breach by individual/s whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has access limited to information assets classified as 'Internal' and 'Public'. Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role employee or third party identified has access to all types of information assets including information assets classified as 'Confidential' Or IT Assets classified as 'Critical'. Security breach by individual/s to whom the role is assigned would severely affect the business operations.

GEMINI SOLUTIONS

INTEGRITY – PEOPLE ASSETS

INTEGRITY REQUIREMENT	EXPLANATION
Low	The role or third party identified has limited privilege to change information assets classified as 'Internal' or 'Public' and the his work is supervised. Security breach by individual/ s to whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has privilege to change information assets classified as 'Internal', and 'Public' Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role or third party identified has privilege to change information assets classified as 'Confidential' Or Change the configuration of IT assets classified as 'Critical' Security breach by individual/s to whom the role is assigned would severely affect the business operations.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

AVAILABILITY – PEOPLE ASSETS

AVAILABILITY REQUIREMENT	EXPLANATION
Low	Unavailability of the individual/s whom the role is assigned would have insignificant affect the business operations.
Medium	Unavailability of the individual/s whom the role is assigned would moderately affect the business operations.
High	Unavailability of the individual/s whom the role is assigned would severely affect the business operations

GEMINI SOLUTIONS

WHAT IS RISK, THREATS AND VULNERABILITIES?

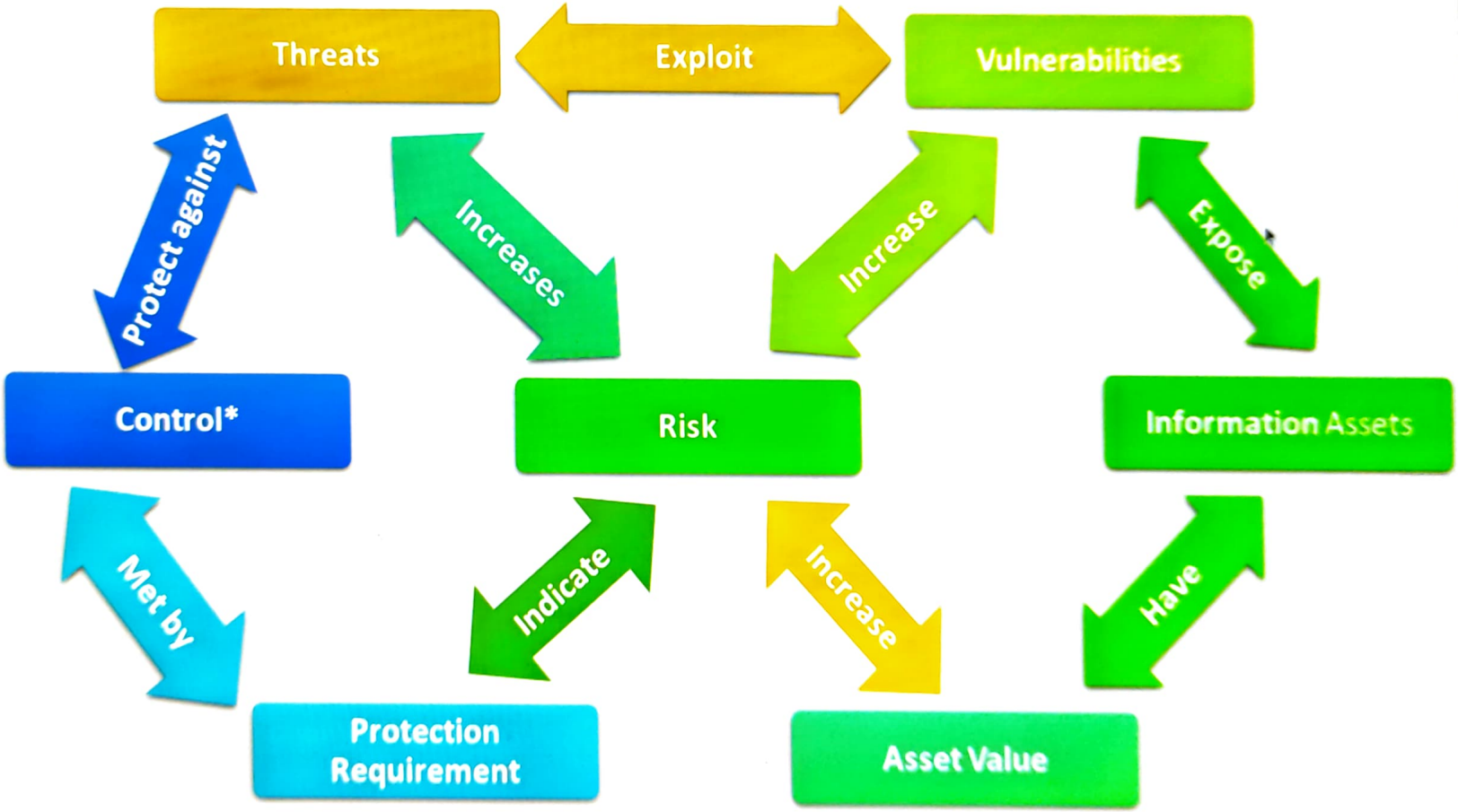
Risk: A possibility that a threat exploits a vulnerability in an asset and causes damage or loss to the asset.

Threat: Something that can potentially cause damage to the organization, IT Systems or network.

Vulnerability: A weakness in the organization, IT Systems, or network that can be exploited by a threat.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

RELATIONSHIP BETWEEN RISK, THREATS, AND VULNERABILITIES



*Controls: A practice, procedure or mechanism that reduces risk

GEMINI SOLUTIONS
VISUALIZE SUCCESS

THREAT IDENTIFICATION

Elements of threats

Agent : The catalyst that performs the threat.

- Human
- Machine
- Nature

Motive : Something that causes the agent to act.

- Accidental
- Intentional
- Only motivating factor that can be both accidental and intentional is human

Results : The outcome of the applied threat. The results normally lead to the loss of CIA

- Confidentiality
- Integrity
- Availability

GEMINI SOLUTIONS
VISUALIZE SUCCESS

Threats:

- Employees
- External Parties
- Low awareness of security issues
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural Disasters e.g. fire, flood, earthquake

Threat Sources

Sources	Motivation	Threat
External Hackers	Challenge Ego Game Playing	System hacking Social engineering Dumpster diving
Internal Hackers	Deadline Financial problems Disenchantment	Backdoors Fraud Poor documentation
Terrorist	Revenge Political	System attacks Social engineering Letter bombs Viruses Denial of service
Poorly trained employees	Unintentional errors Programming errors Data entry errors	Corruption of data Malicious code introduction System bugs Unauthorized access

SOLUTIONS

No.	Categories of Threat	Example
1	Human Errors or failures	Accidents, Employee mistakes
2	Compromise to Intellectual Property	Piracy, Copyright infringements
3	Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
4	Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
5	Deliberate Acts of sabotage / vandalism	Destruction of systems / information
6	Deliberate Acts of theft	Illegal confiscation of equipment or information
7	Deliberate software attacks	Viruses, worms, macros Denial of service
8	Deviations in quality of service from service provider	Power and WAN issues
9	Forces of nature	Fire, flood, earthquake, lightening
10	Technical hardware failures or errors	Equipment failures / errors
11	Technical software failures or errors	Bugs, code problems, unknown loopholes
12	Technological obsolescence	Antiquated or outdated technologies

GEMINI SOLUTIONS
VISUALIZE SUCCESS

RISKS & THREATS

High User Knowledge of IT Systems

Theft, Sabotage, Misuse

Virus Attacks

Systems & Network Failure

Lack Of Documentation

Lapse in Physical Security

Natural Calamities & Fire

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CYBER SECURITY

GEMINI SOLUTIONS

CYBER SECURITY

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing.

Types of cyber threats:

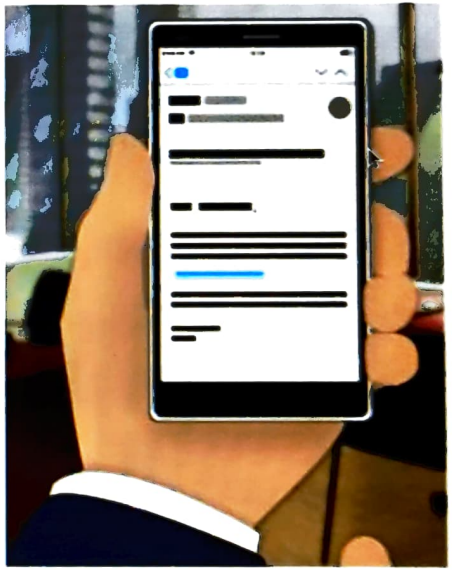
- **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
- **Cyber-attack** often involves politically motivated information gathering.
- **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

CYBER SECURITY ON MOBILE DEVICES

- **Always On, Always Available:**
  - Checking email is probably one of the most common things you do on your smartphone or tablet. Being available always means you may read and take action as soon as a malicious email arrives.
  - Multi-tasking on mobile devices may mean you are more distracted when using email. Take extra care when using email on your mobile device.
- **Space Is Scarce:**
  - The small form factor of mobile devices makes it harder to spot obvious indicators of phishing emails. If you receive a suspicious email, inspect it on a larger screen if necessary.

CYBER SECURITY ON MOBILE DEVICES

- **Malware Is Invisible on Most Mobile Devices:**
  - It can send harmful emails to your contacts. It may extract valuable personal information and your organization's proprietary data.
  - It may record your phone conversations, capture your location, manipulate text messages, and more. Most smartphones and tablets have little in the way of security and anti-malware protection.



- **Think Before You Click:**
  - When you receive an email, pause for a moment. Attackers count on your immediate action from messages that communicate urgency.
  - Take the time to really read an email before deciding to do anything with it. Phishing emails will also be easier to spot if you are less distracted.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CYBER SECURITY ON MOBILE DEVICES

- **Verify the Sender:**
  - If someone you are familiar with sends you an unexpected email containing a link or attachment, you should be suspicious.
  - Send an instant message, make a phone call, or speak directly to the person you think sent the email to verify the email's authenticity.

- **Notify Cybersecurity:**
  - If you suspect an email to be a phish or malicious, report it as a phishing email or mark it spam and alert Gemini's cybersecurity in the IT department. Forwarding the mail to the IT team will allow for cyber professionals to review and validate the communication.
  - If the mail is determined to be malicious it will be quarantined and removed from the environment. Legitimate email will be returned.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CYBER SECURITY ON MOBILE DEVICES

- **Read It Elsewhere:**
  - When you're in doubt, don't click the link or open the attachment. Instead, review the email on a laptop or desktop computer.
  - The larger screen will give you greater visibility in order to verify an email's authenticity.

- **Find Out Where Email Links Go:**

- Your smartphone or tablet lacks a cursor, so it's harder to make hovering over links a habit. You can still find out a link's true destination:
  - Carefully tap and press the link until you see a menu pop up. Note: Depending on your device, how hard and long you tap and press varies. Refer to your device's instructions for checking URLS.
  - In the menu, make sure that the web address is recognizable and seems to be related to the content of the email.
  - If the web address looks unrelated to the email's message or the sender's email domain, don't follow the link.

TYPES OF CYBER THREATS

GEMINI SOLUTIONS
VISUALIZE SUCCESS

TYPES OF CYBER THREATS

Malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Bot-nets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

TYPES OF CYBER THREATS

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

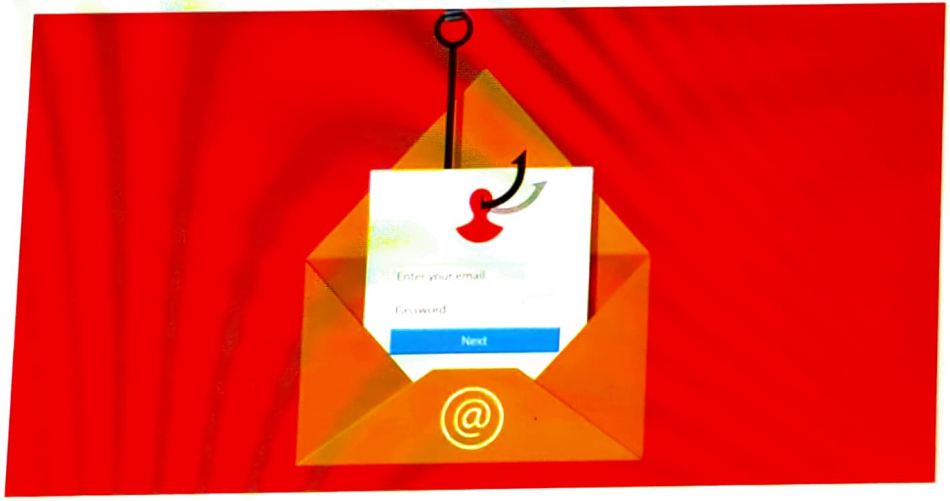
SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

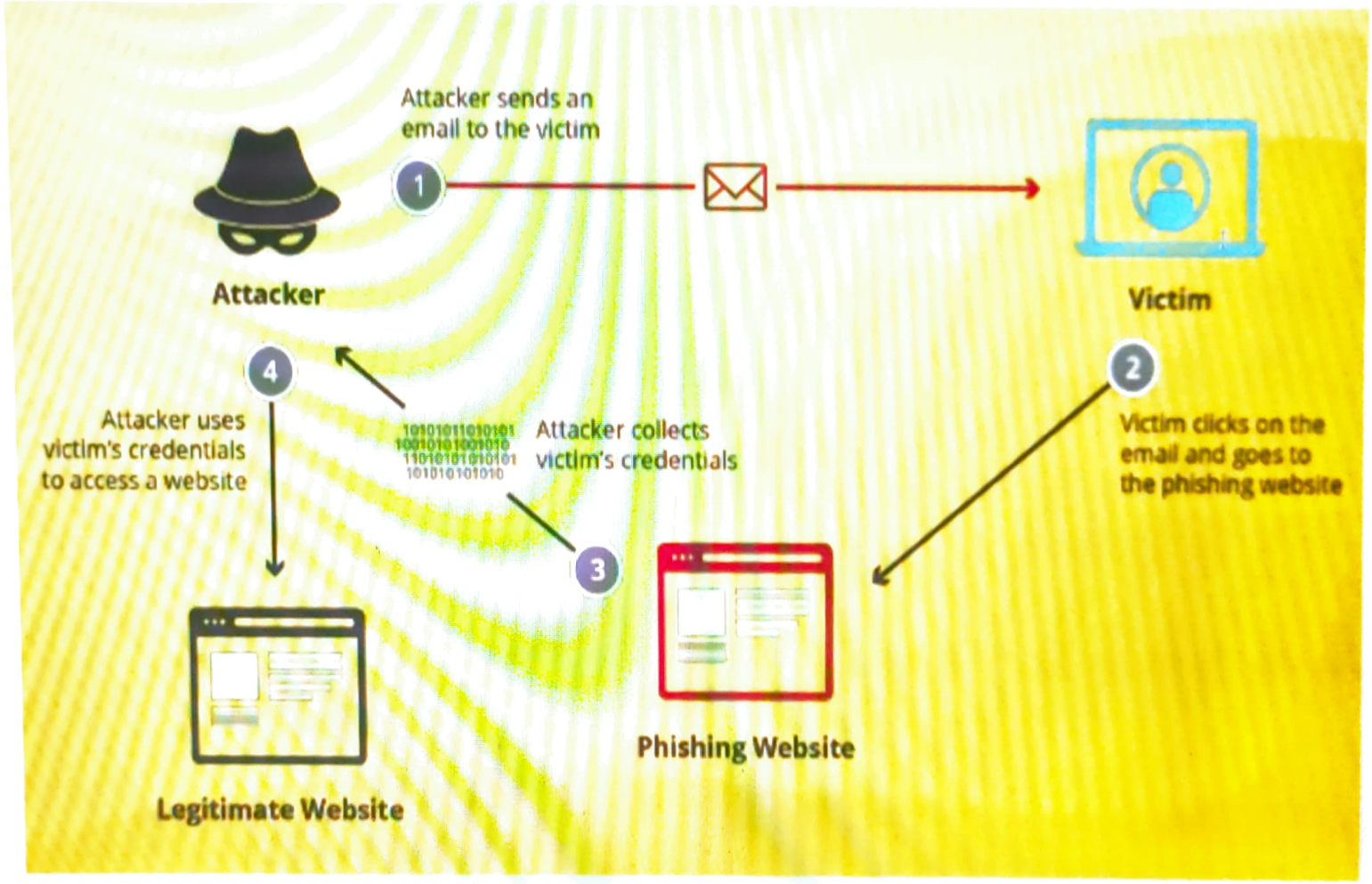
PHISHING

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with.



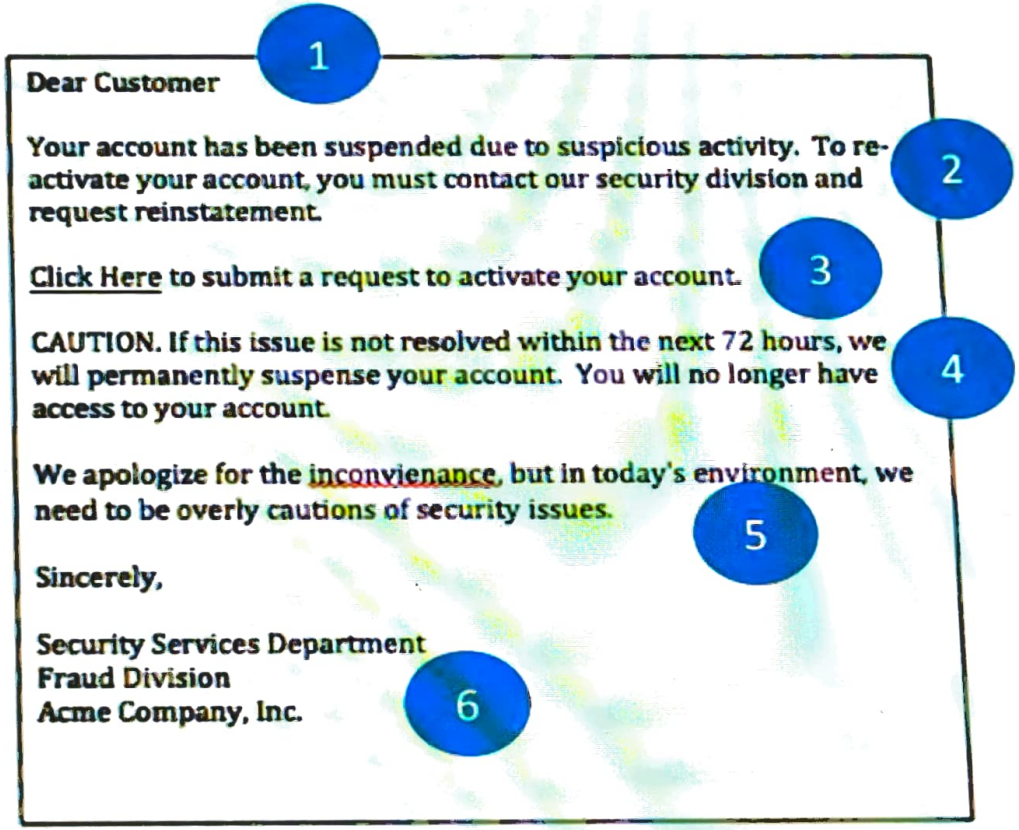
HOW DOES PHISHING WORK?



GEMINI SOLUTIONS
VISUALIZE SUCCESS

EXAMPLE OF PHISHING

EXAMPLE OF PHISHING

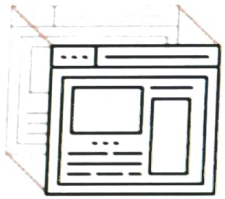


1. Generic Greeting
2. Invokes Fear
3. Requires Action
4. Threatening Language
5. Grammar Issues
6. Generic Closing

GEMINI SOLUTIONS
VISUALIZE SUCCESS

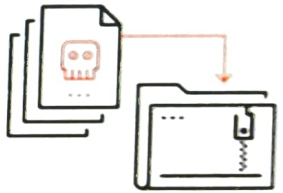
WHAT IS A PHISHING KIT?

The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources and tools that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits as well as mailing lists are available on the dark web.

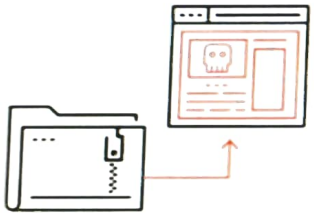


The legitimate website is cloned

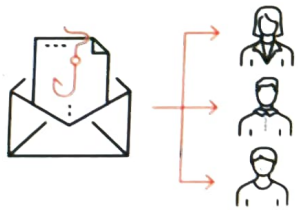
The login page is changed to point to a credential-stealing script



The modified files are bundled into a zip file to make a phishing kit



The phishing kit is uploaded to the hacked website, files are unzipped

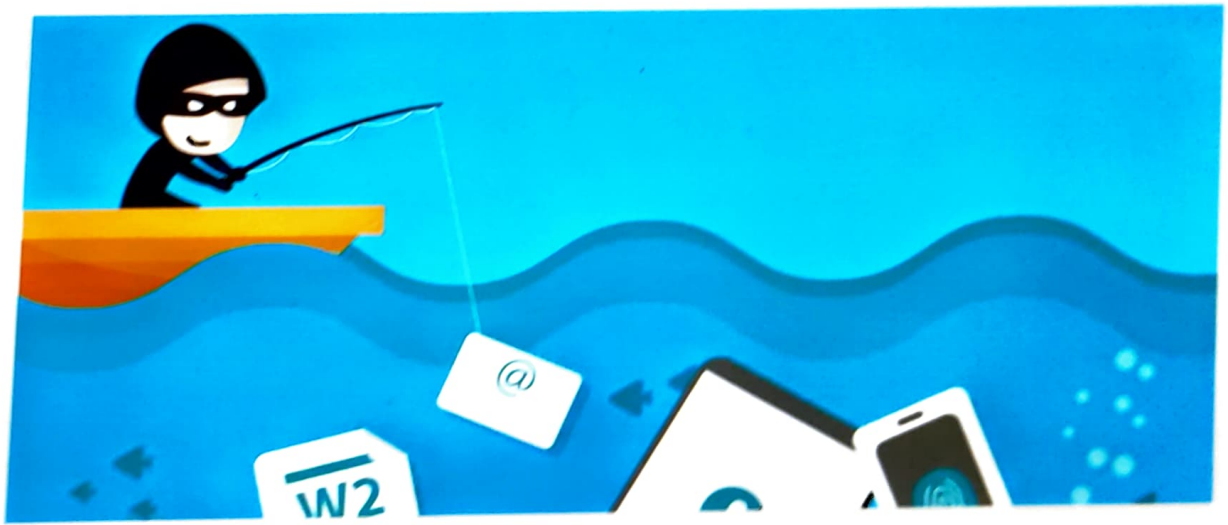


Emails are sent with links pointing to new spoof website

GEMINI SOLUTIONS
VISUALIZE SUCCESS

EFFECTS OF PHISHING

- Internet Fraud
- Identity Theft
- Financial Loss to Organization
- Difficulty in Law Enforcement Investigations
- Erosion of Public Trust in the Internet



GEMINI SOLUTIONS

HOW TO PREVENT PHISHING

There are a number of steps you can take and mind-sets you should get into that will keep you from becoming a phishing statistic, including:

- Always check the spelling of the URLs in email links before you click or enter sensitive information
- Watch out for URL redirects, where you're subtly sent to a different website with identical design
- If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media

BE CAUTIOUS OF E-MAIL PHISHING SPECIFICALLY RELATED TO COVID-19

Since March, we have seen a rapidly increasing number of cybercriminals using COVID-19 themed spear-phishing attacks. These cybercriminals are looking to bait targets to fake websites and collect Office 365 credentials.
Consider these steps to help reduce risk of working remotely:

- Raise awareness of the heightened risk of COVID-19 themed fraud and phishing attacks. The employees should voice concern if something seems out of place
- Be aware that there could be people posing as a CEO, CFO or another senior company figure looking to transfer corporate funds to other bank accounts
- Ensure all company provided technology has up to date anti-virus and firewall software
- Encrypt data-at-rest on laptops and add data loss prevention software to detect data breaches and leaks
- Before visiting any link, first hover over it to see the URL and try to avoid opening any unwanted or irrelevant attachments

REMOTE WORK'S MAIN SECURITY CHALLENGES

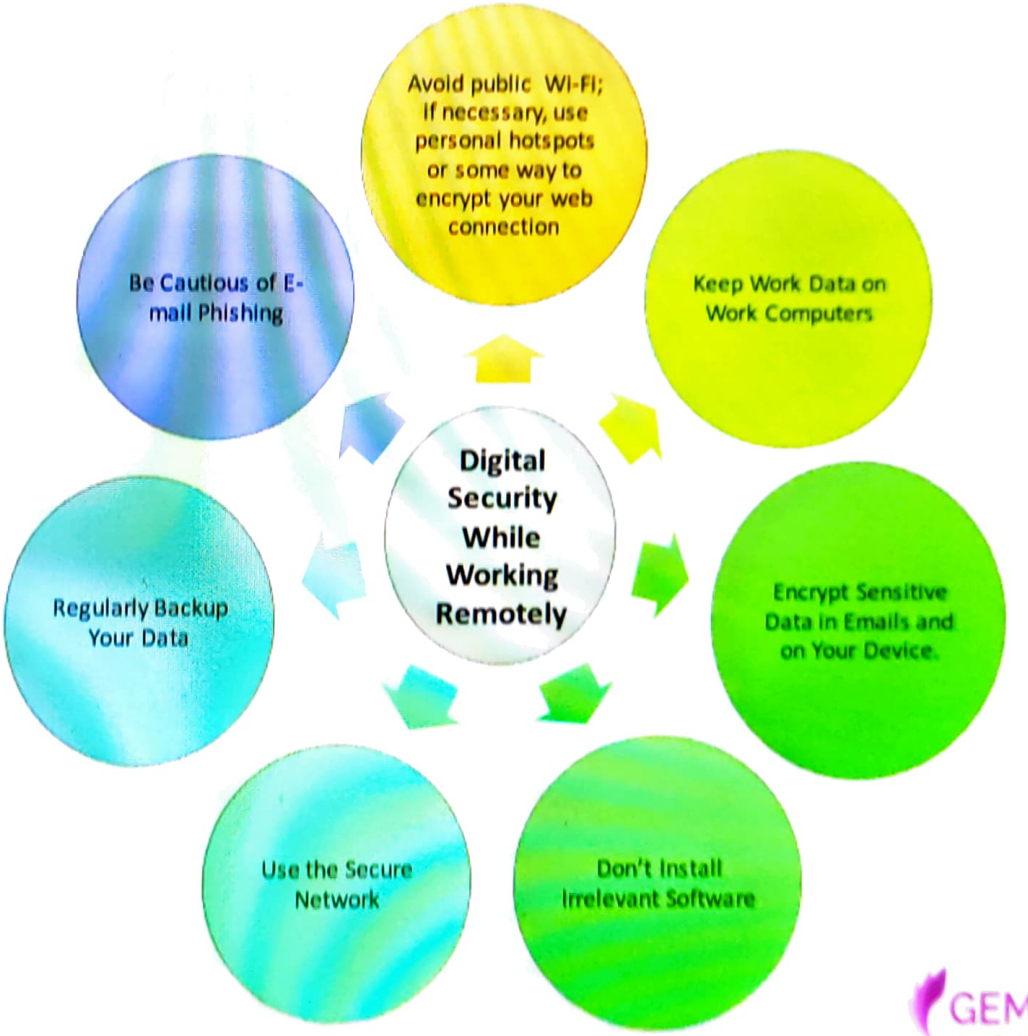
- **Remote Workers Lack Security Awareness**: Many employees are working from home for the first time. They don't know the best practices that experienced remote workers know well, such as using a VPN on public networks, or not saving sensitive information on their personal devices. Negligent employees are the number one cause of cybersecurity breaches and the risk increases exponentially when working remotely.
- **Reduced security on devices used remotely:** While at the office, companies have complete control of devices, defining secure physical and electronic layers. In remote work, employees often make use of personal devices and public networks.
- **Loss of data on remote devices:** Lack of proper options for data backup and recovery on remote devices can increase the damage from a data loss incident.
- **Breach of legal requirements:** Outside of the company's environment, it is more difficult to ensure employees' compliance with laws (e.g., GDPR) and contract clauses related to data protection.
- **Low engagement of remote employees with security practices:** Less contact with remote employees can make them less likely to follow security practices

GEMINI SOLUTIONS
VISUALIZE SUCCESS

BEST PRACTICES FOR WORKING REMOTELY

GEMINI SOLUTIONS

DIGITAL SECURITY WHILE WORKING REMOTELY



GEMINI SOLUTIONS

PHYSICAL SECURITY WHILE WORKING REMOTELY

- Lock Your Doors while working
- Never Leave Your Devices or Laptop in the Car
- Use a USB Data Blocker when Charging Up at a Public Phone Charging Station to prevent data exchange and guard against malware
- While working remotely, you must ensure that your system is password protected and secure
- Since you need to manage the login credentials or other sensitive data properly so do not leave such information written on any paper or notepad as a little carelessness with the same can cost you and the organization a lot.

GEMINI SOLUTIONS
VISUALIZE SUCCESS

ACCESS CONTROL - PHYSICAL

DO'S

- Follow Security Procedures
- Wear Identity Cards and Badges
- Ask unauthorized visitor his credentials
- Attend visitors in Reception and Conference Room only

DON'T'S

- Bring visitors in operations area without prior permission
- Bring hazardous and combustible material in secure area
- Practice "Piggybacking"
- Bring and use pen drives, zip drives, iPod, other storage devices unless and otherwise authorized to do so

GEMINI SOLUTIONS
VISUALIZE SUCCESS

PASSWORD GUIDELINES

DO'S

- Always use at least 8 character password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)
- Use passwords that can be easily remembered by you
- Change password regularly as per policy
- Use password that is significantly different from earlier passwords

DON'T'S

- Use passwords which reveals your personal information or words found in dictionary
- Write down or Store passwords
- Share passwords over phone or Email
- Use passwords which do not match above complexity criteria

GEMINI SOLUTIONS
VISUALIZE SUCCESS

INTERNET USAGE

DO'S

- Use internet services for business purposes only

DON'T'S

- Do not access internet through dial-up connectivity
- Do not use internet for viewing, storing or transmitting obscene or pornographic material
- Do not use internet for accessing auction sites
- Do not use internet for hacking other computer systems
- Do not use internet to download / upload commercial software / copyrighted material

➢ *Technology Department is continuously monitoring Internet Usage. Any illegal use of internet and other assets shall call for Disciplinary Action.*

E-MAIL USAGE

DO'S

- Use official mail for business purposes only
- Follow the mail storage guidelines to avoid blocking of E-mails
- If you come across any junk / spam mail, do the following
  - Remove the mail
  - Inform the security help desk
  - Inform the same to server administrator
  - Inform the sender that such mails are undesired

DON'T'S

- Do not use official ID for any personal subscription purpose
- Do not send unsolicited mails of any type like chain letters or E-mail Hoax
- Do not send mails to client unless you are authorized to do so
- Do not post non-business related information to large number of users
- Do not open the mail or attachment which is suspected to be virus or received from an unidentified sender

SECURITY INCIDENTS

Report Security Incidents (IT) to Helpdesk through

- E-mail to
- Telephone

e.g.: IT Incidents: Mail Spamming, Virus attack, Hacking, etc.

Non-IT Incidents: Unsupervised visitor movement, Information leakage, Bringing unauthorized Media

NOTE : Incase you receive an email from unknown sender that is outside Gemini or the content of the mail look suspicious, make sure that you mark the email as **SPAM**

SECURITY INCIDENTS

DO'S

- Ensure your Desktops are having latest antivirus updates
- Ensure your system is locked when you are away
- Always store laptops/ media in a lockable place
- Be alert while working on laptops during travel
- Ensure sensitive business information is under lock and key when unattended
- Ensure back-up of sensitive and critical information assets
- Understand Compliance Issues such as Cyber Law IPR, Copyrights, IT act2000 etc. Contractual Obligations with customer
- Verify credentials, if the message is received from unknown sender
- Always switch off your computer before leaving for the day
- Keep your self updated on information security aspects

DON'T'S

- Do not discuss security incidents with any one outside organization
- Do not attempt to interfere with, obstruct or prevent anyone from reporting incidents

GEMINI SOLUTIONS
VISUALIZE SUCCESS

CASE STUDY: Heartland Payment Systems

- Heartland was processing 100 million payment card transactions per month for 175,000 merchants — mostly small- to mid-sized retailers. The breach was discovered in January 2009 when **Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed**. The attackers exploited a known vulnerability to perform a SQL injection attack. Security analysts had warned retailers about the vulnerability for several years, and it made **SQL injection** the most common form of attack against websites at the time.
- Because of the breach, **the Payment Card Industry (PCI) deemed Heartland out of compliance with its Data Security Standard(DSS) and did not allow it to process payments of major credit card providers until May 2009**. The company also paid an estimated $145 million in compensation for fraudulent payments. **134 million credit cards were exposed.**
- The Heartland breach was a **rare example** where authorities caught the attacker. A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban American, was alleged to have masterminded the international operation that stole the credit and debit cards. **He was sentenced in March 2010 to 20 years in federal prison.**

GEMINI SOLUTIONS
VISUALIZE SUCCESS

Human Wall Is Always
Better Than A Firewall

. . . LET US BUILD A HUMAN WALL ALONG WITH FIREWALL

GEMINI SOLUTIONS
VISUALIZE SUCCESS

THANKYOU

GEMINI SOLUTIONS