RxLogix Corporation

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

Information Security Awareness Training

2020

CONFIDENTIAL

“Information Security is everyone’s responsibility”

RxLogix

Document control

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

Document ID	Version	Date	Author	Change Description
RX-TRN-DevOps-002	1.0	09-Oct-2020	Shiv Kant Sharma	Initial Version

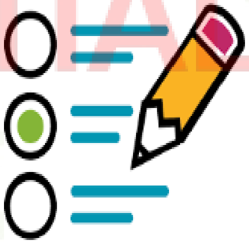
CONFIDENTIAL

Ground Rules

- Keep your mobile phone on silent mode.
- Ask questions if you have any doubts.
- Mute the microphone, if you are not speaking.
- Complete the assessment after the training.
- Have a fun / use humour.

Printed by [illegible]@rxlogix.com on [illegible] Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL



What is Information Security

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

Information security, often referred to as **InfoSec**, refers to the processes and tools designed and deployed to protect sensitive business information from unauthorize access, modification, disruption, destruction, and inspection.

CONFIDENTIAL

-Definition by Cisco Systems, Inc.

What is ISMS

- An **information security management system (ISMS)** is a framework of policies and controls that manage security and risks systematically and across the organization.

Printed by [illegible] on [illegible] 2021 at [illegible] AM UTC

- ISMS describes and demonstrates the organization's approach to Information Security. It includes how people, policies, controls and systems identify, address the opportunities and threats revolving around valuable information and related assets.

CONFIDENTIAL

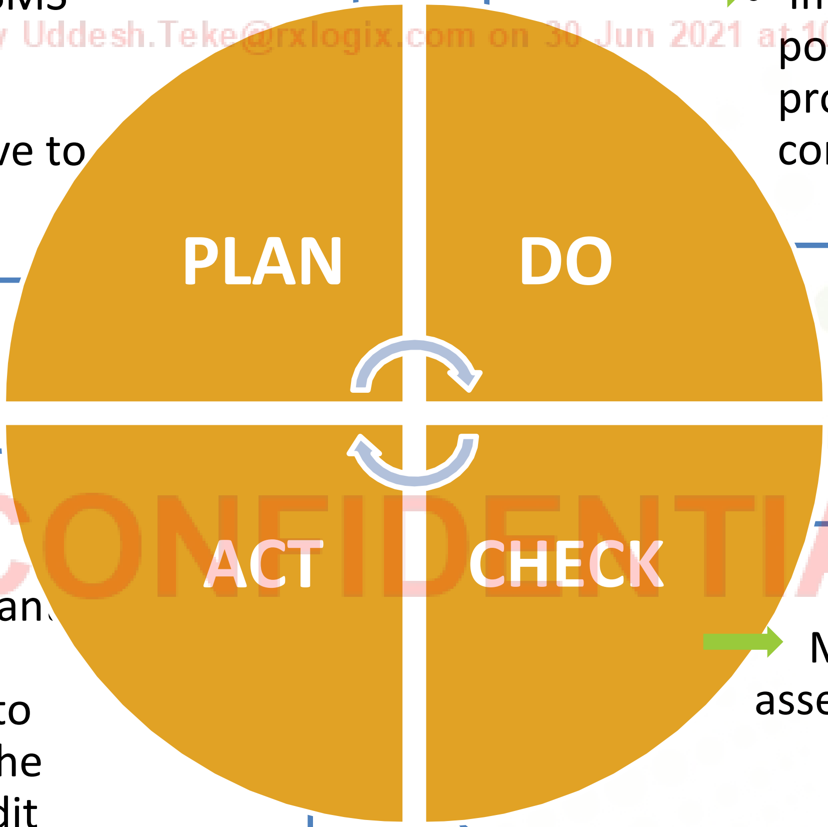
- ISMS standards and guidelines help organizations ready and compliant with information security part of below compliance **ISO2001, GDPR, NIST 800-53, HIPAA**

PDCA Cycle

- Establish ISMS policy, objectives, processes, and procedures relative to risk management

- Implement the ISMS policy, processes, procedures, and controls.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC



CONFIDENTIAL

- Initiate any relevan update or improvements to ISMS based on the results of an audit

- Monitor, review and assess ISMS

ISO 27001:2013 Clauses with PDCA

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

S.No	ISO 27001:2013 Clauses	PDCA Cycle
1	Scope	
2	Normative references	
3	Terms and definitions	
4	Context of the organization	PLAN
5	Leadership	PLAN
6	Planning	PLAN
7	Support	PLAN
8	Operation	DO
9	Performance evaluation	CHECK
10	Improvement	ACT

CONFIDENTIAL

ISO 27001:2013 Controls Domains

There are 114 controls in 14 domain:

A.5: Information security policies (2 controls)

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

A.6: Organization of information security (7 controls)

A.7: Human resource security - 6 controls that are applied before, during, or after employment

A.8: Asset management (10 controls)

A.9: Access control (14 controls)

A.10: Cryptography (2 controls)

A.11: Physical and environmental security (15 controls)

A.12: Operations security (14 controls)

A.13: Communications security (7 controls)

CONFIDENTIAL

A.14: System acquisition, development and maintenance (13 controls)

A.15: Supplier relationships (5 controls)

A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance (8 controls)

Need of Information Security

Information security is important because:

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- Protects information/data against various threats
- Maintain data confidentiality
- Ensures business continuity
- Minimize financial loss and other impacts
- Optimizes return on investments
- Creates opportunities to do business safely
- Maintains privacy and compliance

CONFIDENTIAL

Why Information Security Awareness is Important ?

- Human beings are still the weakest link (Most vulnerable) in any organization's Information Security system.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- When we analyze the anatomy of most successful cyberattacks, nearly all of them have one thing in common. Some user, somewhere, did something wrong that could have been avoided. In fact, research shows that human error is involved in 90%+ of all security breaches.

CONFIDENTIAL

- What employees do or don't do is the biggest threat to information systems and assets and every employee should aware of it.

Consequences Impact of Security breaches

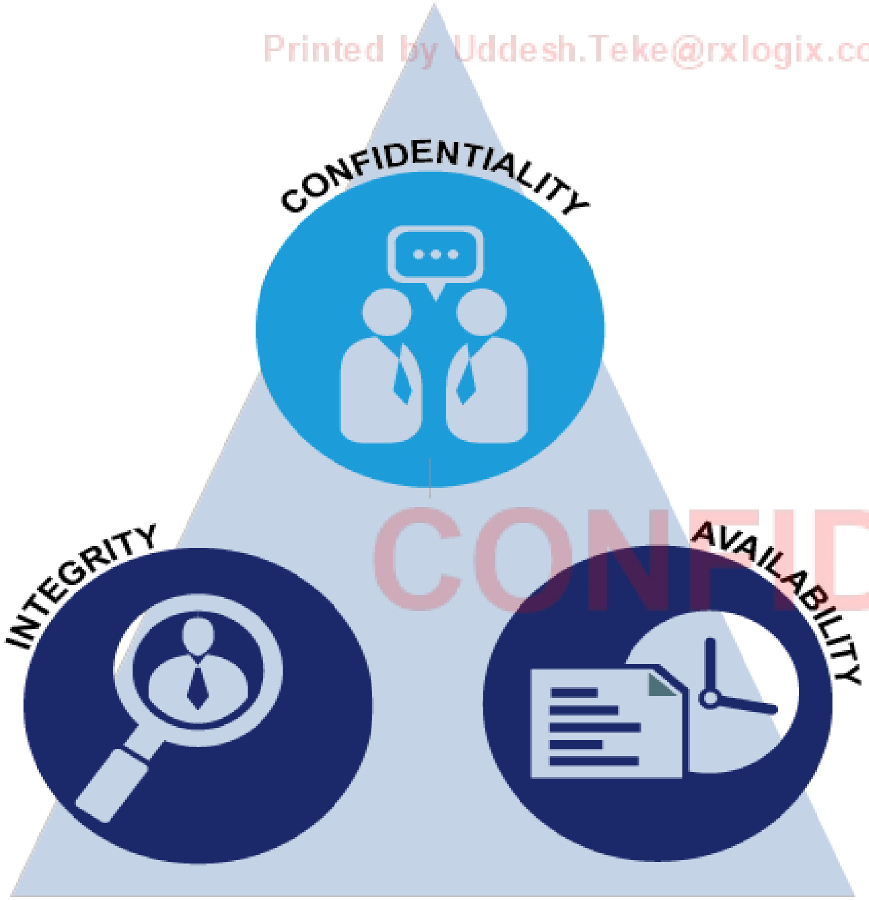
- Direct and indirect financial loss
- Damage to Reputation
- Loss of market and customer confidence
- Disruption in business
- Closure of business

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Information Security Framework (CIA Triad)

The 3 Pillars of Information Security:



1) **Confidentiality** : Information keep private and secure.

2) **Integrity:** assurance that the Information is trustworthy and accurate and not be altered from its original state.

3) **Availability:** ensuring that authorized users have access to information and associated assets when required.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Vulnerability, Threat and Risk

Vulnerability	Threat	Risk
Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset	Any activity that can exploit a vulnerability, intentionally or accidentally, and damage or destroy an asset.	The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

Printed by Uddesh Teke@rxlogix.com on 29 Jan 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Vulnerability, Threat and Risk (Cont…)

- Risk = Vulnerability (V)* Threat (T)

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

How to reduce IT Risk ?

- Conduct the RA (Risk Assessment)
- Risk Treatment Plan (RTP)
- Vulnerability assessment and Penetration testing.
- User Awareness
- Track the closure of above points

CONFIDENTIAL

Vulnerability, Threat and Risk Example

Identity and access management in AWS cloud:

- **Vulnerability:**

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

-Multifactor authentication (MFA) not implemented.

-User access and rights are not validate on regular basis.

- **Threat :**

-Password may be leaked, compromised.

-User can take advantage of Unvalidated access.

- **Risk:**

CONFIDENTIAL

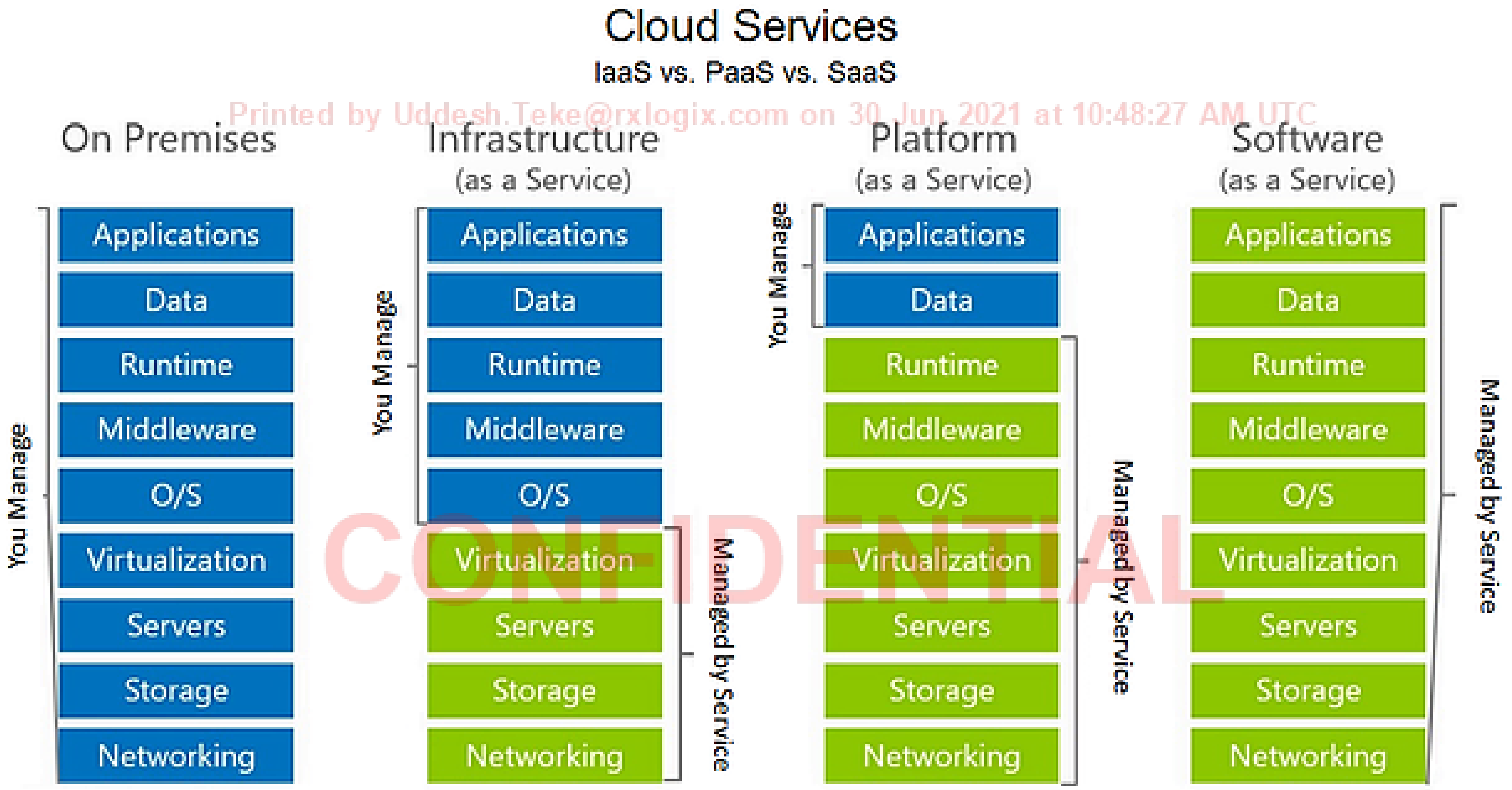
- Attacker may gain unauthorized access of cloud instance.

-Loss of Data.

-Business reputation and Legal Penalties

Cloud computing Model

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC



Cloud Services

IaaS vs. PaaS vs. SaaS

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

CONFIDENTIAL

Data Classification

Data Classification	Definition	Protection Requirements	Confidentiality Impact Level
Restricted	Confidential information requiring the highest level of security and privacy protection. Access must restricted to authorized personnel only.	Encryption of data at Rest and transmission as per data type requirement and secure storage. Access Authorization required Circulation is limited - may not be copied outside of designated systems.	High
Confidential	Less sensitive than restricted data but still needs protection from unauthorized access.	Access Authorization required Circulation is limited - may not be copied outside of designated systems. Encryption of data at Rest and transmission as per data type requirement and secure storage.	High
Internal	Confidential RxLogix information requiring security and privacy protection. Information may be shared internally with RxLogix employees.	Encryption of data at Rest and transmission as per data type requirement and secure storage. Access Authorization required	Moderate
Public	Information may be published and shared freely.	None	Low

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:40:27 AM UTC

CONFIDENTIAL

Confidentiality Impact Levels

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

Impact Level	Definition
High	The unauthorized disclosure of information would have severe adverse effect on client and/or RxLogix
Moderate	The unauthorized disclosure of information would have moderate adverse effect on RxLogix.
Public	No impact.

CONFIDENTIAL

Data Types Examples

Data Type	Data Classification
Personal Data, or data containing Personally Identifiable Information (PII) or Protected Health Information (PHI)	Restricted
Drug Safety System Database	Restricted
RxLogix product source code	Restricted
Contractual Non-Disclosure Documents	Restricted
SOP and Policy documents, internal department Reports, Training content.	Confidential
RxLogix Quality Management System	Internal
RxLogix Product documentation such as requirements, designs, mapping documents, and validation packages	Internal
Press Releases and Information on Website	Public

Printed by [illegible]@rxlogix.com on [illegible] 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Example of Information Security Threats

- ❖ **Physical Theft of any asset.**

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- ❖ **Technology Failure**

  Hardware, Software and Network Failure.

- ❖ **Social Engineering**

  I. Phishing
  II. Vishing
  III. Smishing
  IV. Tailgating

CONFIDENTIAL

Example of Information Security Threats

❖Logical Theft:

I. Unauthorized Access

II. Stealing password

III. Hacking

IV. Sniffing

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

❖ Data Corruption:

I. Virus Attack

II. Information modification

III. Forgery

IV. Sabotage

V. Fraud

CONFIDENTIAL

Example of Information Security Threats

❖Data/Service Denial:

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

I. Distributed/Denial of Service (DoS)/DDoS attack
II. Business Continuity Risk

❖Calamity or Disaster

I. Natural disaster: Flood, earthquake, hurricane etc.
II. Man Made disaster: fires, terrorist attacks, war etc.

CONFIDENTIAL

Social Engineering : Phishing

- Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords, Bank account and credit card details by fake URL link in e-mail.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- Phishing can also involve sending malicious attachments or website links that may contain malware or payload with these they can infect computers or mobile devices and get remote access of your devices.

- Phishing e-mail may request to transfer funds into bank account for any fake invoice, fees, rental amount or subscription charges for any services.

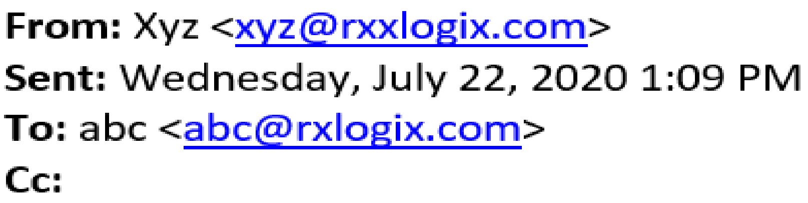
CONFIDENTIAL

Example of Phishing e-mails – looks like similar domain

- **Phishing mail may look with similar name and very little difference in the spelling of email id, Example:**

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

Always check the domain spelling of sender



From: Xyz <xyz@rxxlogix.com>
Sent: Wednesday, July 22, 2020 1:09 PM
To: abc <abc@rxlogix.com>
Cc:

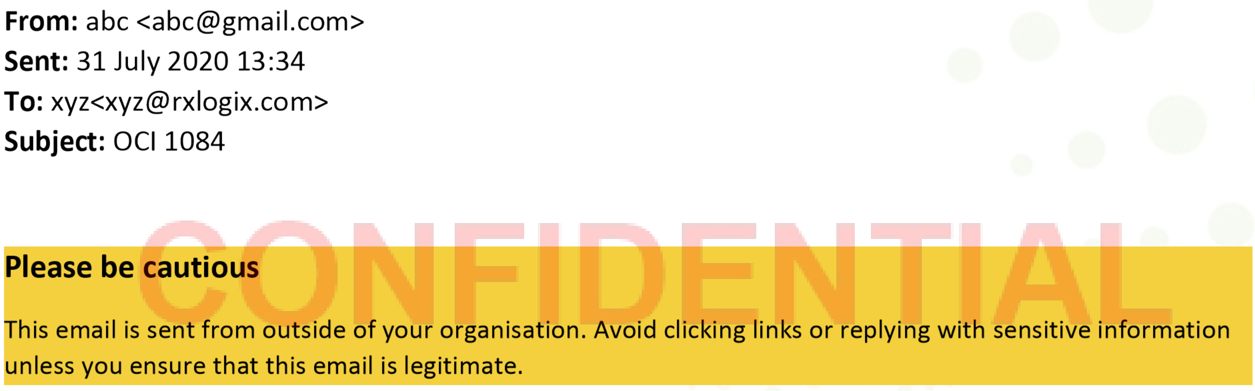
CONFIDENTIAL

Example of Phishing e-mails – **out side e-mail highlighted**

- Be careful, if you received any e-mail from the outside domain of Rxlogix.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- **Out side e-mails will be highlighted in Orange strip, e.g.**



From: abc <abc@gmail.com>
Sent: 31 July 2020 13:34
To: xyz<xyz@rxlogix.com>
Subject: OCI 1084

Please be cautious

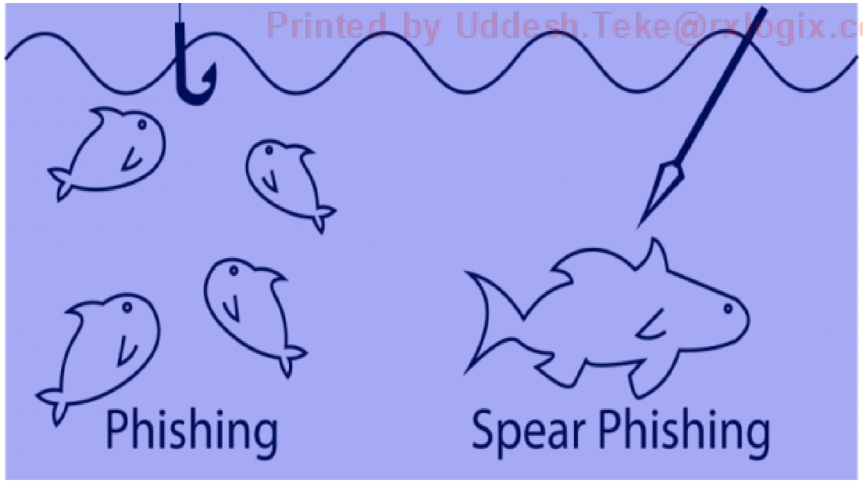
This email is sent from outside of your organisation. Avoid clicking links or replying with sensitive information unless you ensure that this email is legitimate.

CONFIDENTIAL

so verify the sender before opening the email

Spear Phishing

Printed by Uddesh.Teke@rxlogix.com on [illegible] Jun 2021 at [illegible] AM [illegible]



Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

CONFIDENTIAL

Other example of Phishing e-mails

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

1. You have won the lottery, please provide bank details and minimum processing charges.
2. Free Netflix/Amazon prime account for you: Never respond these mail and avoid to get in trap.
3. Direct Job offers from unknown sources
4. Fake bank mails like : upgrade card or account deactivation, they create the urgency to respond the mail.

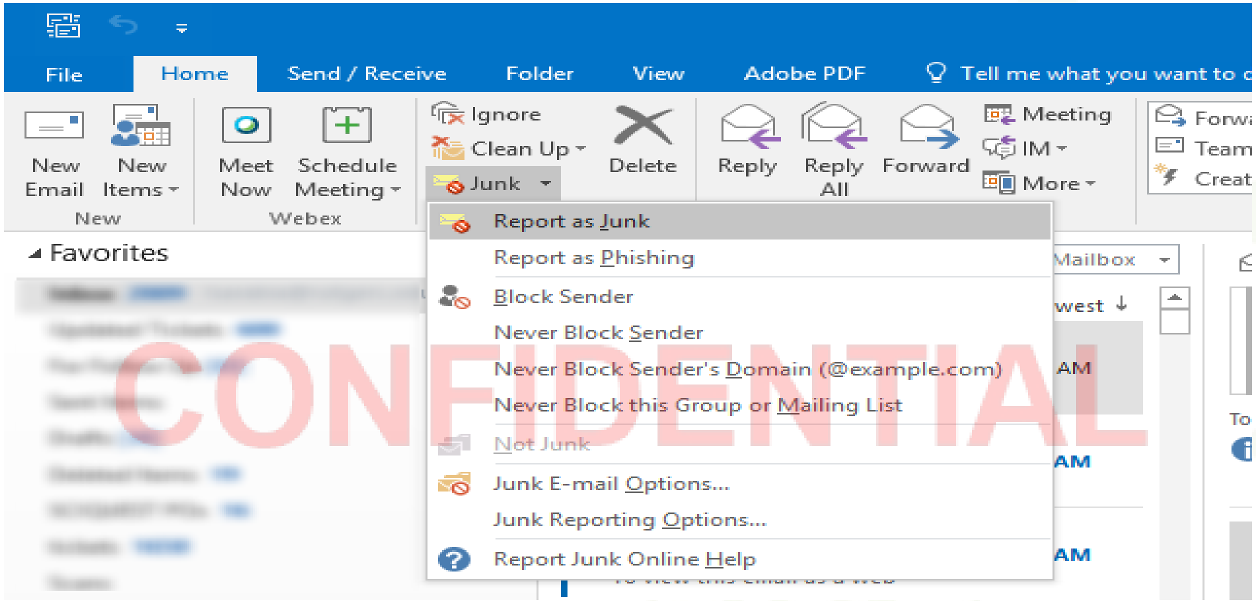
   Your Bank never ask sensitive information like CVV, OTP.
5. Switch your 4G Sim to 5G Sim card free.
6. Password expiry and reset password from smiler domain.
7. Technical support representing like from Microsoft.

CONFIDENTIAL

How to report phishing email on Outlook

Printed by [illegible] AM UTC

1. In the message list, select the message or messages you want to report.
2. Above the reading pane, select **Junk** > **Phishing** > **Report** to report the message sender.



Social Engineering : Vishing (Voice Phishing)

- Vishing is when fraudsters obtain personal details of a victim by phone call

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- Bank fraud vishing scams are some of the most common you'll come across. Scammers will typically pose as a financial institution representative and obtain your bank account and card details e.g. your card going to expire, bank account going to freeze, KYC not updated then they request to share OTP, password.

- Calls in general are far less abundant than email, so there is a higher chance of getting someone's attention.

CONFIDENTIAL

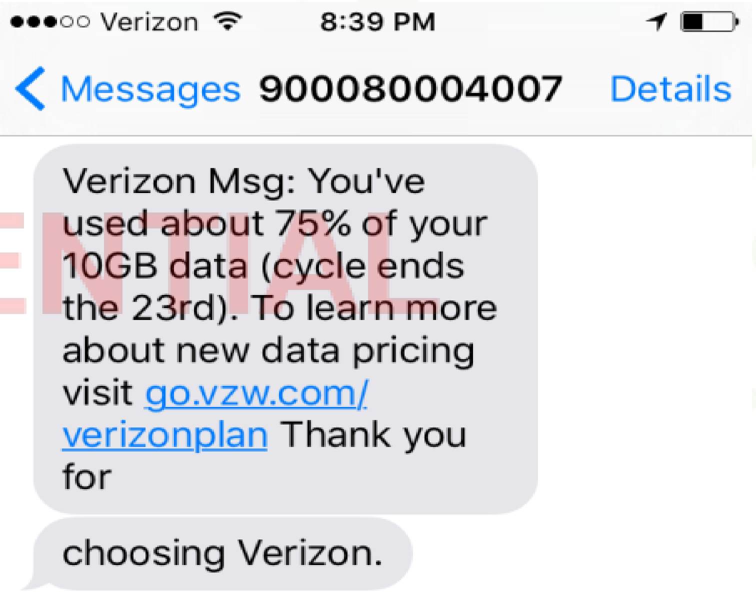
Social Engineering : Smishing (SMS Scam)

- SMS phishing, or “smishing” attack, targets receive a text message that uses a short code. Often, these messages mimic the legitimate ones you might get, e.g., “Free reward points” confirm your bank transaction.” This type of message would include a shortened link.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- Clicking on shortened link lead to a malicious app being installed on your smartphone. Once it’s on there, the malicious app could track your keystrokes, steal your identity, or encrypt the files on your phone and hold them for ransomware.

CONFIDENTIAL



Verizon Msg: You've used about 75% of your 10GB data (cycle ends the 23rd). To learn more about new data pricing visit go.vzw.com/ verizonplan Thank you for

choosing Verizon.

E-mail Security Guidelines:

- **Don’ts**
  - Do not open the mail or attachment which is suspected to be virus or received from an unidentified sender
  - 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 or spamming
  - Do not send chain mails to everyone in office and don’t reply to it
  - Do not send official content on personal email

CONFIDENTIAL

- **Do’s:**
- Use official mail for business purposes only.
- If you come across any junk / spam mail, report to IT Help desk and follow the instructions.
- Always check the @domainname.com of email of email ID.

Password security

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

A password is like a toothbrush

CONFIDENTIAL

Choose a good one

Don't share it with anyone

Change it regularly

Password security

- **Never share** your password to anyone.
- Use strong passwords that are not dictionary words
- Use uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), punctuation marks (!@#$%^&*()_+=-)
- Password should be minimum 12-15 characters long.
- Don't use any personal related information for creating password.
- Never write your password down.
- Do not store your password in a plain text file on your computer.
- Reset your password on Regularly basis.
- Don't reuse passwords.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Internet Security

- Do not download anything unless you have the authorization to do so.
- Never give out own or other's personal information and passwords.
- Be careful with the information that you share online.
- Don't open, forward, reply to, or click any links or attachments in unsolicited emails that you don't know who sent them.
- Be cautions when installing screen savers, games or programs from various internet sources.
- Don't post company or proprietary information on public discussion forums.
- Don't connect your Laptop/Mobile to free public Wi-Fi.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Desktop and Laptop Computer Security

- Use of company provided assets restricted to official purpose only.
- Do not use personal laptop/desktop to perform official work
- **Use of personal pen drives and laptops is restricted inside office premises.**
- Incase of any theft or loss of assets please inform to your Immediate manager, respective HOD's, Admin Team & IT Team.
- Only use authorized software for official purpose, Do not download freeware or open source software without approval from Infosec team
- Uninstall programs that are not used or unnecessary.
- **Please keep Windows, macOS, Linux, Antivirus and all software updated.**
- Do not connect Laptop to Public networks such as Airports, Coffee Shops, Train/Metro Stations.
- Never leave laptops unattended in public areas or in a car & Beware of shoulder surfing.
- NEVER give your password to anyone, even the help desk.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Physical Security

- Never enter the area where you do not have access and ensure nobody tailgates and Most of the visitors should be entertained outside the restricted area.
- Always wear your official ID card.
- Escort visitors and question strangers
- Visitor should sign the entry register (Entry and exit both) if requires access to production area.
- Visitor should declare the Laptops/Tablets/removable media etc.. carried by them at reception desk.
- Keep your Desk neat and clean.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:46:27 AM UTC

CONFIDENTIAL

Clean Desk Policy

- Employees are required to ensure that all Restricted and Internal information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations screens must be locked when workspace is unoccupied.
- Portable computers must be protected by full disk encryption utilizing FIPS 140-2 compliant encryption.
- Any Restricted or Internal information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Internal information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Internal information must not be left at an unattended desk.

Printed by [illegible]@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Clean Desk Policy cont…

- Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Internal information must be immediately removed from the printer.
- Sharing of Restricted or Internal information with unauthorized parties is forbidden.
- Upon disposal, Restricted and Internal documents must be shredded in the official shredder bins or placed in lock confidential disposal bins.
- Whiteboards containing Restricted information must be erased.
- When not in use lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Incident Management and Reporting

All employees will report any incident which is a violation of security policies and best security practices.

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- Types of Incidents
  - Power Malfunctions (Power spikes, short circuits etc.)
  - Denial of Service (DOS)
  - Malicious Code
  - Unauthorized Access
  - Inappropriate Usage
  - Failure / crash of IT equipment
  - Observed unusual conditions viz. sparking, smoke
  - Hardware resources and components lost / stolen
  - Hardware, Software, and Operational errors that result in erroneous data.

CONFIDENTIAL

Incident Response: What you can do?

- Please report the Incident/phishing e-mails or suspicious activity to your immediate supervisor and IT Team.

- To report any Incident/phishing/internet fraud, you can also e-mail to :

si@rxlogix.com

CONFIDENTIAL

Quick summary for Employees Responsibility

“Do”

- ✓ Use strong passwords and do not share them
- ✓ Follow clear desk and clear screen policy (Alt + Ctrl + Del)
- ✓ Always keep lockers / drawers locked when unattended
- ✓ Shred Confidential documents yourself
- ✓ Ensure physical security of information assets.
- ✓ Escort visitors and question strangers
- ✓ Participate in all safety and security drills
- ✓ Ensure backup of information
- ✓ Incidence Response – Suspicious Activities should be reported.
- ✓ Details should be shared with others on need to know basis.

Printed by uddesh.reke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Quick summary for Employees Responsibility

“Don’t”

- ✘ Do not discuss critical / confidential information in public

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

- ✘ Do not send confidential documents on email without password protection or encryption.
- ✘ Do not appreciate unsolicited calls seeking confidential information
- ✘ Do not install personalized software and Games
- ✘ Do not reuse obsolete hard copies of confidential information in printers/photocopiers
- ✘ Do not carry any process related documents outside the office
- ✘ Do not tailgate
- ✘ Do not disclose / give out your password
- ✘ Do not try to investigate incidents on your own.

CONFIDENTIAL

Any Questions ?

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

CONFIDENTIAL

Printed by Uddesh.Teke@rxlogix.com on 30 Jun 2021 at 10:48:27 AM UTC

You are our last line of defence,

Your cooperation with IT Team is highly appreciated.

Security is everyone's responsibility

CONFIDENTIAL

THANK YOU..!!

REVISION HISTORY

Version 01 Effective on 23-Oct-2020

1.0

DOCUMENT ELECTRONIC SIGNATURES

DOCUMENT APPROVAL WORKFLOW

Author Approval

Shiv Kant Sharma
Senior Engineer – IT Security
Shivkant.Sharma@rxlogix.com

I am the author of this document.
Signed 5:59:51 AM UTC 09-Oct-2020

Required Workflow Steps for this Category

Shiv Kant Sharma
Senior Engineer – IT Security
Shivkant.Sharma@rxlogix.com

RxLOGIX / Author
I am the author of this document.
Signed 6:05:43 AM UTC 09-Oct-2020

Rajesh Mishra
Associate Director-IT
Rajesh.Mishra@rxlogix.com

RxLOGIX / Approver
I have reviewed and approve this document.
Signed 9:39:57 AM UTC 09-Oct-2020

Jayashree Acharya
Director
Jayashree.Acharya@rxlogix.com

RxLOGIX / Approver
I have reviewed and approve this document.
Signed 10:02:46 AM UTC 09-Oct-2020