SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

The Rise of Cyber Frauds:

How to Secure Small Businesses in the New Normal

SEQRITE

Enterprise Cybersecurity Solutions by Quick Heal

MEET THE EXPERT

Mr. Sanjay Katkar

Joint MD & CTO
Quick Heal
Technologies Limited

Agenda

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

01 **The “New Normal” for the businesses to adapt, survive and thrive.**

02 **The Rising Cyber Risks**

- Attack Surface: The new targets and opportunities for cyber criminals.
- Attack Vectors: New wine in old bottle
- Challenges, Risks and Threats posed by remote working tools.
- The era of Cognitive Threats.

03 **Security considerations for remote workforce**

- Security Posture and the Blind spots: Finding weaknesses before attackers do.
- The changing rules of the game for IT Teams.
- Defence-in-Depth Strategy
- Cyber Hygiene: Educating the remote workforce

04 **Cyber Resilience**

05 **Q & A**

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

The “**New Normal**”
for the businesses to
adapt, survive and thrive.

The “New Normal”

The rules have changed - Eliminate old ways of doing things

Virtual Communication

Reimagine business model

Ability to adapt to changing circumstances

A forceful Tectonic-shift to go Digital

Accelerate adoption of Advanced Technologies

Remote Working

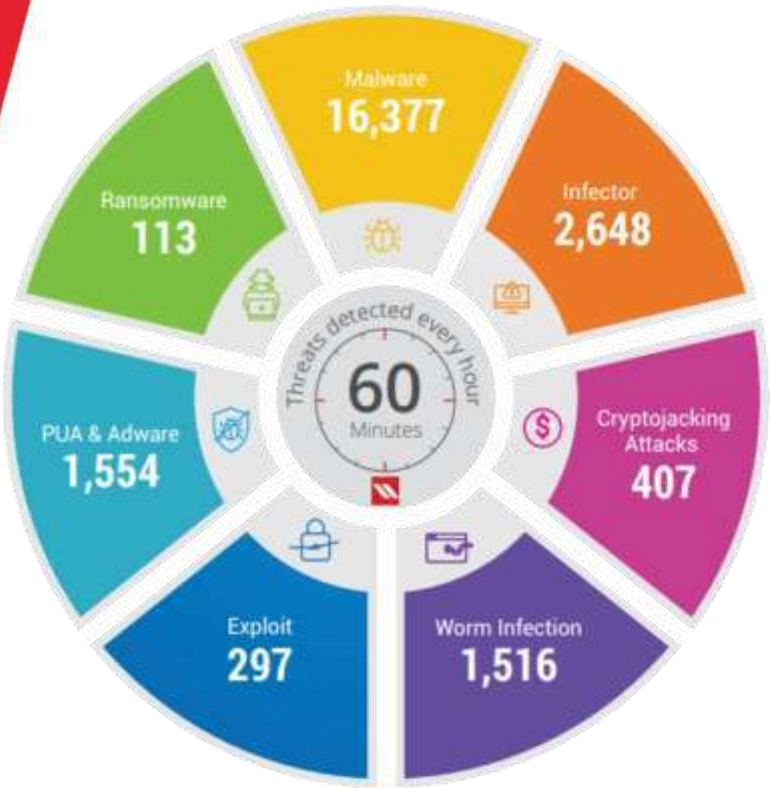
Health Focus

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

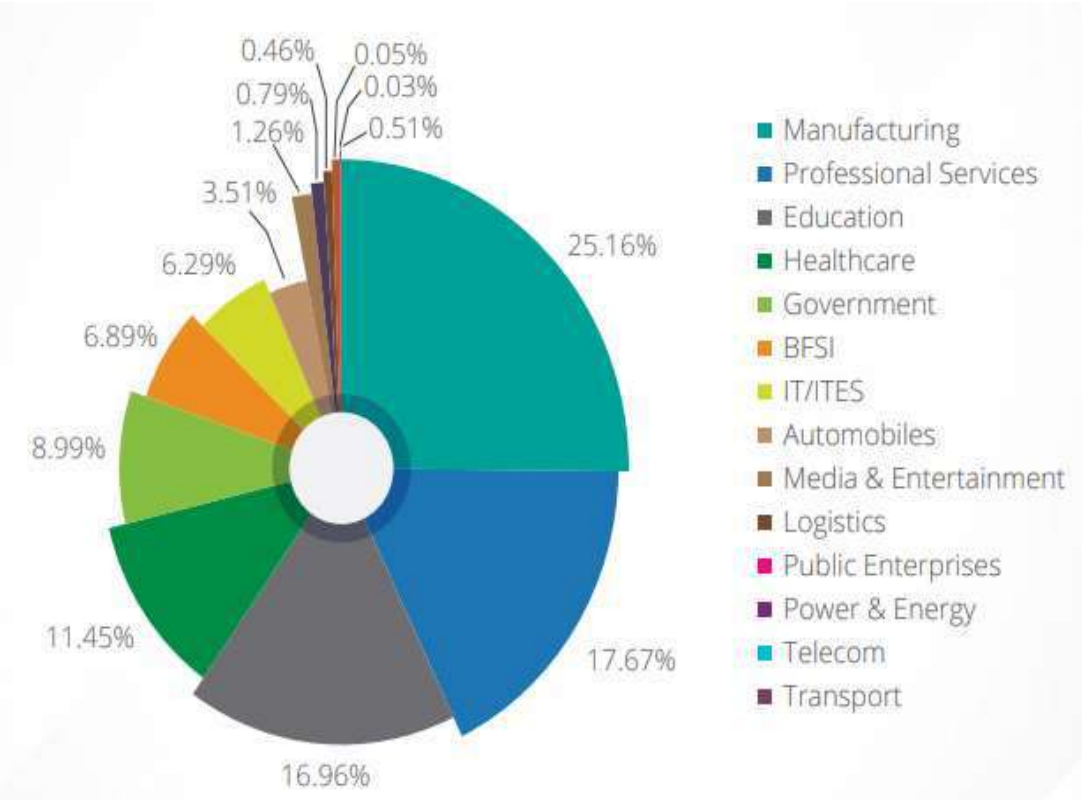
The Rising **Cyber Risks**

The Rising Cyber Attacks

SEQRITE THREAT REPORT Q1 2020



Industry wise Detection Stats



At 25%, the manufacturing industry had the maximum malware detections in Q1 2020.

Attack Surface:
The new targets and opportunities for cyber criminals

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

What is an Attack Surface?

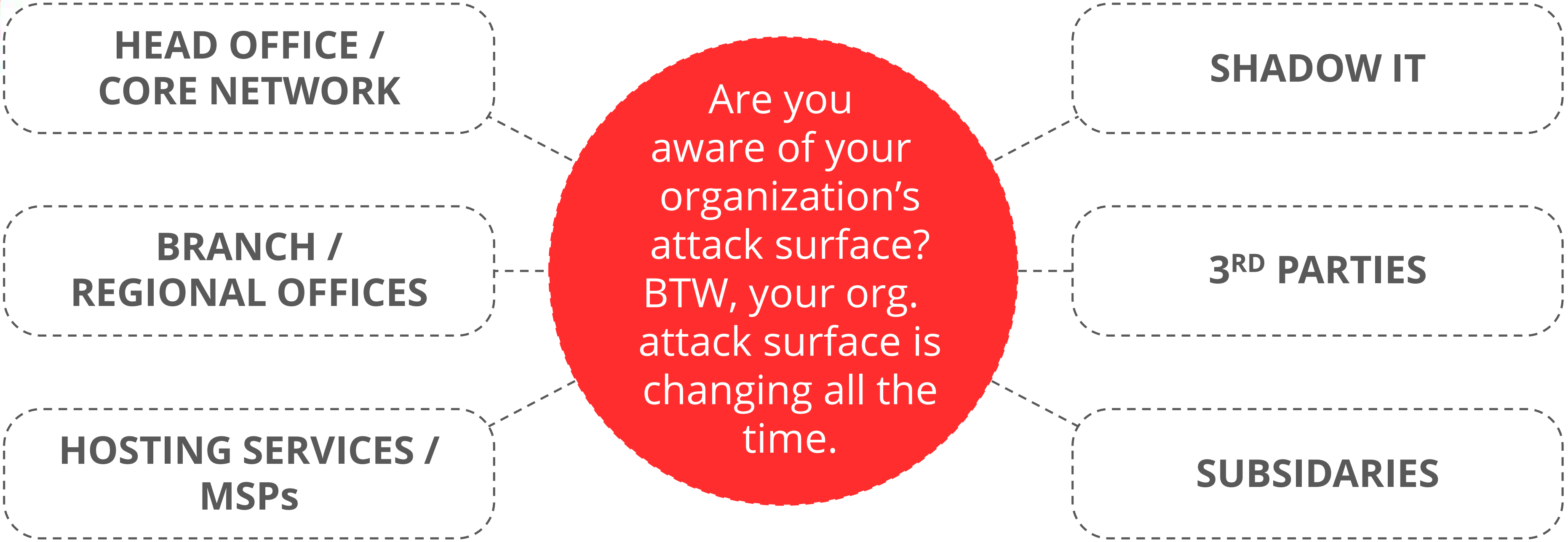
An Attack Surface is conventionally defined as the sum of all "attack vectors" – i.e. the first way an attacker gains access – across your network.

An aggregate of all known, unknown, and potential vulnerabilities, and controls across all hardware, software, and network components.

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Attack Surface:
The new targets and opportunities for cyber criminals

Your attack surface comprises of public-facing exposures and misconfigurations i.e. your DIGITAL EDGE.



Are you aware of your organization’s attack surface? BTW, your org. attack surface is changing all the time.

HEAD OFFICE / CORE NETWORK

BRANCH / REGIONAL OFFICES

HOSTING SERVICES / MSPs

SHADOW IT

3RD PARTIES

SUBSIDARIES

Attack Vectors:

New Wine in Old Bottle

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Wi-Fi Routers

Personal Devices

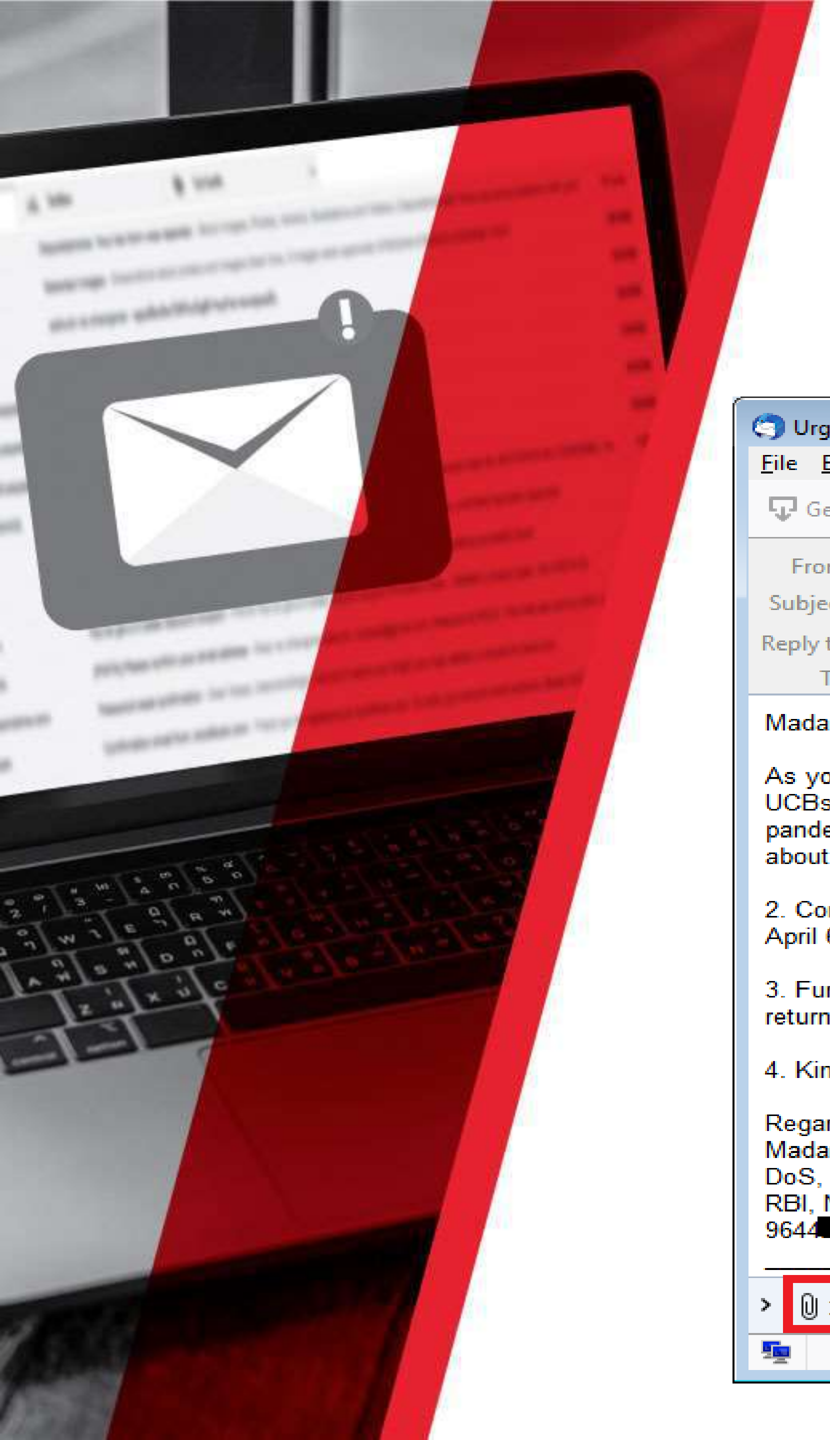
Collaboration Tools

Remote Support

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

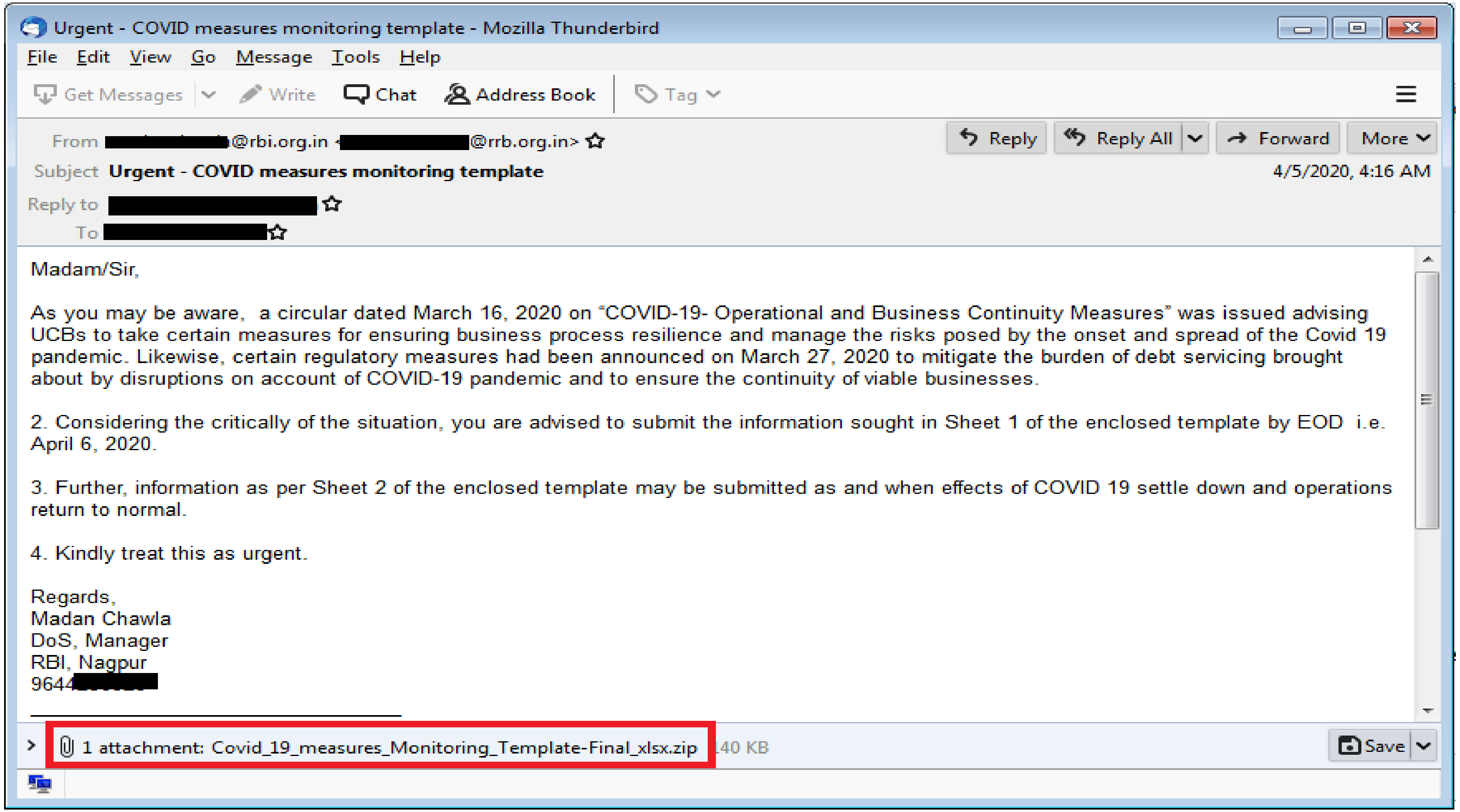
Security risks in COVID-19 situation

- Business email compromise attacks using COVID-19 as phishing bait.
- Malware distribution using COVID-19 as bait
- Remote working and supply chain threats
- More vulnerable systems as lack of awareness



Email Attachments | Guard Against Spear phishing attacks | Sample 1

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal


Urgent - COVID measures monitoring template - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Save

From [redacted]@rbi.org.in <[redacted]@rrb.org.in> ☆
Subject **Urgent - COVID measures monitoring template**
4/5/2020, 4:16 AM
Reply to [redacted] ☆
To [redacted] ☆

Madam/Sir,

As you may be aware, a circular dated March 16, 2020 on "COVID-19- Operational and Business Continuity Measures" was issued advising UCBs to take certain measures for ensuring business process resilience and manage the risks posed by the onset and spread of the Covid 19 pandemic. Likewise, certain regulatory measures had been announced on March 27, 2020 to mitigate the burden of debt servicing brought about by disruptions on account of COVID-19 pandemic and to ensure the continuity of viable businesses.

2. Considering the critically of the situation, you are advised to submit the information sought in Sheet 1 of the enclosed template by EOD i.e. April 6, 2020.

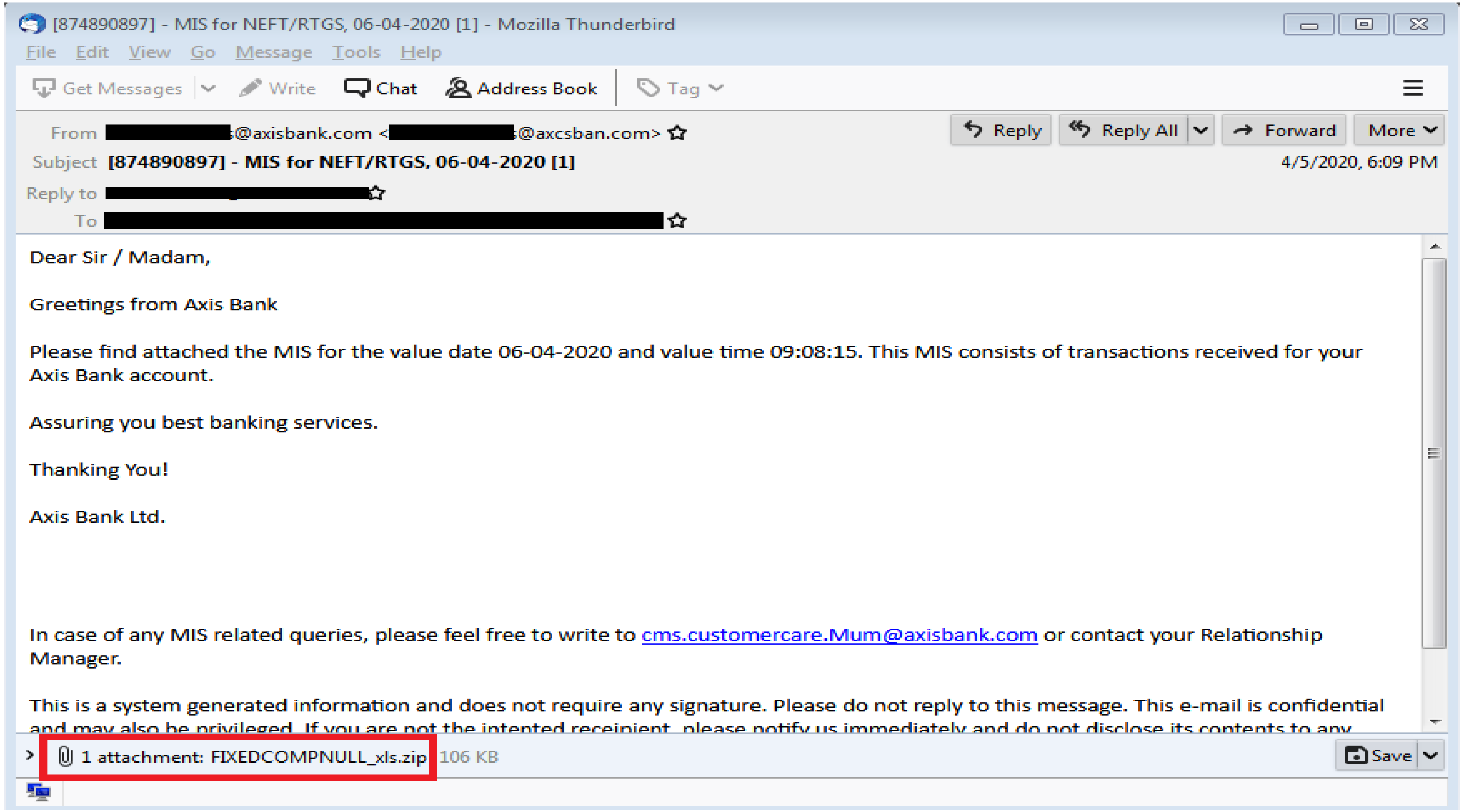
3. Further, information as per Sheet 2 of the enclosed template may be submitted as and when effects of COVID 19 settle down and operations return to normal.

4. Kindly treat this as urgent.

Regards,
Madan Chawla
DoS, Manager
RBI, Nagpur
9644[redacted]

1 attachment: Covid_19_measures_Monitoring_Template-Final_xlsx.zip 40 KB

Email Attachments | Guard Against Spear phishing attacks | Sample 2



From [redacted]@axisbank.com <[redacted]@axcsban.com>

Subject **[874890897] - MIS for NEFT/RTGS, 06-04-2020 [1]**

4/5/2020, 6:09 PM

Reply to [redacted]

To [redacted]

Dear Sir / Madam,

Greetings from Axis Bank

Please find attached the MIS for the value date 06-04-2020 and value time 09:08:15. This MIS consists of transactions received for your Axis Bank account.

Assuring you best banking services.

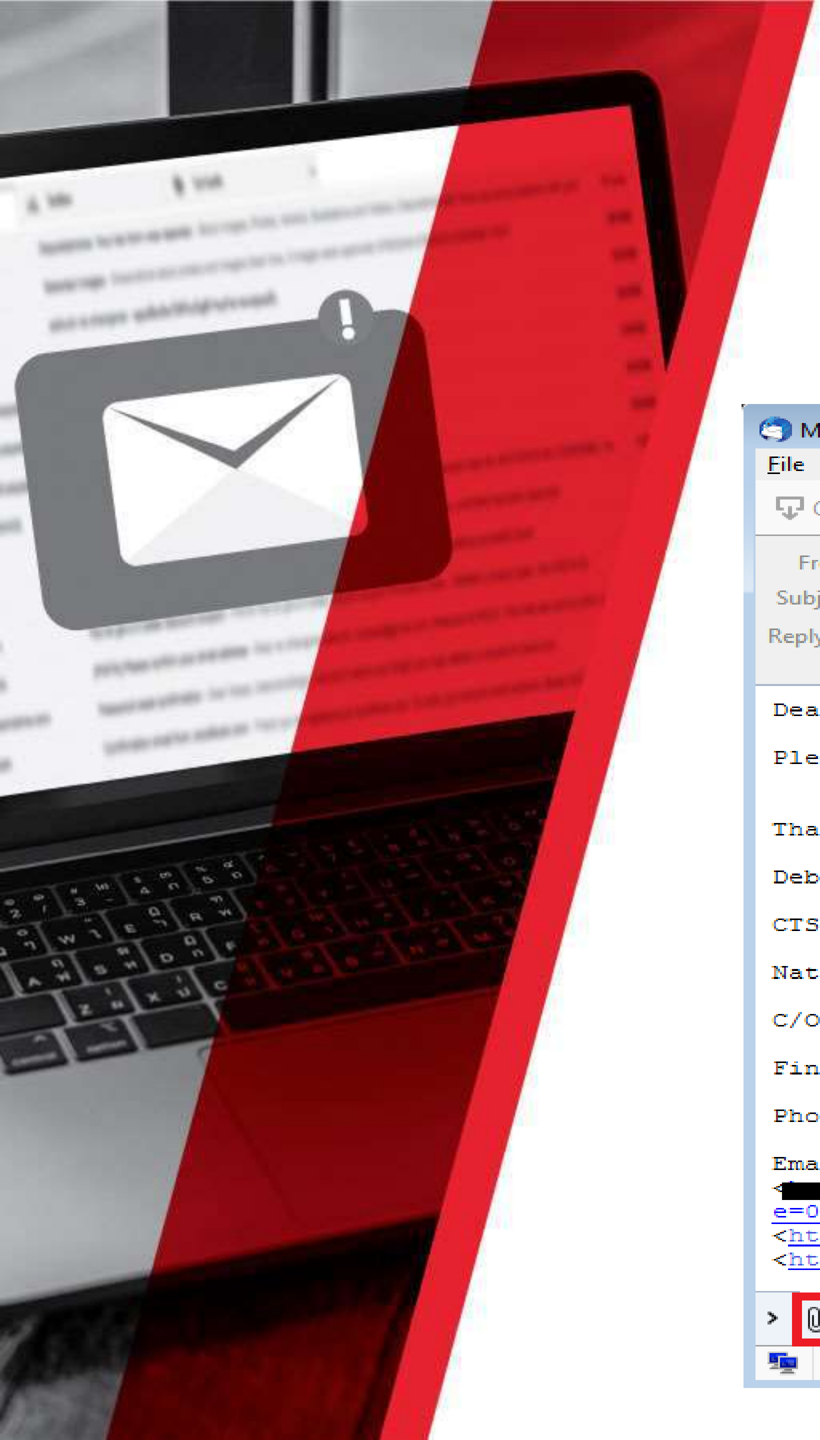
Thanking You!

Axis Bank Ltd.

In case of any MIS related queries, please feel free to write to cms.customercare.Mum@axisbank.com or contact your Relationship Manager.

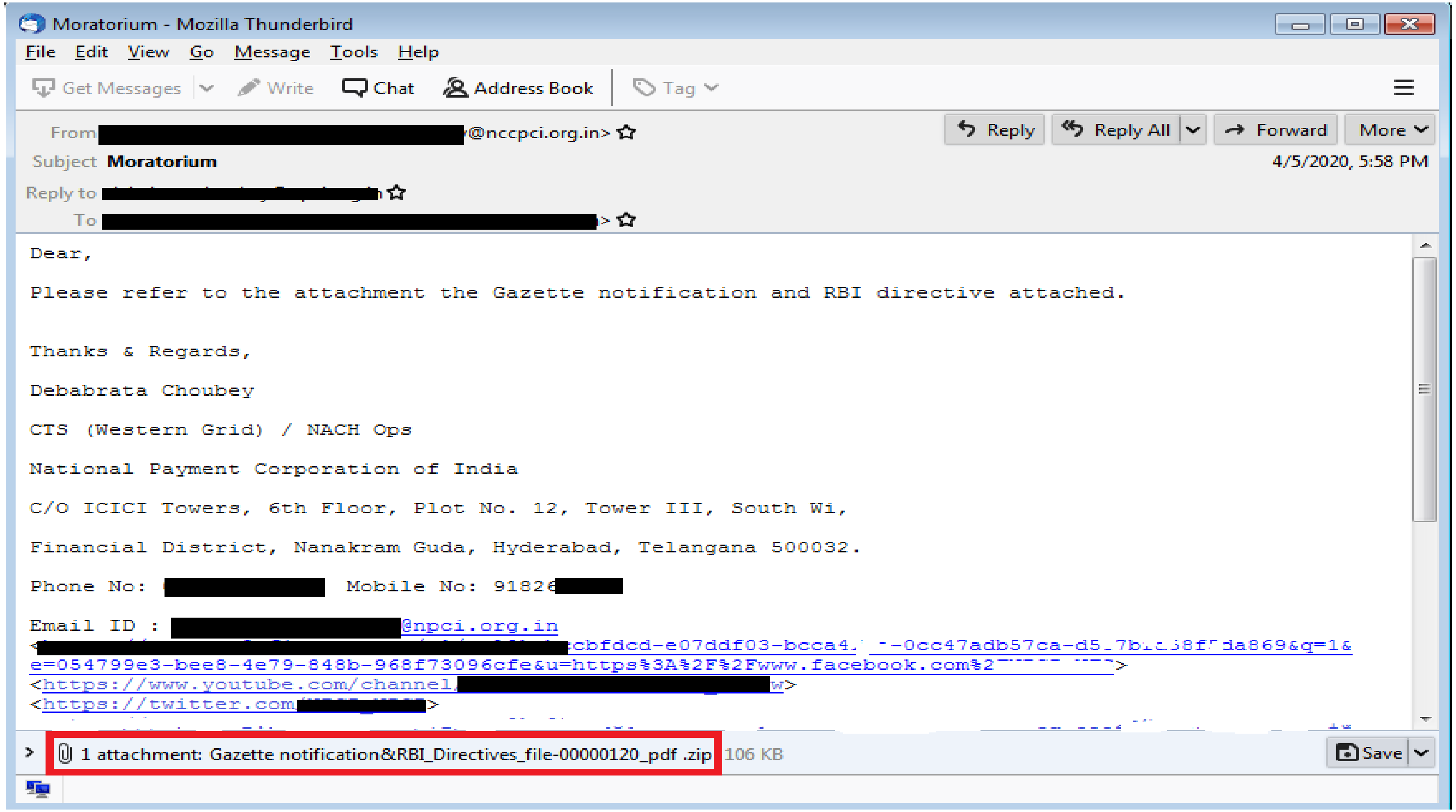
This is a system generated information and does not require any signature. Please do not reply to this message. This e-mail is confidential and may also be privileged. If you are not the intented receipient, please notify us immediately and do not disclose its contents to any

1 attachment: FIXEDCOMPNULL_xls.zip 106 KB



Email Attachments | Guard Against Spear phishing attacks | Sample 3

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal



Moratorium - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Save

From [redacted]@nccpci.org.in>

Subject **Moratorium**

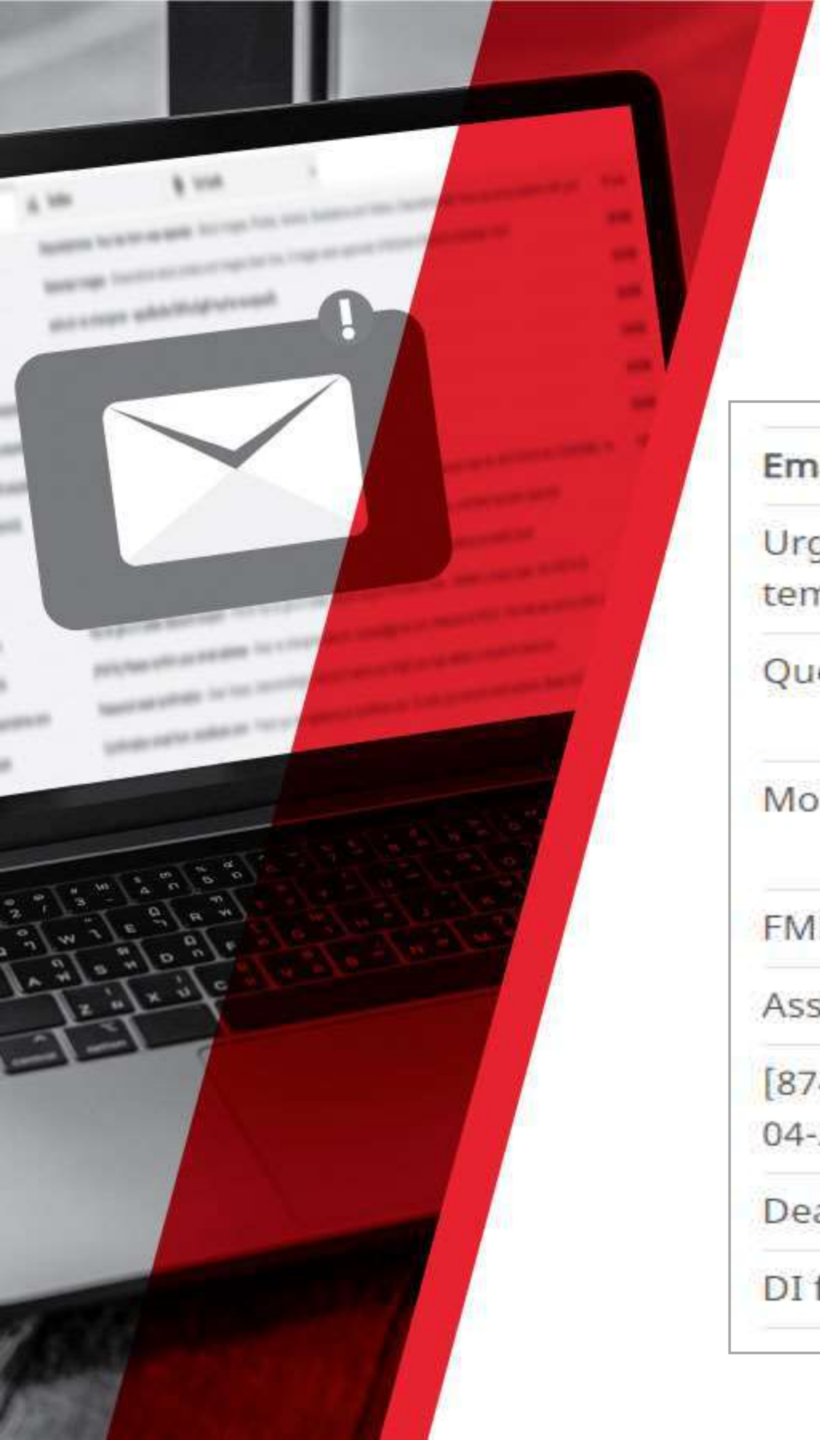
4/5/2020, 5:58 PM

Reply to [redacted]

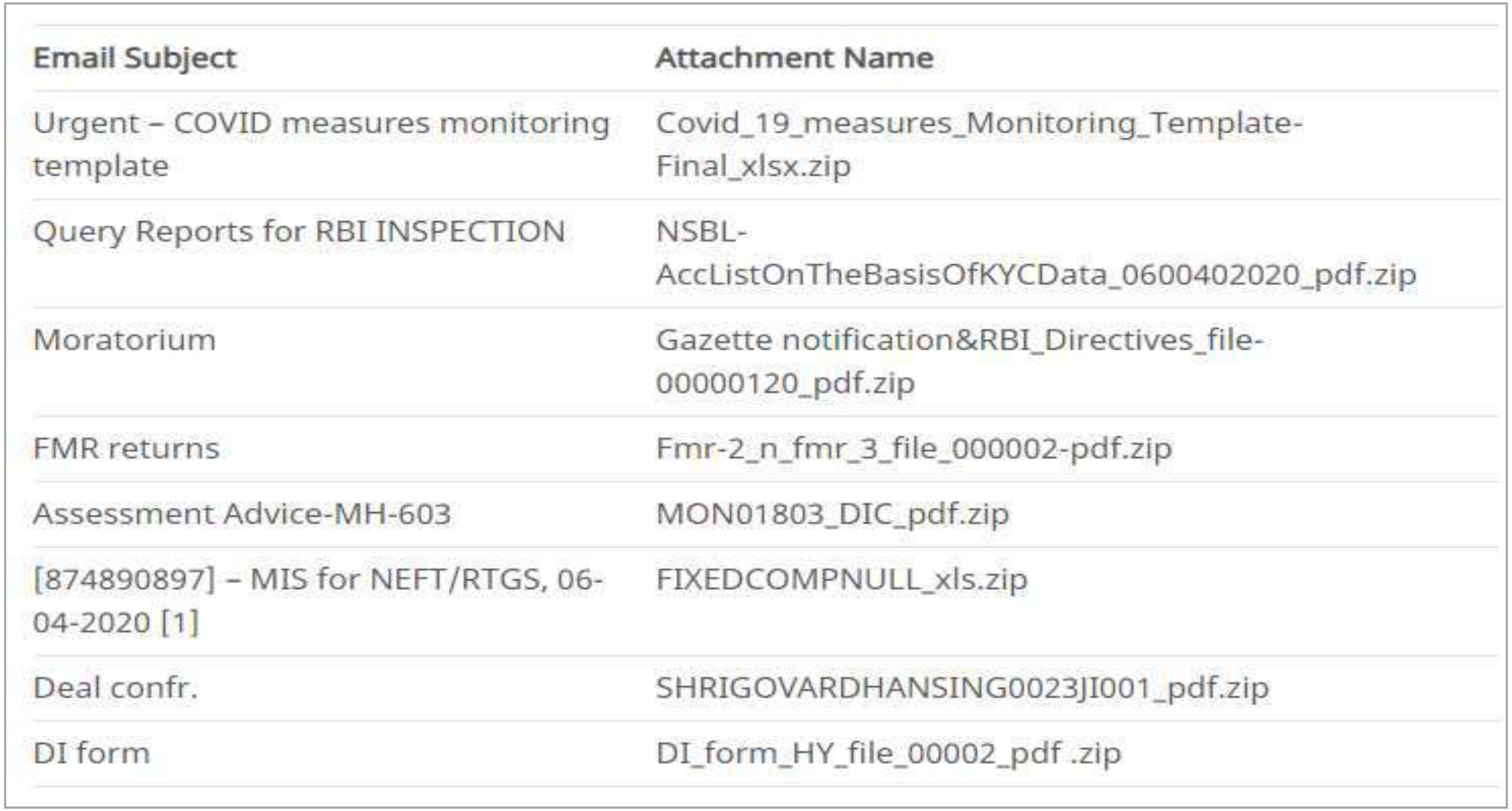
To [redacted]>

```
Dear,

Please refer to the attachment the Gazette notification and RBI directive attached.


Thanks & Regards,

Debabrata Choubey

CTS (Western Grid) / NACH Ops

National Payment Corporation of India

C/O ICICI Towers, 6th Floor, Plot No. 12, Tower III, South Wi,

Financial District, Nanakram Guda, Hyderabad, Telangana 500032.

Phone No: [redacted]  Mobile No: 91826[redacted]

Email ID : [redacted]@npci.org.in
<[redacted]cbfdcd-e07ddf03-bcca4[redacted]-0cc47adb57ca-d5[redacted]da869&q=1&
e=054799e3-bee8-4e79-848b-968f73096cfe&u=https%3A%2F%2Fwww.facebook.com%2[redacted]>
<https://www.youtube.com/channel/[redacted]w>
<https://twitter.com[redacted]>
```

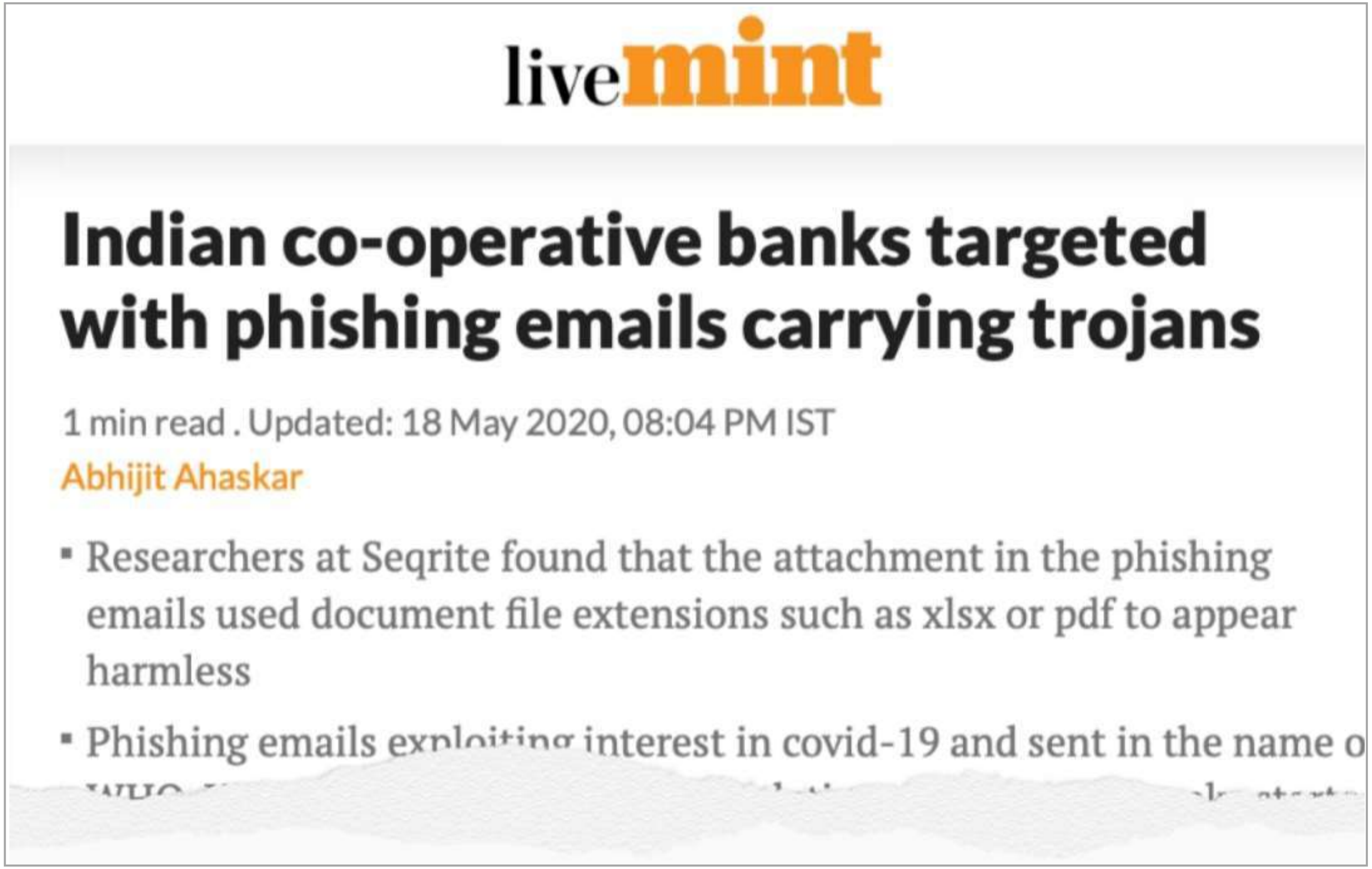
1 attachment: Gazette notification&RBI_Directives_file-00000120_pdf .zip 106 KB



Email Subjects and Attachment Names



Email Subject	Attachment Name
Urgent – COVID measures monitoring template	Covid_19_measures_Monitoring_Template-Final_xlsx.zip
Query Reports for RBI INSPECTION	NSBL-AccListOnTheBasisOfKYCData_0600402020_pdf.zip
Moratorium	Gazette notification&RBI_Directives_file-00000120_pdf.zip
FMR returns	Fmr-2_n_fmr_3_file_000002-pdf.zip
Assessment Advice-MH-603	MON01803_DIC_pdf.zip
[874890897] – MIS for NEFT/RTGS, 06-04-2020 [1]	FIXEDCOMPNULL_xls.zip
Deal confr.	SHRIGOVARDHANSING0023JI001_pdf.zip
DI form	DI_form_HY_file_00002_pdf .zip



livemint

Indian co-operative banks targeted with phishing emails carrying trojans

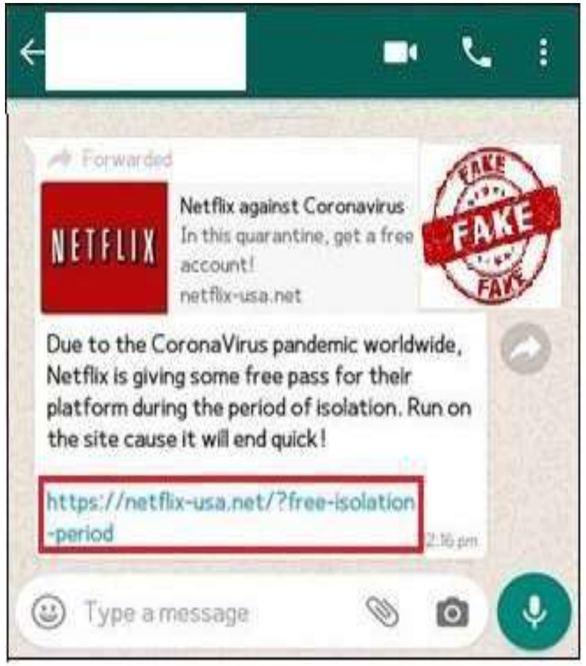
1 min read . Updated: 18 May 2020, 08:04 PM IST

Abhijit Ahaskar

- Researchers at Seqrite found that the attachment in the phishing emails used document file extensions such as xlsx or pdf to appear harmless
- Phishing emails exploiting interest in covid-19 and sent in the name o

Instant Messaging and Payment Apps - **Attack Vectors**

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal



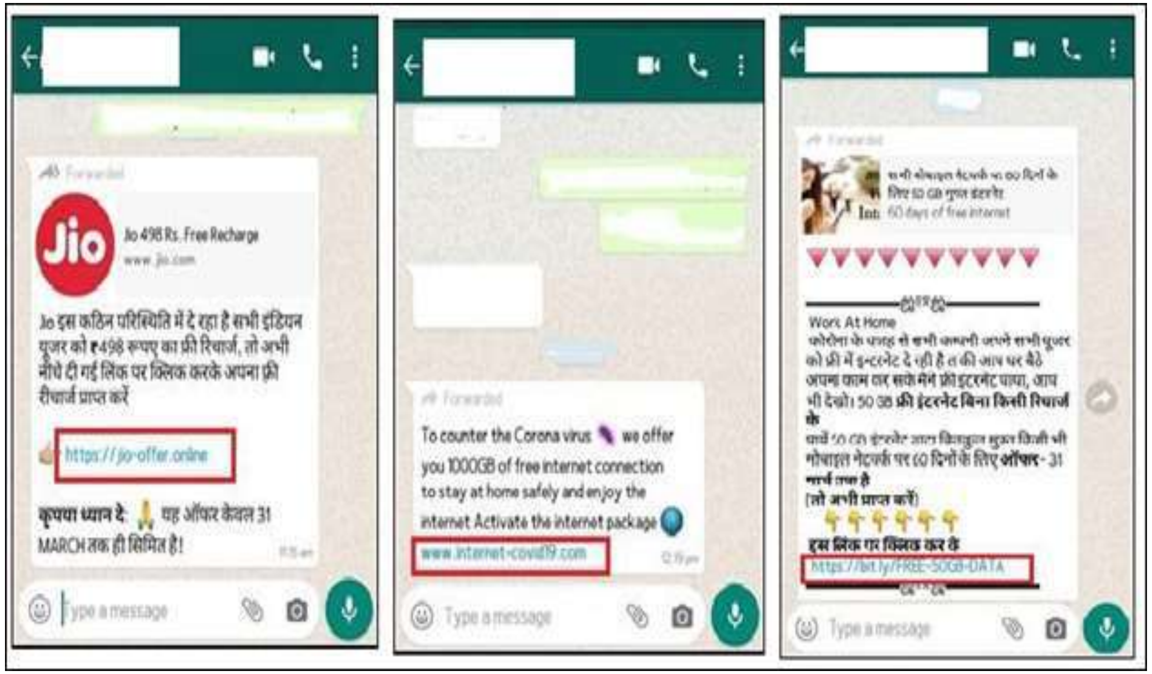
Forwarded

Netflix against Coronavirus
In this quarantine, get a free account!
netflix-usa.net

Due to the CoronaVirus pandemic worldwide, Netflix is giving some free pass for their platform during the period of isolation. Run on the site cause it will end quick!

https://netflix-usa.net/?free-isolation-period

2:16 pm



Forwarded

Jio 498 Rs. Free Recharge
www.jio.com

Jio इस कठिन परिस्थिति में दे रहा है सभी इंडियन यूजर को ₹498 रूपए का फ्री रिचार्ज, तो अभी नीचे दी गई लिंक पर क्लिक करके अपना फ्री रीचार्ज प्राप्त करें

https://jio-offer.online

कृपया ध्यान दे: 🙏 यह ऑफर केवल 31 MARCH तक ही सिमित है!

Forwarded

To counter the Corona virus 🦠 we offer you 1000GB of free internet connection to stay at home safely and enjoy the internet Activate the internet package 🌐

www.internet-covid19.com

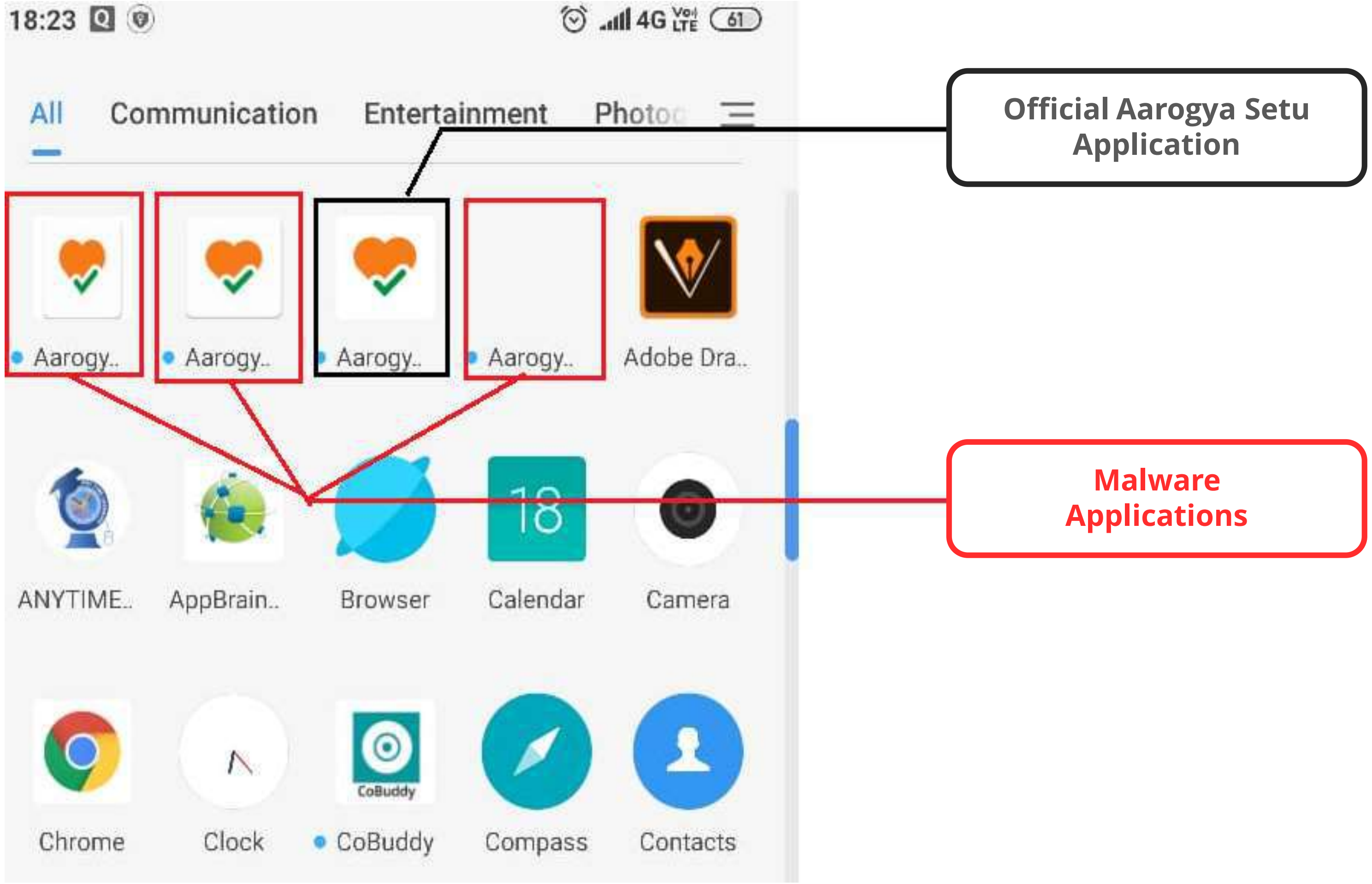
Forwarded

सभी मोबाइल नेटवर्क पर 60 दिनों के लिए 50 GB मुफ्त इंटरनेट
60 days of free internet

🔻🔻🔻🔻🔻🔻🔻🔻🔻🔻

Work At Home
कोरोना के वजह से सभी कम्पनी अपने सभी यूजर को फ्री में इन्टरनेट दे रही है त की आप घर बैठे अपना काम कर सके मैंने फ्री इंटरनेट पाया, आप भी देखो। 50 GB **फ्री इंटरनेट बिना किसी रिचार्ज के**
पायें 50 GB इंटरनेट आज बिलकुल मुफ्त किसी भी मोबाइल नेटवर्क पर 60 दिनों के लिए **ऑफर** - 31 **मार्च तक है**
(तो अभी प्राप्त करें)
👇👇👇👇👇👇
इस लिंक पर क्लिक कर के
https://bit.ly/FREE-50GB-DATA

Fake Aarogya Setu App



Circulated as APKs hosted on different sites, phishing links etc.

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Security considerations for remote workforce

Security Considerations for Remote Workforce

Blind spots: Finding weaknesses before attackers do

- Remote workforce:
  - Personal devices likely to have poor cybersecurity hygiene.
  - Losing visibility of devices and how they are configured, updated, patched and secured.
  - Increased risk of old and insecure personal device accessing your network, the risk of flat mates, partners, or children using corporate devices or seeing/hearing sensitive details goes up if staff don’t have dedicated private workspaces at home.
  - Personal devices and Work devices through same potentially unsecured Wi-Fi Access Point (AP).

Security Considerations for Remote Workforce

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

The changing rules of the game for IT Teams

- Visibility of Real-time inventory - All hardware and software
- Access Control Lists, Privileges, Security Configurations, Certificates, Password Strengths
- Security Patches – All Business and Mission critical Assets
- Control the Remote/WFH Environment
  - Wi-Fi Router Security Settings (WPA2/WPA3, **STRICTLY NO WEP**)
  - Wi-Fi Router Strong Password - Default Credentials "admin/admin" - Potentially inviting trouble
  - Can Disable SSID broadcast
  - Personal Devices – Install latest security updates/patches

Security Considerations for Remote Workforce

The changing rules of the game for IT Teams

- Connectivity to corporate network over VPN
- Define Information Classification and Handling
- Implement Multi-Factor Authentication
- File and disk encryption
- Device Controls
- Password Manager
- Backup – both online and offline
- Turn off your work laptop

Cyber Hygiene: Educating the Remote Workforce

- Cyber Security Risks and Awareness program
- Developing Cyber “instincts”

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Cyber Resilience

Cyber Resilience

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Complete or Absolute security is impossible.

Cyber Resilience is the ability of an organization to relentlessly deliver the defined outcomes despite cyber events. It’s the **ability to prepare, respond, and recover when cyberattacks happen.**

Cyber Resilience – Changing Security Postures

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

Shifts we need to make:

- Reacting to Anticipating.
- Make systems difficult to attack, to minimize impact and potential loss when a cyber attack happens.
- Systems and networks architected to be fault tolerant, redundant

SEQRITE

Enterprise Cybersecurity Solutions by Quick Heal

Thank You

www.seqrite.com