CERT-MU
Computer Emergency Response Team of Mauritius

www.cert-mu.org.mu

The Evolving Cyber Threat Landscape & Data Protection

By Reechaye Sachindra
Information Security Consultant
sreechaye@cert.ncb.mu

NCB
National Computer Board

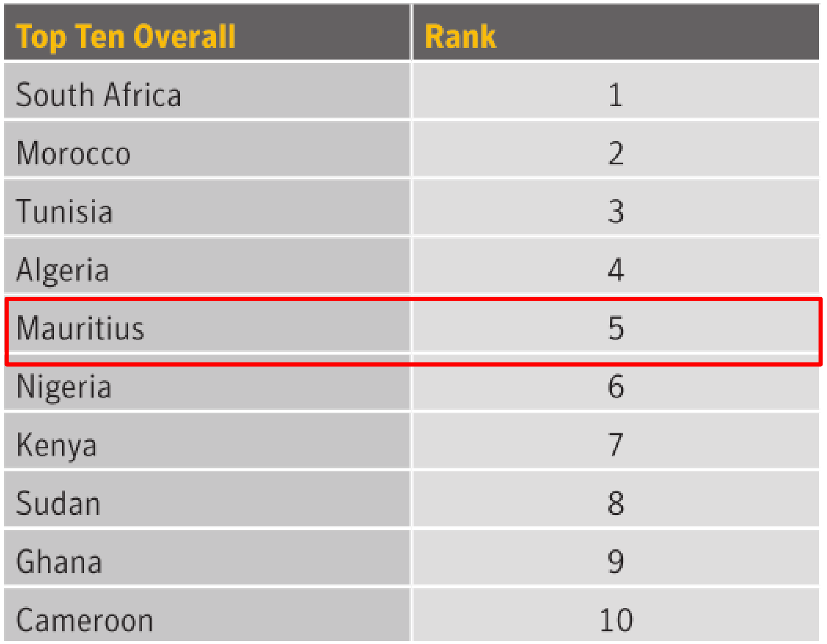
CERT–MU

PASSWORD

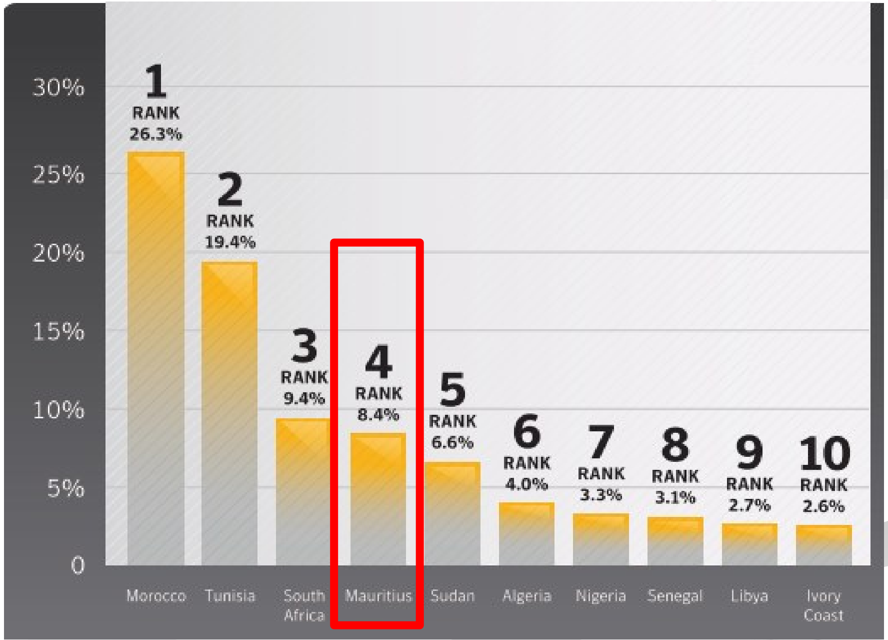
African Statistics on Threat

- Mauritius ranked 5th and is among the top ten countries in the African region that has an Internet Threat profile

- Mauritius ranked 4th and is one among the top ten countries that has spam zombies in the African region



Top Ten Overall	Rank
South Africa	1
Morocco	2
Tunisia	3
Algeria	4
Mauritius	5
Nigeria	6
Kenya	7
Sudan	8
Ghana	9
Cameroon	10



Source: Symantec Corporation - Internet Security Threat Report: Volume 18
South Africa – Current Snapshot, February 28, 2013

Some of the Recent Incidents

- The US government notifies 3,000 companies that they were attacked and charges nation-backed hackers with economic espionage
- Compromises of retailers culminate in a recent breach of 56 million credit cards
- Heartbleed bug results in the loss of 4.5 million healthcare records

Some of the Recent Incidents

- Shellshock bug has compromised millions of devices and cause damage to web servers around the world
- Powerful malware infects hundreds of energy companies worldwide
- More than half of global securities exchanges are hacked
- Regin spy malware has been detected by Symantec which is extremely complex and dangerous

Some of the Recent Incidents..

- Nuclear Power
- Steal Plants
- Solar Power
- ATM Account Thefts
- Stock Exchanges
- Payment Card Accounts
- Theft of email addresses, passwords
- Attacks on government sites (websites defacement)
- Financial companies
- Power Grids
- World most trusted news organizations
- Zero day threats
- Advanced Pertinent Threats

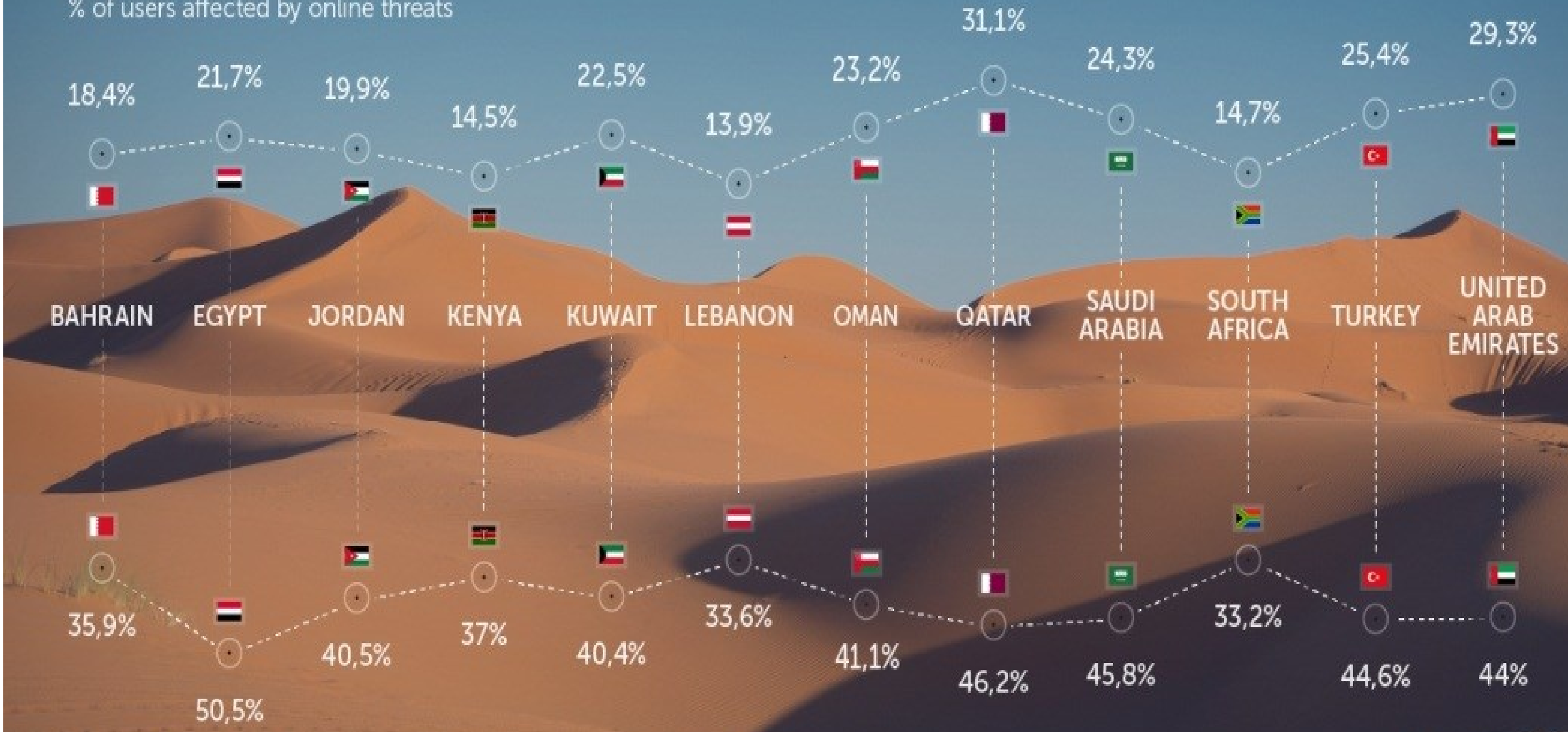
CYBERSECURITY THREAT LANDSCAPE

KASPERSKY lab

In the countries of the Middle East, Turkey and Africa

Online Detections

% of users affected by online threats



Local Detections

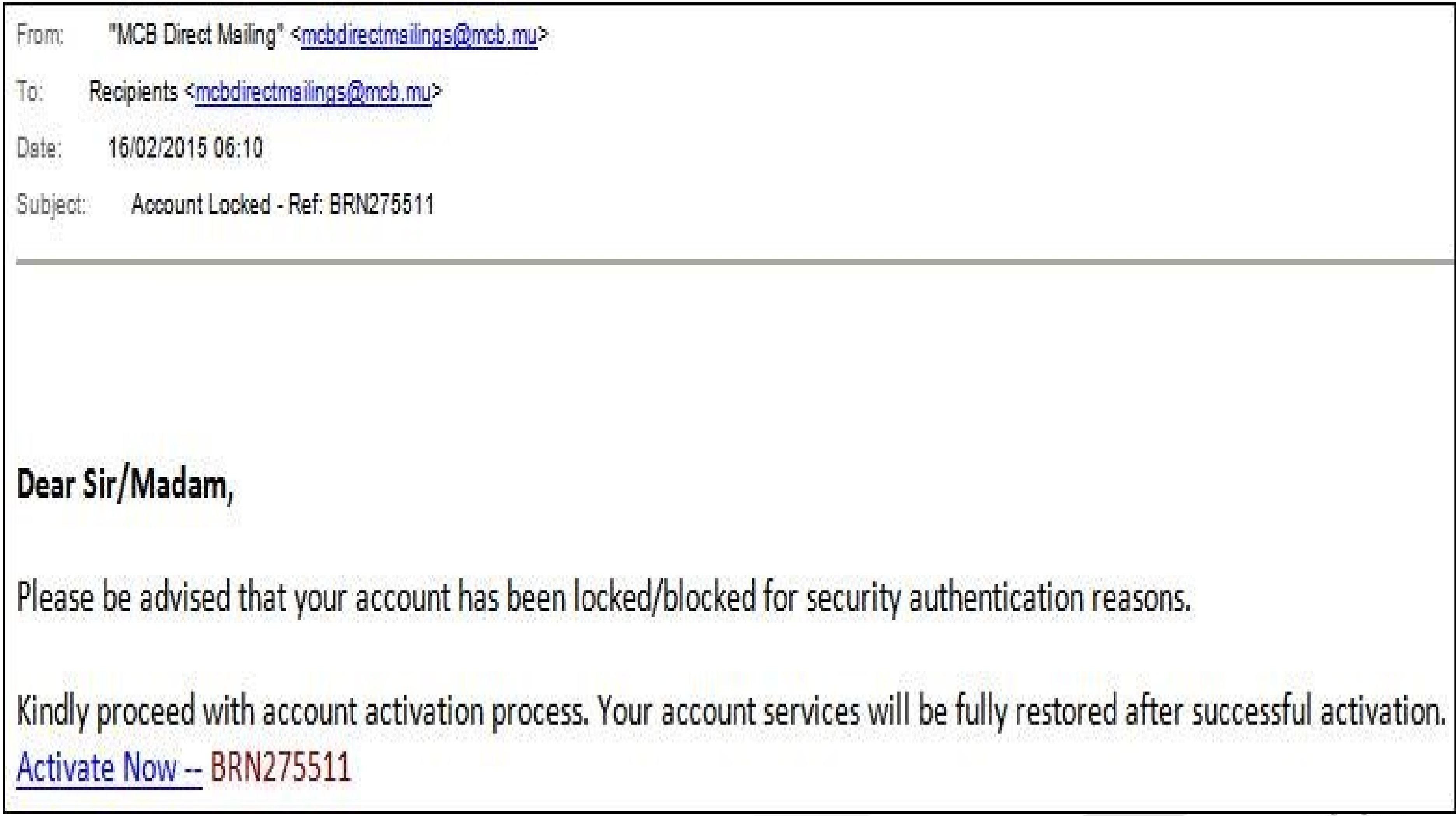
% of users affected by local threats
(malware spread in local networks, by USBs, CDs, DVDs)

*Source: Kaspersky Security Network,
statistics for January-March 2015

Data Threats

- Phishing
- Ransomware
- Identity Theft
- Malware (backdoor trojans)
- Social Engineering
- Insider Threat

Phishing



From: "MCB Direct Mailing" <mcbdirectmailings@mcb.mu>

To: Recipients <mcbdirectmailings@mcb.mu>

Date: 16/02/2015 06:10

Subject: Account Locked - Ref: BRN275511

Dear Sir/Madam,

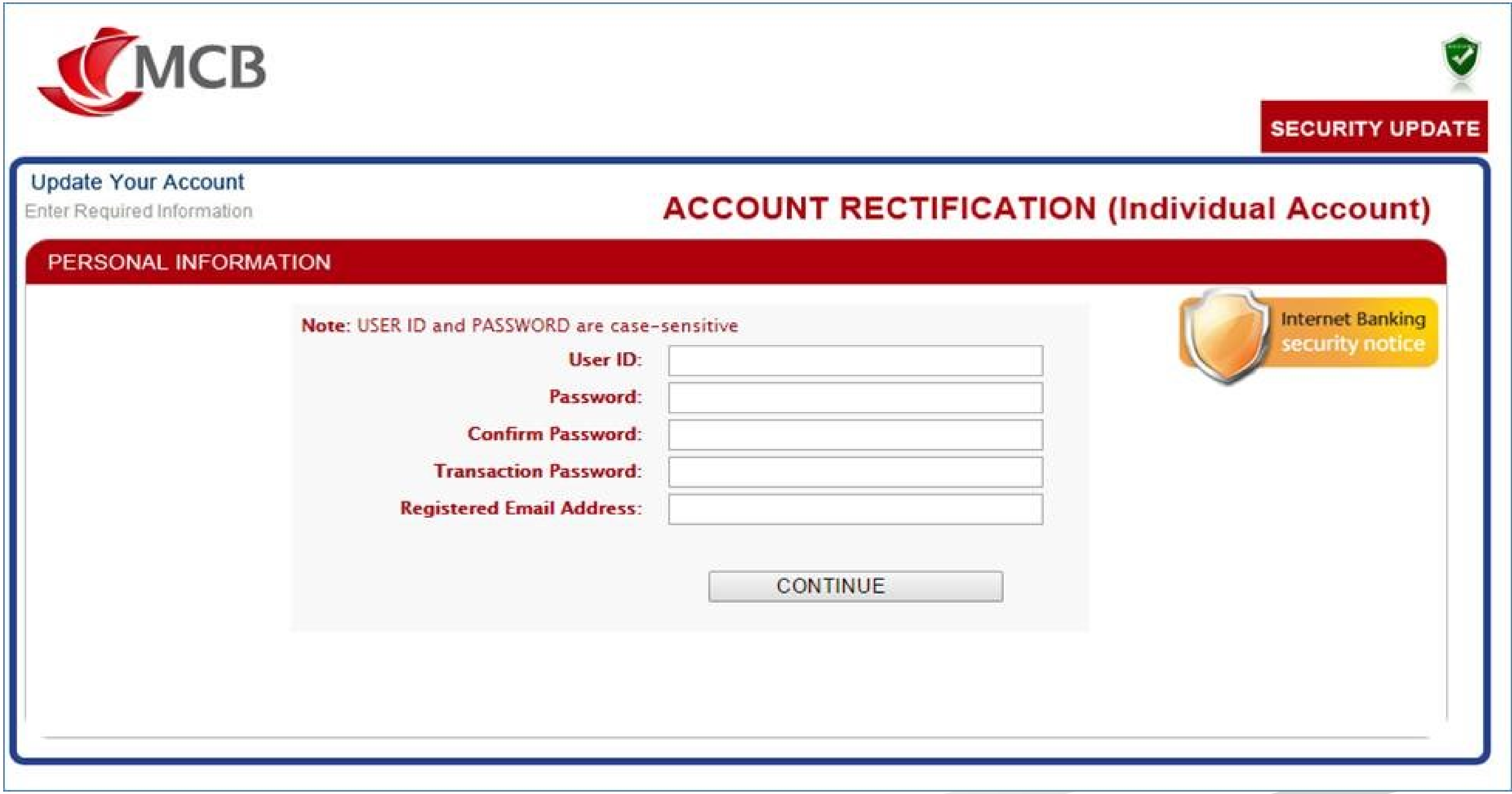
Please be advised that your account has been locked/blocked for security authentication reasons.

Kindly proceed with account activation process. Your account services will be fully restored after successful activation.
Activate Now -- BRN275511

National Computer Board

CERT–MU

Phishing



MCB

SECURITY UPDATE

Update Your Account

Enter Required Information

ACCOUNT RECTIFICATION (Individual Account)

PERSONAL INFORMATION

Note: USER ID and PASSWORD are case-sensitive

User ID:

Password:

Confirm Password:

Transaction Password:

Registered Email Address:

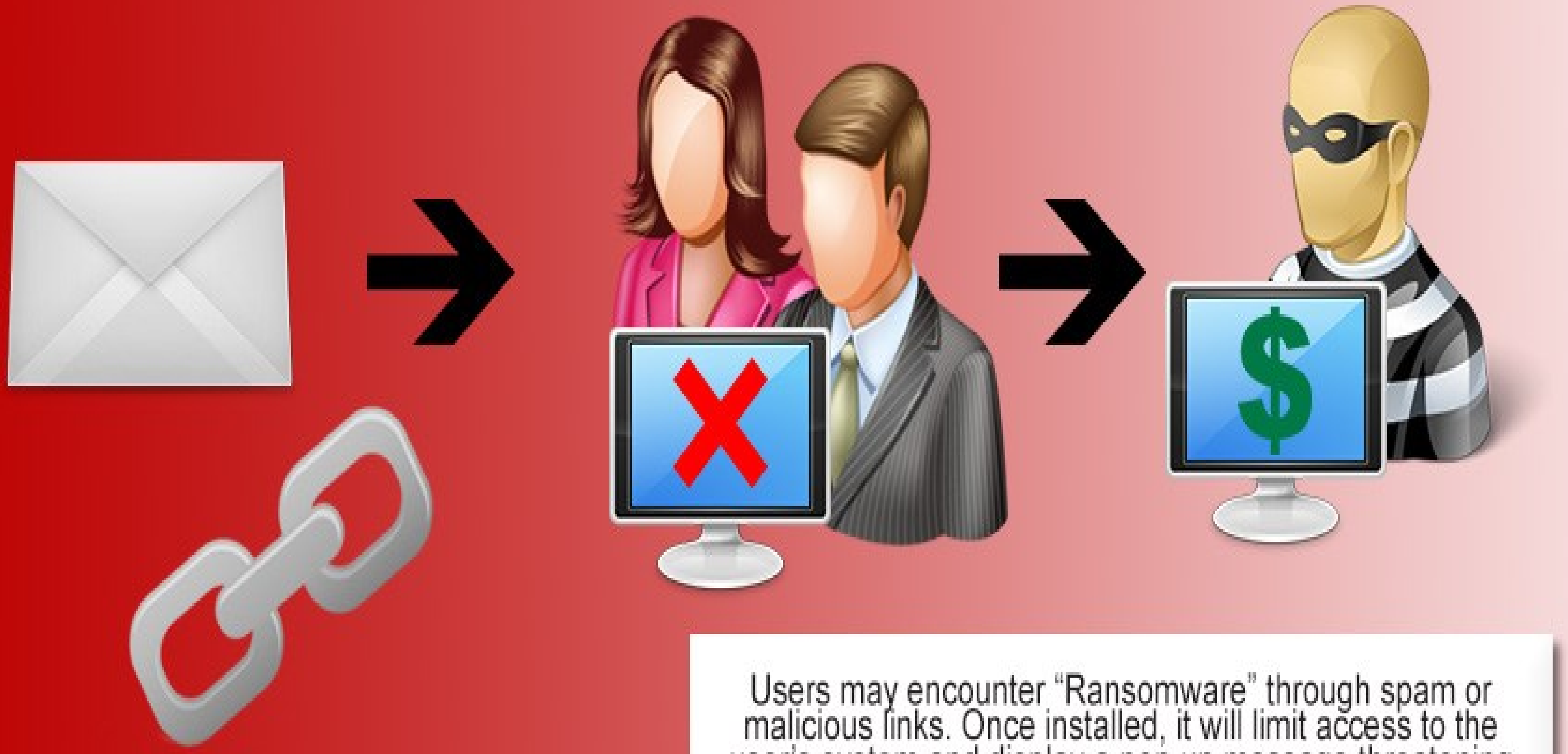
National Computer Board

CERT–MU

Malware

- Backdoor Trojans
- Keylogggers
- Rootkits
- Viruses
- Worms

RANSOMWARE

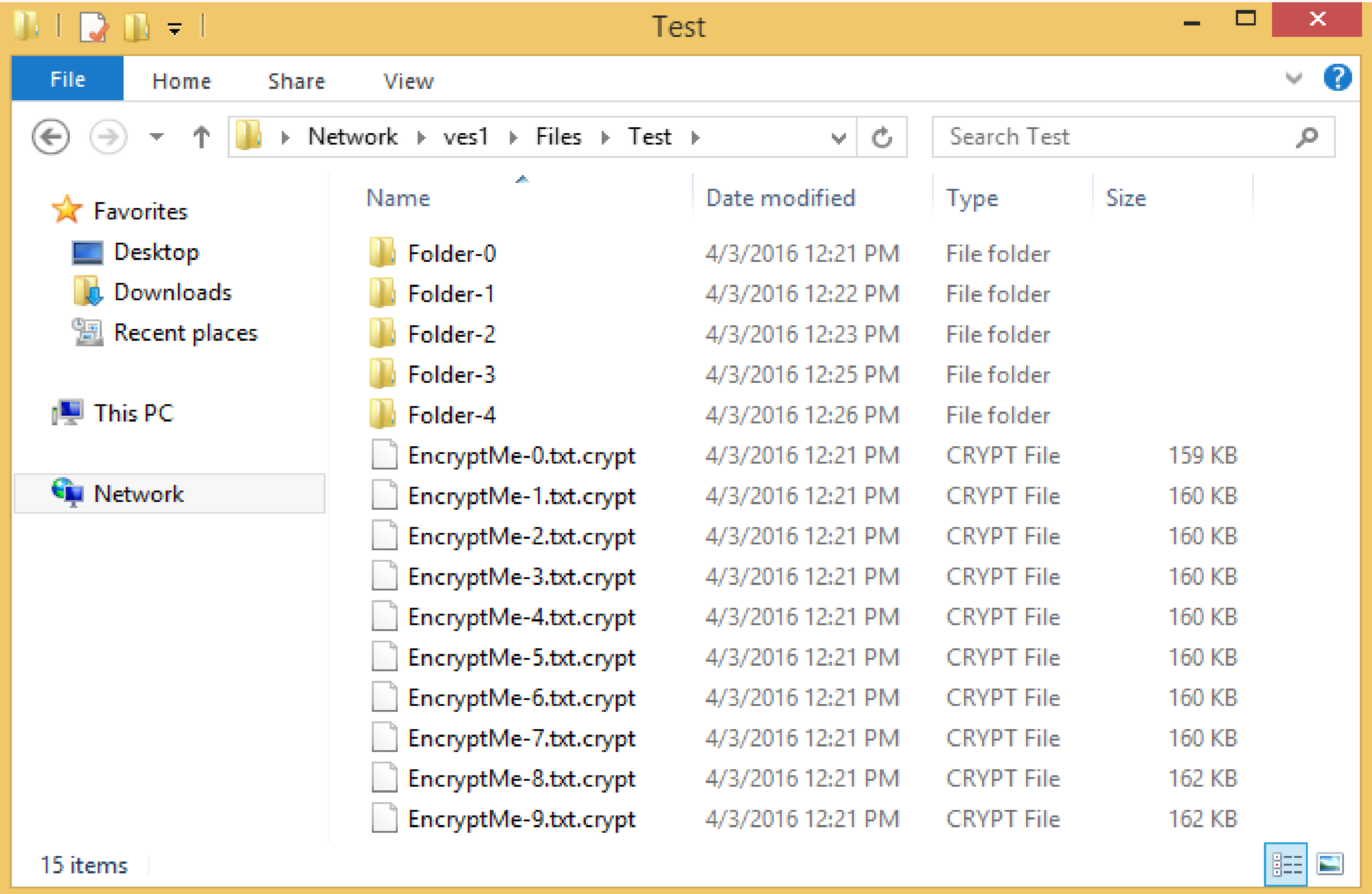


Users may encounter "Ransomware" through spam or malicious links. Once installed, it will limit access to the user's system and display a pop up message threatening the user to pay to have access to their information.

Ransomware Types

- Locky
- CTB-Locker
- CryptoWall 2.0
- Jigsaw

Ransomware Post Attack



Name	Date modified	Type	Size
Folder-0	4/3/2016 12:21 PM	File folder	
Folder-1	4/3/2016 12:22 PM	File folder	
Folder-2	4/3/2016 12:23 PM	File folder	
Folder-3	4/3/2016 12:25 PM	File folder	
Folder-4	4/3/2016 12:26 PM	File folder	
EncryptMe-0.txt.crypt	4/3/2016 12:21 PM	CRYPT File	159 KB
EncryptMe-1.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-2.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-3.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-4.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-5.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-6.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-7.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-8.txt.crypt	4/3/2016 12:21 PM	CRYPT File	162 KB
EncryptMe-9.txt.crypt	4/3/2016 12:21 PM	CRYPT File	162 KB

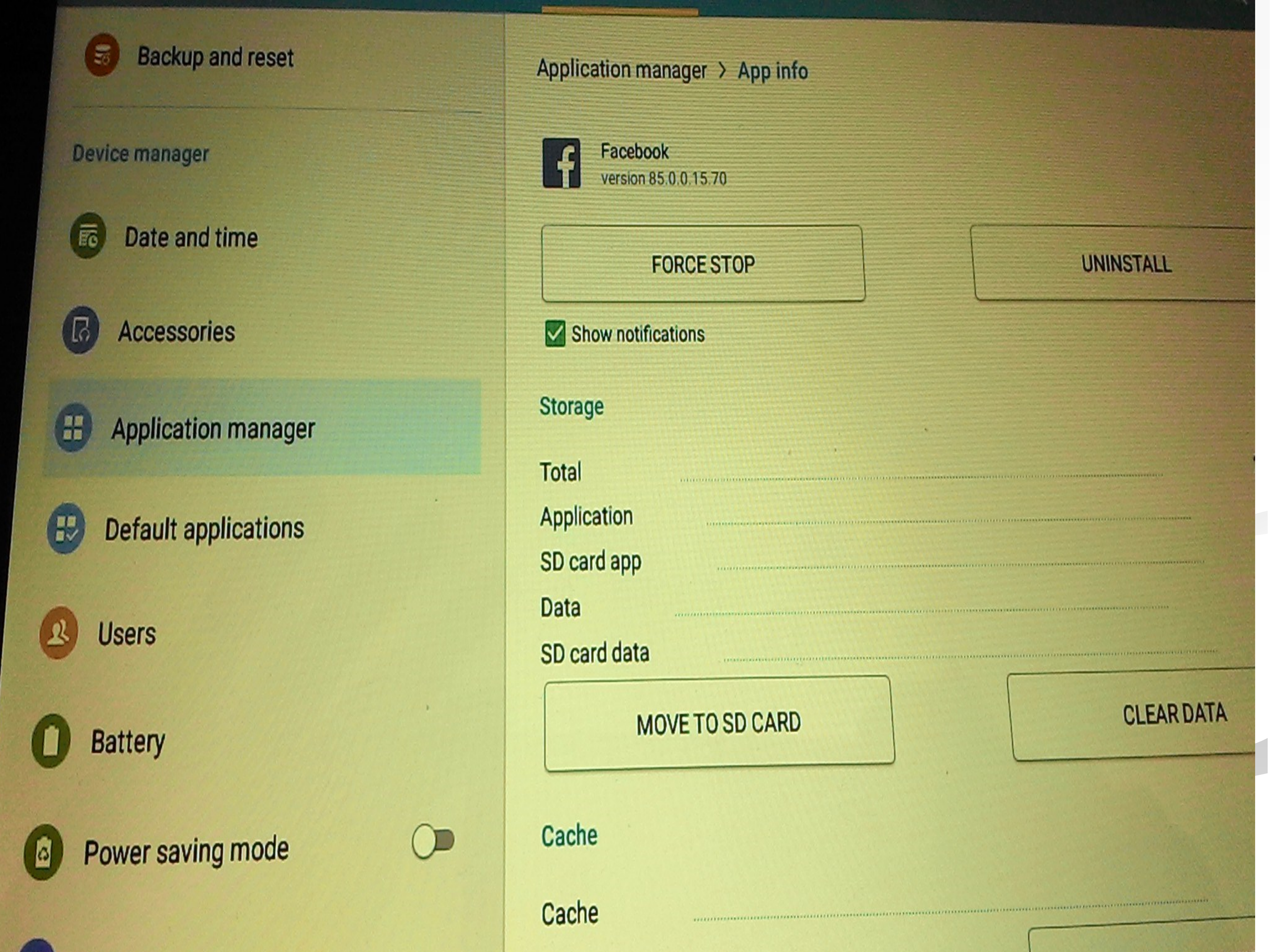
15 items

Social Engineering

- Phone
- Email
- Social Networks

Insider Threat

- Disgruntled Employees
- Lack Of Proper Access Control
- Unsafe Information Keeping
- Lack of Clear Screen & Clear Desk policy



Application manager > App info

Facebook
version 85.0.0.15.70

☑ Show notifications

Storage

Total

Application

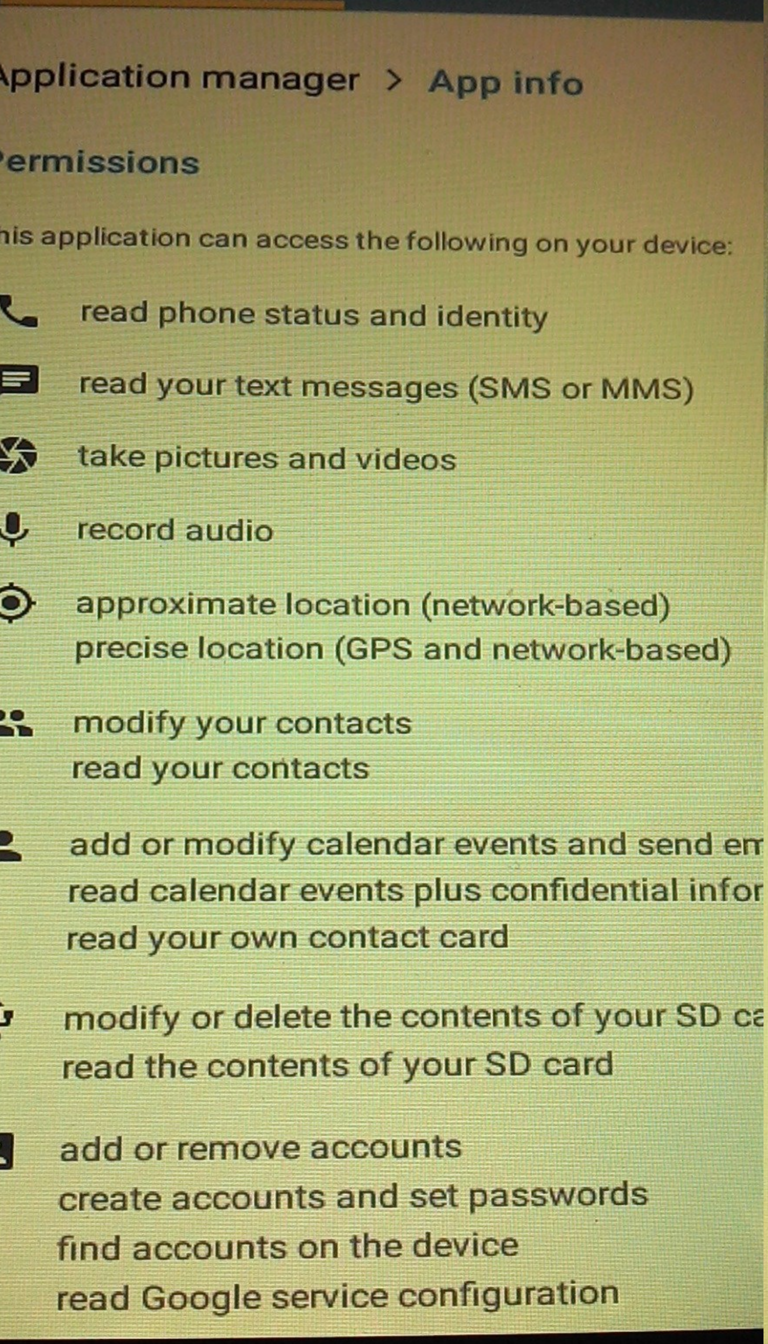
SD card app

Data

SD card data

Cache

Cache



pplication manager > App info

ermissions

his application can access the following on your device:

read phone status and identity

read your text messages (SMS or MMS)

take pictures and videos

record audio

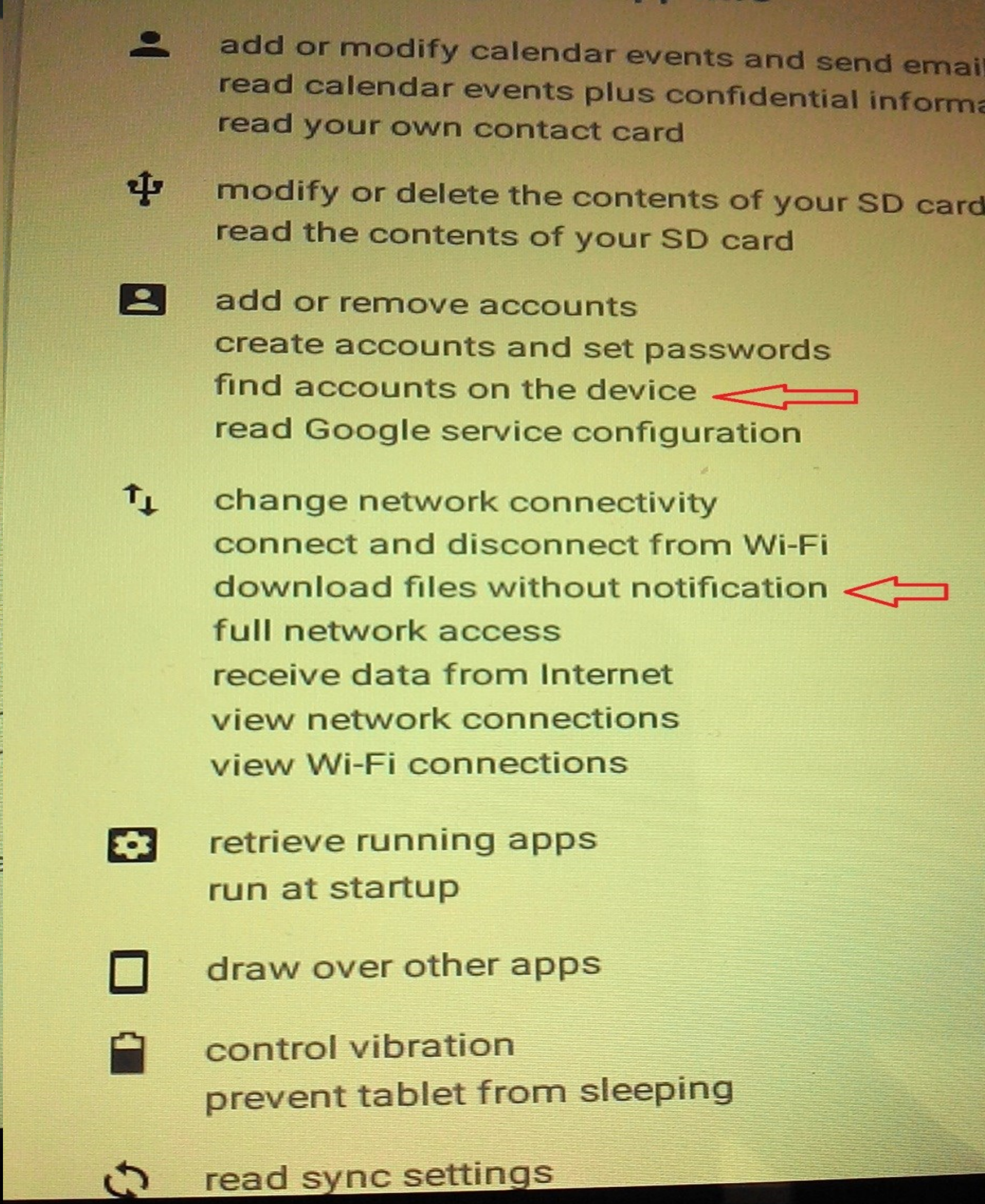
approximate location (network-based)
precise location (GPS and network-based)

modify your contacts
read your contacts

add or modify calendar events and send em
read calendar events plus confidential infor
read your own contact card

modify or delete the contents of your SD ca
read the contents of your SD card

add or remove accounts
create accounts and set passwords
find accounts on the device
read Google service configuration



add or modify calendar events and send emai
read calendar events plus confidential informa
read your own contact card

modify or delete the contents of your SD card
read the contents of your SD card

add or remove accounts
create accounts and set passwords
find accounts on the device
read Google service configuration

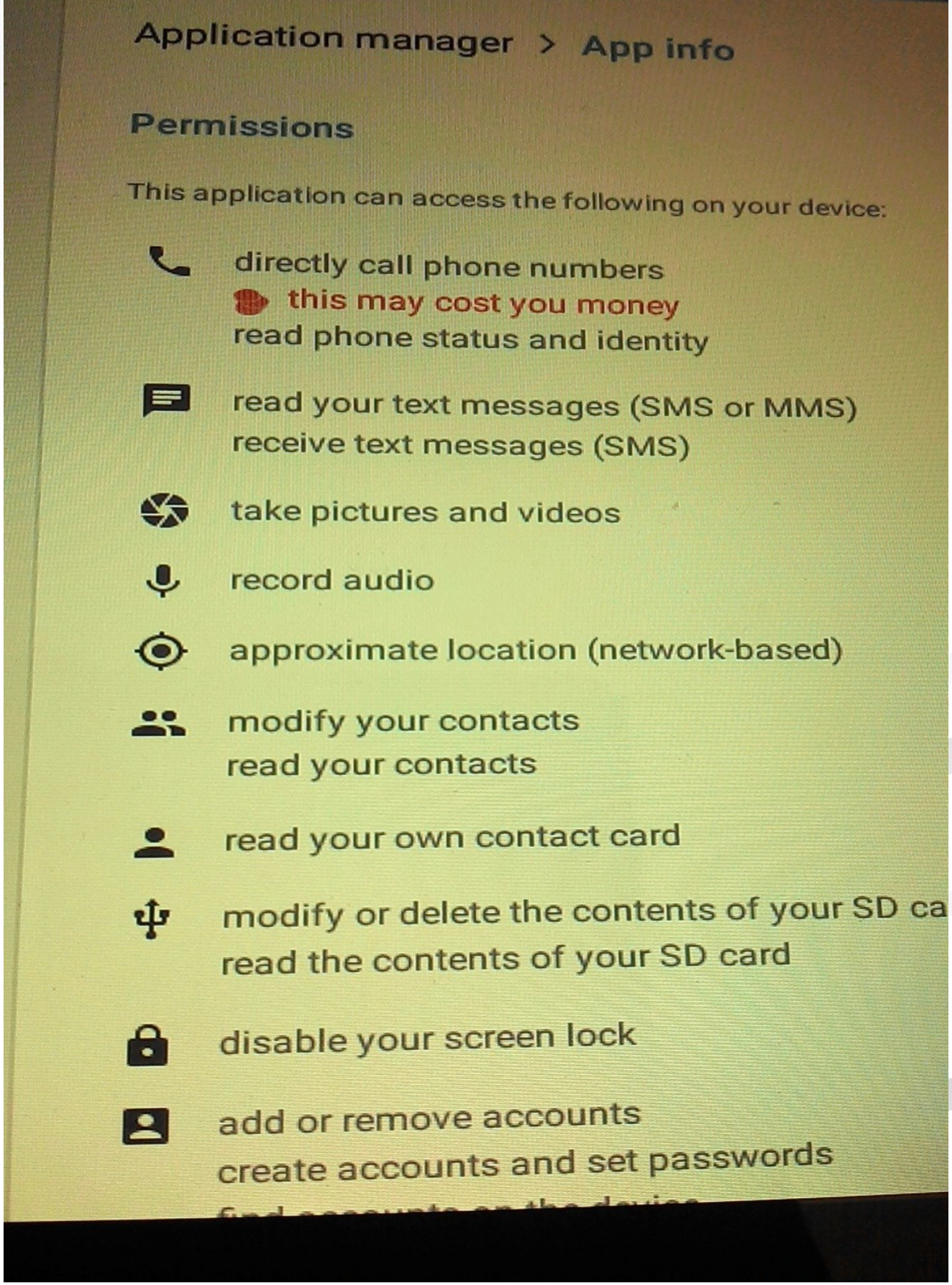
change network connectivity
connect and disconnect from Wi-Fi
download files without notification
full network access
receive data from Internet
view network connections
view Wi-Fi connections

retrieve running apps
run at startup

draw over other apps

control vibration
prevent tablet from sleeping

read sync settings



Application manager > App info

Permissions

This application can access the following on your device:

directly call phone numbers
this may cost you money
read phone status and identity

read your text messages (SMS or MMS)
receive text messages (SMS)

take pictures and videos

record audio

approximate location (network-based)

modify your contacts
read your contacts

read your own contact card

modify or delete the contents of your SD ca
read the contents of your SD card

disable your screen lock

add or remove accounts
create accounts and set passwords
find accounts on the device

Mauritian Strategy/Policy - by CERT-MU

- Data Protection Act 2004
- Critical Information Infrastructure Protection (CIIP)
- Cybercrime Strategy
- Cybersecurity Strategy

Cyber Security Strategy

- Driven by CERT-MU
- Endorsed by Government in October 2014
- To enhance the cyber threat preparedness of Mauritius and managing the disturbances caused by these threats
- 28 projects being implemented

- Anti Cyber Threat Monitoring System
- Capacity Building
- International Collaboration
- Cyber Education

Anti Cyber Threat Monitoring System

- Monitor and mitigate the risk of cyber security threats and attacks on government websites and portals, as well as on critical information infrastructures.
- Carry out round-the-clock security operations for early detection and prevention of potential cyber threats.
- Gather cyber threat intelligence, which it will analyse and assess for drawing up defensive measures at the national level.
- Promote awareness of cyber threats and coordinate security responses in both public and private sectors.

Contact CERT-MU

- Hotline: 800-2378
- Website: www.cert-mu.org.mu
- General Queries: contact@cert.ncb.mu
- Incident Reporting: incident@cert.ncb.mu
- Mailing List Subscription: subscribe@cert.ncb.mu
- Vulnerability Reporting: vulnerability@cert.ncb.mu