



Cyber Crime Types, Prevention & Reporting

Session Objectives

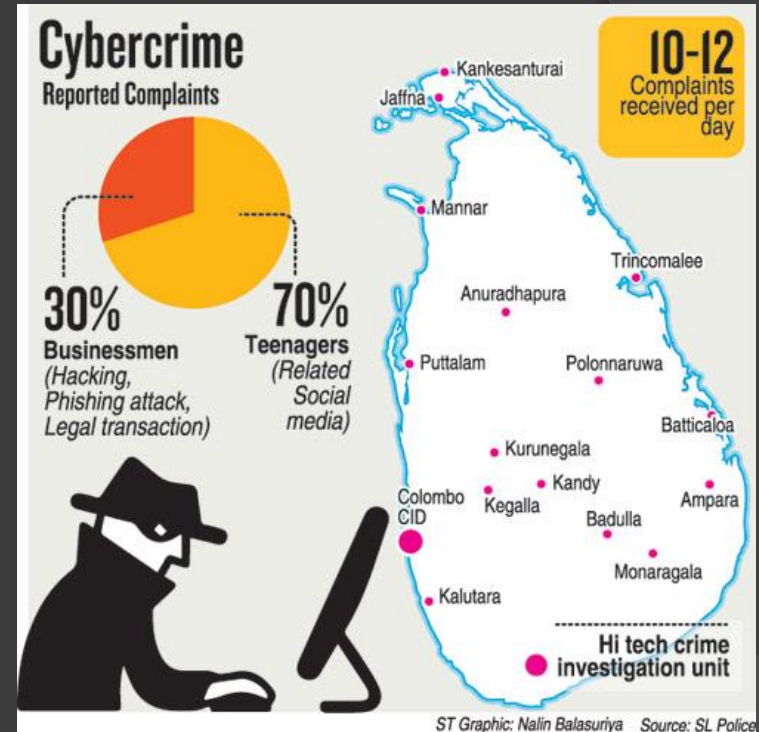
At the end of this session participants will be able to:

- Identify Type of Cybercrime Reported in Sri Lanka.
- Related Laws.
- Describe Standard Reporting Procedures.
- How to Prevent.

Cyber Crime

Types Reported In Sri Lanka

- ◉ EMAIL - SPOOFING & PHISHING
- ◉ IP SPOOFING
- ◉ PACKET SNIFFING
- ◉ HACKING
- ◉ VIRUS, WORMS & TROJANS
- ◉ DENIAL OF SERVICE ATTACK



E-mail spoofing & Phishing

- **E-mail spoofing** is a term used to describe (usually fraudulent) e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source.
- E-mail spoofing is a technique commonly used for [spam](#) e-mail and [phishing](#) to hide the origin of an [e-mail](#) message
- Anonymous Emails ?

Google Security Team to chaftimehmood

Verification Required.

Dear Gmail User,

The Gmail infrastructure is going through an annual security and performance overhaul. In the same respect, you are requested to verify your account by clicking on the following link. The Google Security Team is available to provide you all the assistance for secure communication over the Internet. Happy surfing!

accountverification.gmail.com/src/verify.php?confirmation=dhPGcsiuUNdnAoN77q5CHwCgl4MmCAXE72d

You are requested to act on this immediately to guarantee the smooth functioning of your mail account.

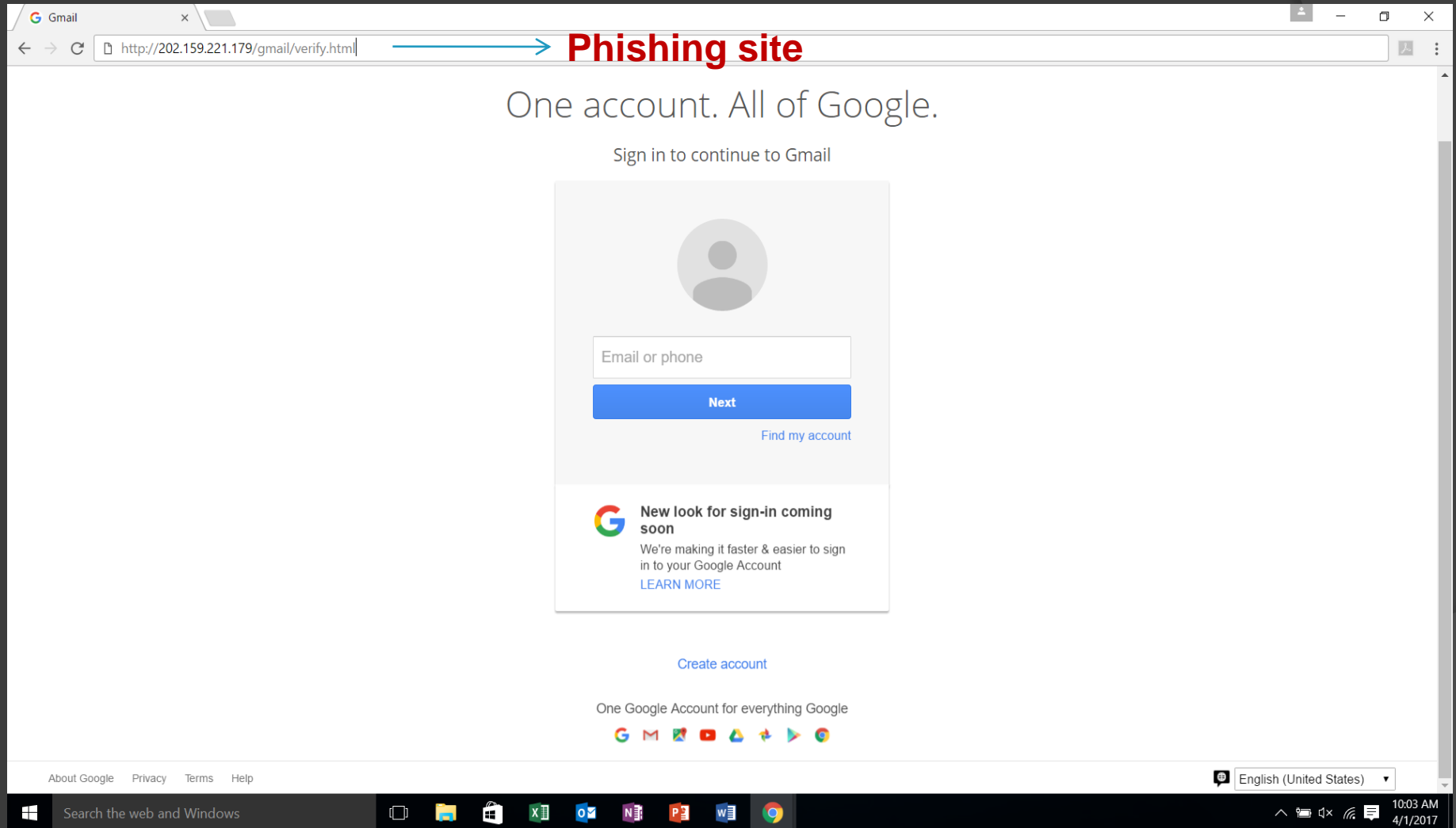
Thanks,
Account Security Administrator
Google Security Team
Google, Inc. Phone: +1 650-253-0000

You are receiving this message from Google because you are a valued member. Google respects your privacy. To learn more, please read our online Privacy Statement. For more information or for general questions regarding your e-mail account, please visit Gmail Help.

Google Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043. All rights reserved.

Phishing ??

<http://202.159.221.179/gmail/verify.html>



One account. All of Google.

Sign in to continue to Gmail



Next

[Find my account](#)



New look for sign-in coming soon

We're making it faster & easier to sign in to your Google Account

[LEARN MORE](#)

[Create account](#)

One Google Account for everything Google



Experience In Cyber Crime Investigation

Committing frauds by inducing the general public to obtain website services which appear to be genuine (phishing attack). Fraudulently obtaining money from Internet Bank Accounts

Cyber Crime Investigation done by CID

- ❖ E-mail header analysis
- ❖ Analyzed e-bank server
- ❖ Evidence of transaction logs
- ❖ Beneficiary account information



03 Suspects were arrested, Case pending in court.

Phishing site

Online Banking

Login



(Corporate Users - CorporateID.UserID)

[Forgot Password?](#)

I want to get to

Dashboard

**Login****Login Using Facebook**[New User? Register for Online Banking now](#)[Complete Your Registration](#)[Do You Need Help?](#)[Downloads](#)[Chat with us on WhatsApp
+94 71 4533670](#)[Report a Problem
Check Problem Status](#)

Search the web and Windows

10:11 AM
4/1/2017



Online Banking

Login



(Corporate Users - CorporateID.UserID)



Forgot Password?

I want to get to

Dashboard



Login

Login Using Facebook



New User? Register for Online Banking now



Complete Your Registration



Do You Need Help?

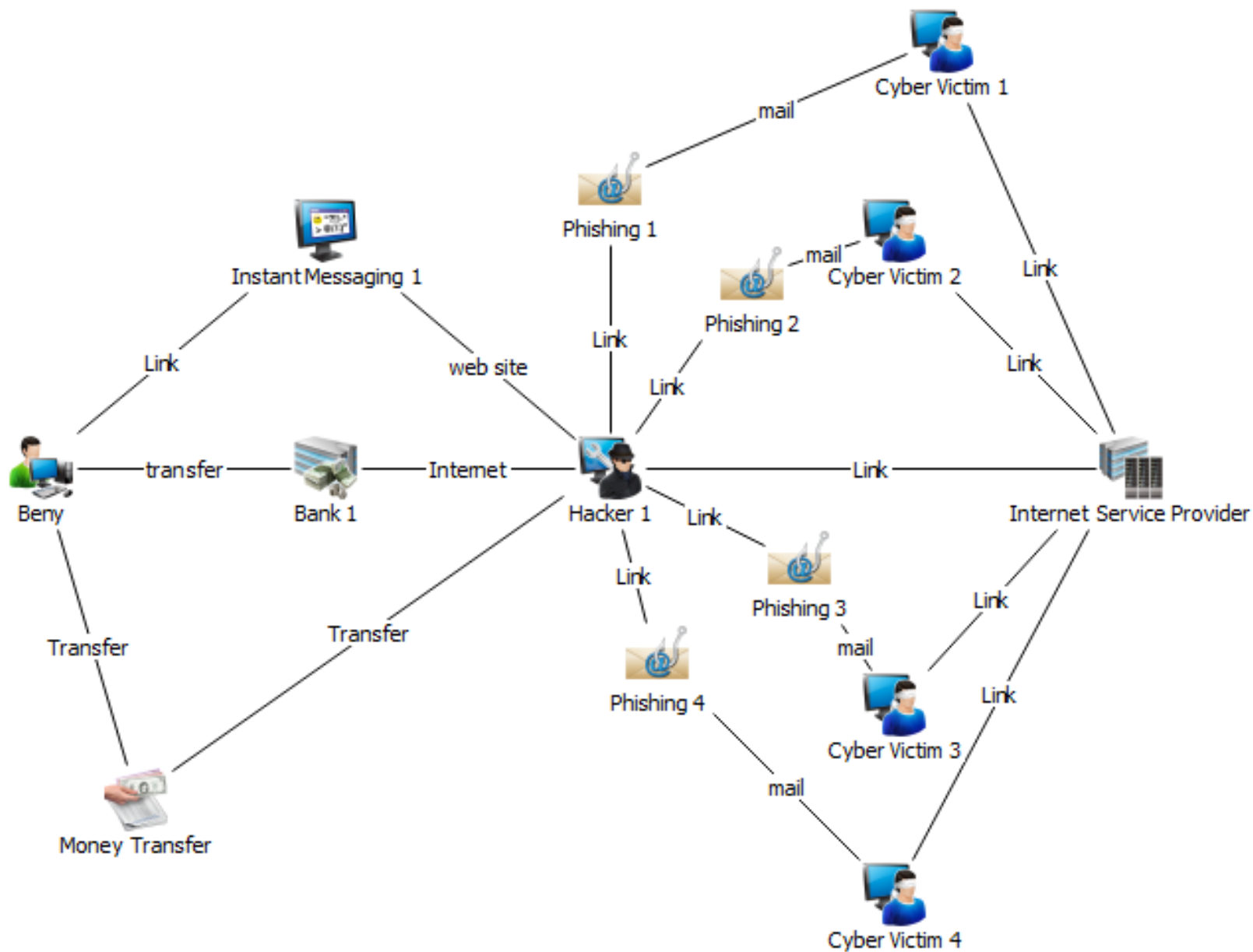


Downloads



Chat with us on WhatsApp
+94 71 4533670

Report a Problem
Check Problem Status



Anonymous Email Service

TOR Networks

Proxy IPs

Anonymouse.Org



AnonEmail

[AnonEmail](#) [AnonWWW](#) [AnonNews](#)

With **AnonEmail** it is possible to send e-mails **without revealing** your e-mail address or **any information about your identity**. Therefore you can **communicate more freely** and you do not have to worry that it might cause consequences for you.

This service allows you to send e-mails without revealing any personal information.

Protect your **privacy, protect your **data**, protect it for **free**.**

To:

Subject:

Message:

Fake mails

Sign-In

Username:

Password:

[Sign In](#)

[Sign up](#)

[Forgot your password?](#)

Visitors

	US	176,407
	IN	63,619
	GB	39,089
	CA	22,522
	IT	21,295
	DE	17,116
	NL	10,553
	BR	9,112
	AU	9,040
	RO	8,436
		1,808,998

FLAG counter

Like 541

[Sitemap](#)

Send fake email.

Send prank emails to your friends.


From Name :	<input type="text"/>	(Optional)
From E-mail *	<input type="text"/>	
To Email *	<input type="text"/>	
Subject of the email :	<input type="text"/>	(Optional)


Fake mails

0

Flattr

Donate


bitcoin



3.4k

Like

205

Tweet

431

Select Language ▼

FAKE MAILER

Online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment:

Attach another file

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

Flash Grader

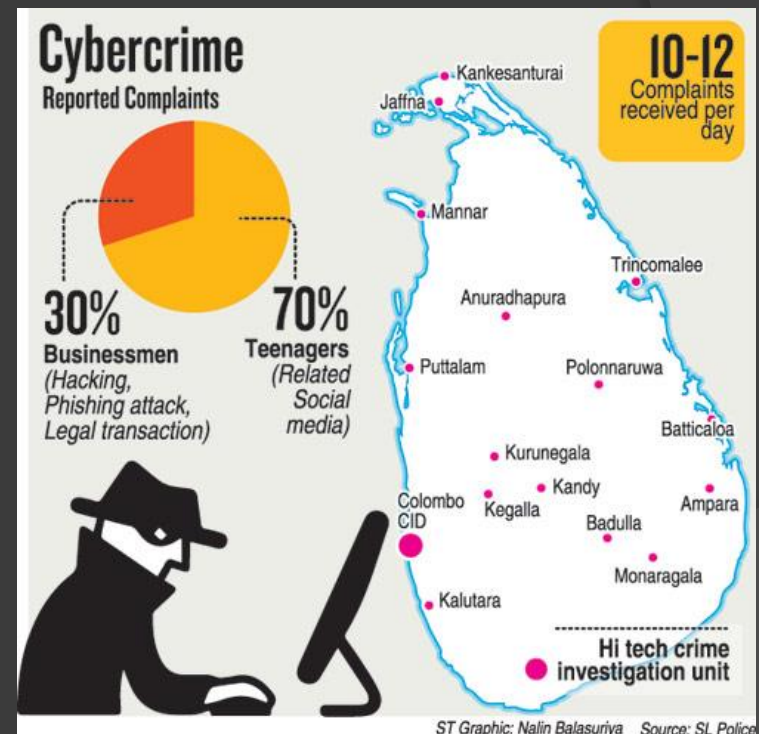
AdChoices ▶

BLADE SOHO
iHair + iCafe
www.BladeSoho.c..
iPad™ Hair Salon
and Coffee Bar -
Experience new
concept book
online!

Cyber Crime

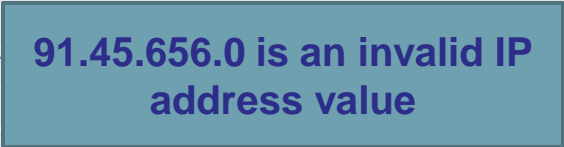
Types Reported In Sri Lanka

- ◉ EMAIL - SPOOFING & PHISHING
- ◉ IP SPOOFING
- ◉ PACKET SNIFFING
- ◉ HACKING
- ◉ VIRUS, WORMS & TROJANS
- ◉ DENIAL OF SERVICE ATTACK



IP Spoofing

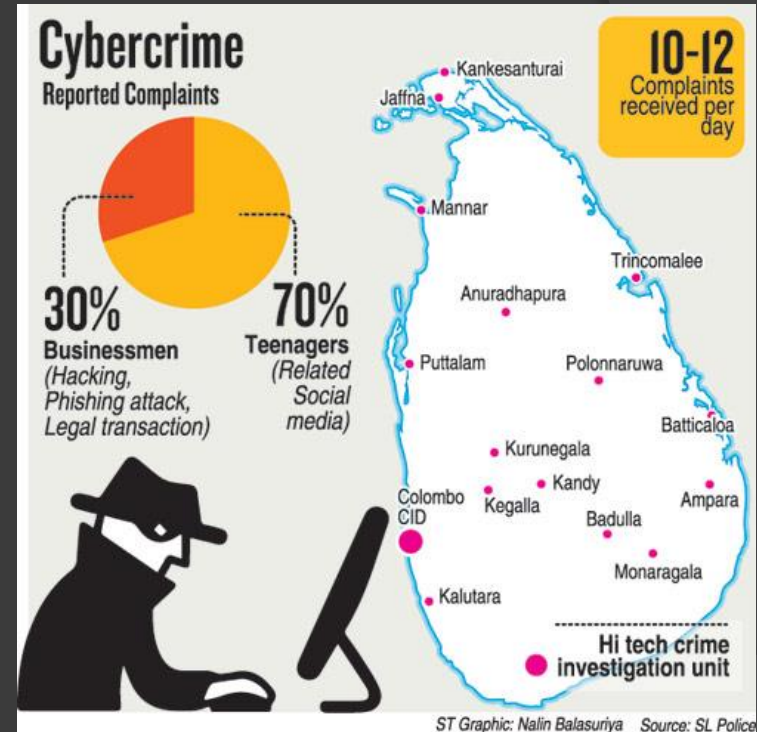
- ◎ **IP** (**Internet Protocol**) **address spoofing** refers to the creation of **IP packets** with a forged (spoofed) source **IP address** with the purpose of concealing the identity of the sender or impersonating another computing system.
- ◎ The Onion Router, Proxy Servers etc

Return-path	<incidencia@centraldellibro.com>	
Received	from avserver.sandesh.cert-in.org.in with ESMTP id <0JHJ00D02MTJWM00@sandesh.cert-in.org.in> for incident@cert-in.org.in; Sat, 05 May 2007 06:30:55 +0530 (IST)	by sandesh.cert-in.org.in ("sandesh.cert-in.org.in SMTP server")
Received	from avserver.sandesh.cert-in.org.in for <incident@cert-in.org.in>; Sat, 05 May 2007 06:44:54 +0530 (IST)	by localhost.sandesh.cert-in.org.in (Postfix) with ESMTP id 7819AF49
Received	from webclust1.cert-in.org.in <incident@cert-in.org.in>; Sat, 05 May 2007 06:44:54 +0530 (IST)	by avserver.sandesh.cert-in.org.in (Postfix) with ESMTP id 5677EF04for
Received	from cpe-24-59-205-142.twcny.res.rr.com ([24.59.205.142]) with SMTP id <0JHJ00D03MTGWI00@sandesh.cert-in.org.in> for incident@cert-in.org.in; Sat, 05 May 2007 06:30:54 +0530 (IST)	by sandesh.cert-in.org.in ("sandesh.cert-in.org.in SMTP server")
Received	(gmail 5503 by uid 479); Fri, 04 May 2007 09:18:28 -0500	
Date	Sat, 05 May 2007 06:30:54 +0530 (IST)	
Date-warning	Date header was inserted by sandesh.cert-in.org.in	
From	admin@microsoft.com	
Subject	Internet Explorer 7.0 Beta	
X-Originating-IP	[91.45.656.0]	
X-Sender	incident@cert-in.org.in	
To	incident@cert-in.org.in	
Message-id	<20070504041828.5505.qmail@cpe-24-59-205-142.twcny.res.rr.com>	
MIME-version	1.0	
Content-type	text/html	
Importance	High	
X-Originating-Email	[incident@cert-in.org.in]	
X-imss-version	2.046	
X-imss-result	Passed	
X-imss-scores	Clean:1.17076 C:2 M:5 S:9 R:5	
X-imss-settings	Baseline:1 C:3 M:3 S:3 R:3 (0.0000 0.0000)	
Original-recipient	rfc822;incident@cert-in.org.in	

Cyber Crime

Types Reported In Sri Lanka

- ◉ EMAIL - SPOOFING & PHISHING
- ◉ IP SPOOFING
- ◉ PACKET SNIFFING
- ◉ CYBER EXTORTION
- ◉ HACKING
- ◉ VIRUS, WORMS & TROJANS
- ◉ DENIAL OF SERVICE ATTACK



Cyber Crime

Types Reported In Sri Lanka

- SOFTWARE PIRACY
- PORNOGRAPHY
- CREDIT CARD FRAUD
- CYBER STALKING
- CYBER DEFAMATION
- CYBER BULLYING
- CYBER SCAMS



Computer Forensics or Electronic Forensics?

- ⦿ Are computers the only devices with microprocessors?
- ⦿ Are computers the only devices with memory (RAM/ROM/PROM/EPROM/EEPROM)?
- ⦿ Are computers the only devices that can input, process, store, and output data?

Stages of Computer Forensics

- ① Identification
(Media that contains potential evidence)
- ② Preservation
(So that data is not lost)
- ③ Analysis & Discovery
(Scope of Investigation & Forensic software tools)
- ④ Documentation
(Comprehensive notes & journals)
- ⑤ Verification
(Hashing)
- ⑥ Presentation
(Investigators & Court)

Identification

Computer Tower



Desktop / Server Hard Drive



Laptop Hard Drive



Wireless Router



iPod



Thumb Drives



Cell Phone



Blackberry



Pager



Storage Media
(CDs, DVDs, Floppy Disks,
Zip Disks and Flash Cards)



Stages of Computer Forensics

- ◉ Identification
(Media that contains potential evidence)
- ◉ Preservation
(So that data is not lost)
- ◉ Analysis & Discovery
(Scope of Investigation & Forensic software tools)
- ◉ Documentation
(Comprehensive notes & journals)
- ◉ Verification
(Hashing)
- ◉ Presentation
(Investigators & Court)

Package and transport

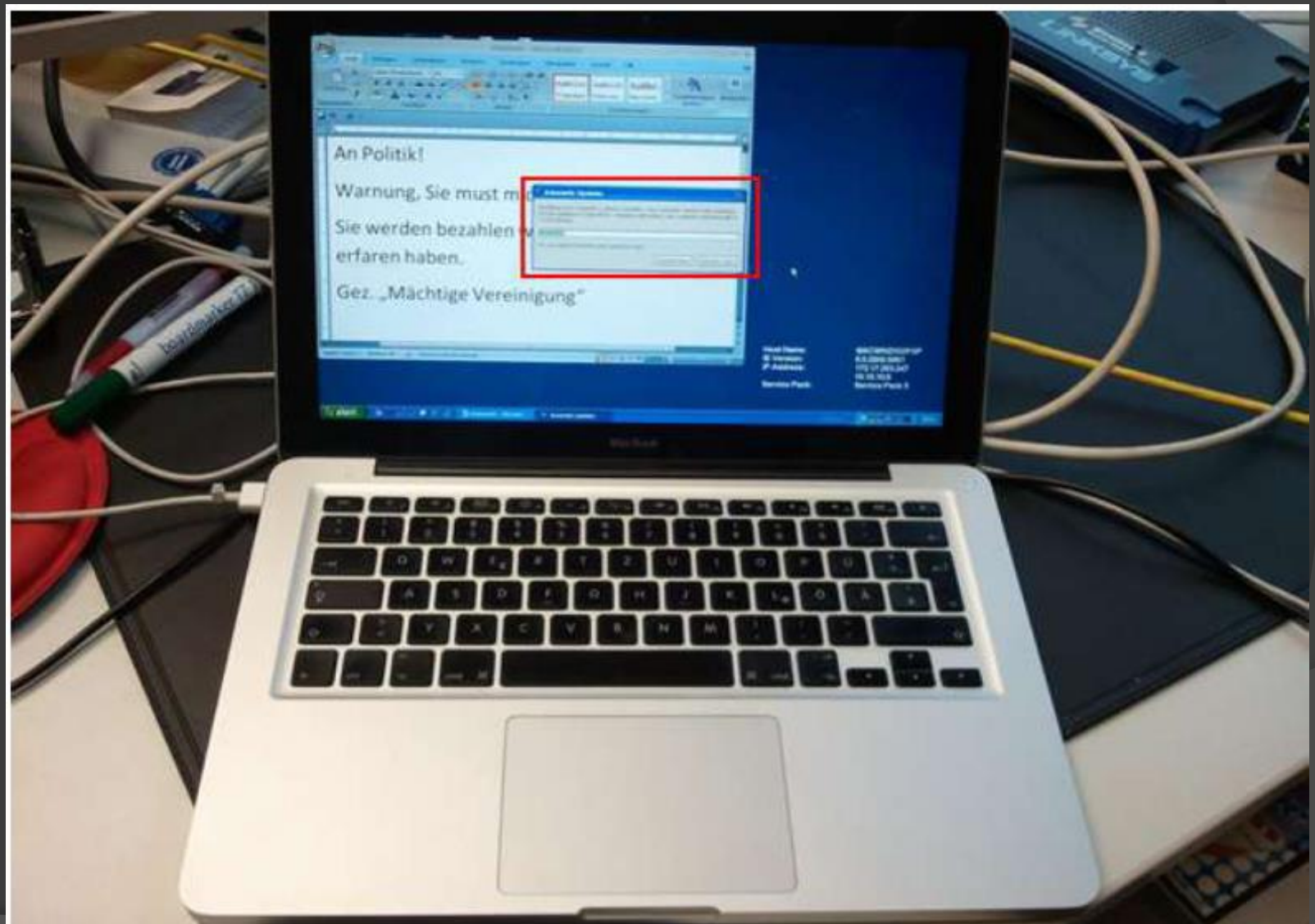
1. Antistatic bags
2. Antistatic bubble wrap
3. Cable ties
4. Evidence bags and tape
5. Boxes for packaging external storage media such as USB devices DVDs, or CDs
6. Packing materials
7. Flat pack assembly boxes or sturdy boxes of various sizes



Package and transport

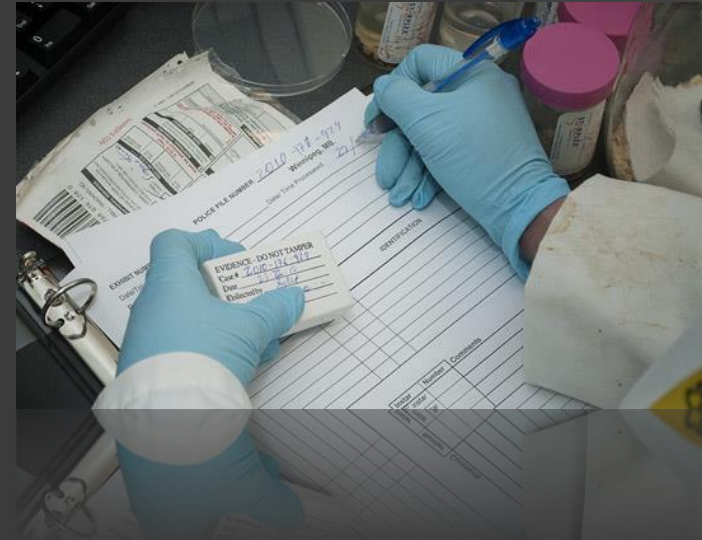
- ❖ properly documented and labelled before packaging
- ❖ transport the collected e-evidence in the original packaging





Storage

- Ensure that evidence is inventoried in accordance with the relevant policies.
- Store evidence in a secure area, away from extreme temperature and humidity.
- Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.



Storage facilities

Use an adequately secure store room with appropriate

- access control,
- fire protection (e.g., alarm, fire extinguishers, no smoking in the storage area or in the vicinity),
- temperature and humidity, and
- protection from magnetic sources (e.g., far from directional radio devices).



Stages of Computer Forensics

- ◉ Identification
(Media that contains potential evidence)
- ◉ Preservation
(So that data is not lost)
- ◉ Analysis & Discovery
(Scope of Investigation & Forensic software tools)
- ◉ Documentation
(Comprehensive notes & journals)
- ◉ Verification
(Hashing)
- ◉ Presentation
(Investigators & Court)

Protection of Digital Evidence

Algorithms of Hash

- ❖ MD5
- ❖ SHA 1
- ❖ SHA 2
- ❖ TIGER
- ❖ PANAMA
- ❖ RIPEMD 160

Protection of Digital Evidence

◎ Hash Calculation Software

- ❖ Hash Cal
- ❖ Helix 4
- ❖ FTK Imager
- ❖ EnCase

Stages of Computer Forensics

- ④ Identification
(Media that contains potential evidence)
- ④ Preservation
(So that data is not lost)
- ④ Analysis & Discovery
(Scope of Investigation & Forensic software tools)
- ④ Documentation
(Comprehensive notes & journals)
- ④ Verification
(Hashing)
- ④ Presentation
(Investigators & Court)

Related Legislations

- ✓ The Computer Crime Act No: 24 of 2007
- ✓ The Payment Devices Frauds Act No: 30 of 2006
- ✓ The Electronic Transaction Act No: 19 of 2006
- ✓ The Payment & Settlement System Act No: 28 of 2005
- ✓ Intellectual Property act No 36 of 2003
- ✓ The Evidence (special provisions) Act No: 14 of 1995
- ✓ Obscene publications Act No: 22 of 1983
- ✓ Penal code & Criminal Procedure Code

Evidence (Special Provisions) Act. No. 14 of 1995

Section 4 : How to proceed contemporaneous records
as a evidence

Section 5 : Computer Evidence

Section 6 : Affidavits for Evidence

Section 7 : Notice to have access to inspect.

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

The Act is defined under sections 1 & 2

On the occasion of a person committing a crime under this Act while residing in Sri Lanka or outside Sri Lanka

A Computer/Program affected as a result of an Act committed which amounts to an offence under the Act “in Sri Lanka or outside” during the relevant period

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Crimes are defined under sections 3 to 14.

- Section 3 – An Act resulting in accessing the computer system illegally
- Section 4 – An act committed in order to illegally access the system to commit a crime
- Section 5 – Performing a computer function without proper authority

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Crimes are defined under sections 3 to 14.

- Section 6 – Crimes against national security
National Security
National Economy
Public Security
- Section 7 – Using data obtained illegally
- Section 8 – Obtaining data illegally

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Crimes are defined under sections 3 to 14.

- Section 9 – Providing illegal assistance to commit a crime
- Section 10- Revealing data without proper authority to access
- Section 11 – Attempting to commit a crime

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Crimes are defined under sections 3 to 14.

- Section 12- Aiding and Abetting a crime
- Section 13 – Conspiring to commit a crime
- Section 14 – Offering financial grant as a reward for profit or loss consequent to committing a crime

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

- By Sections 15 & 16, the applicability of provisions of sections 15 and 16 of Crime Act No.15 of 1979 are defined.
- Section 17 ;a specialist is defined
- A special committee appointed by the Minister consisting of academics of the University
- Enter upon any premises along with a police officer not below the rank of a sub-inspector.
- Section 18 – Powers to check and confiscate
- Section 19 – Powers to protect data and systems involved in the investigation.

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Section 20; Normal use of computer not to be hampered.

Section 21; Powers of police officer to arrest, search and seize

No police officer shall access any computer for the purpose of an investigation under this Act unless the IGP has certified in writing that such police officer possesses adequate knowledge and skill in the field

Provisions under Computer Crimes Act No.24 of year 2007 and the relevance of the Act.

Section 22; Police officer to record and afford access to
police officer should issue a complete list of such items
and data including the date and time of such seizure

Section 23; Duty to assist investigation.



Section 24; Confidentiality of information obtained in the
course of an investigation.

Section 25; Jurisdiction; delegated to the Supreme Court

Reporting Procedures

- Tell IGP (telligp@police.lk)
- 119 Call System
- Police Cyber Crime Reporting Center
(<http://www.telligp.police.lk/>)
- Reporting CID (dir.cid@police.lk)
 - Hot line 0112422176
 - Cybercrime Unit 0112326979
- All Police Stations

“தேவதீபநிபிதி”
“பொலிஸ்மா அதிபருக்கு சொல்லுங்கள்”
“TELL IGP”

Public Feedback	Complain Status
Your District	-Select District-
Nearest Police Station	-Select Police Station-
Complaint Category	-Select Complain Category-
Type Your Name	
Address	
NIC Number	
Contact Number	
Email Address	
Complaint Subject	
Complaint * (Please send us your complain in Hindi,English or Tamil language.)	
I need notification about status of the complaint	
Enter Verification Code *	
	
 Click the refresh button to generate a new one.	
Attachment (If you have any document or image related to the complaint, Please attach to this complaint.) <div> <input type="button" value="Choose File"/> <input type="button" value="No file chosen"/> </div>	
<input type="button" value="Submit"/>	

* පොදුජීපීටී ඩිසත්ත *
* பொலிஸ்மது அதிகருக்கு சொல்லுங்கள் *
* TELL IGP *

Public Feedback

Complain Status

Your District

-Select District-

Nearest Police Station

-Select Police Station-

Complaint Category

-Select Complain Category-

Type Your Name

Address

NIC Number

Contact Number

Email Address

Complaint Subject

Complaint * (Please send us your complain
in Sinhala,Tamil or English language.)I need notification about status of the
complaint

Enter Verification Code *



Click the refresh button to generate a new one.

Attachment (If you have any document or
image related to the complaint, Please
attach to this complaint.)

Choose File

No file chosen



Submit

Reporting Procedures

- Tell IGP (telligp@police.lk)
- 119 Call System
- Police Cyber Crime Reporting Center
(<http://www.telligp.police.lk/>)
- Reporting CID (dir.cid@police.lk)
 - Hot line 0112422176
 - Cybercrime Unit 0112326979
- All Police Stations

Questions?



THANK
YOU....