# TICT 3142 Social and Professional Issues in IT

## Lesson 08 Cybercrime Techniques

T. Nusky Ahamed
Lecturer (Prob)
Department of ICT
Faculty of Technological Studies
University of Vavuniya

# Introduction to Cybercrime Techniques

Cybercrime refers to illegal activities that exploit computer systems, networks, or digital platforms. As cybercriminals become more advanced, understanding their methods is vital. Prevention begins with awareness. This includes not just software threats but also human-targeted manipulation.

# Cybercrime Tools and Methods

Common tools used by cybercriminals include:

•**Phishing**: Tricking users into revealing personal info.

•**Malware/Ransomware**: Infecting and locking devices for ransom.

•**Keyloggers**: Recording keystrokes to steal credentials.

•**DDoS attacks**: Overloading servers with traffic.

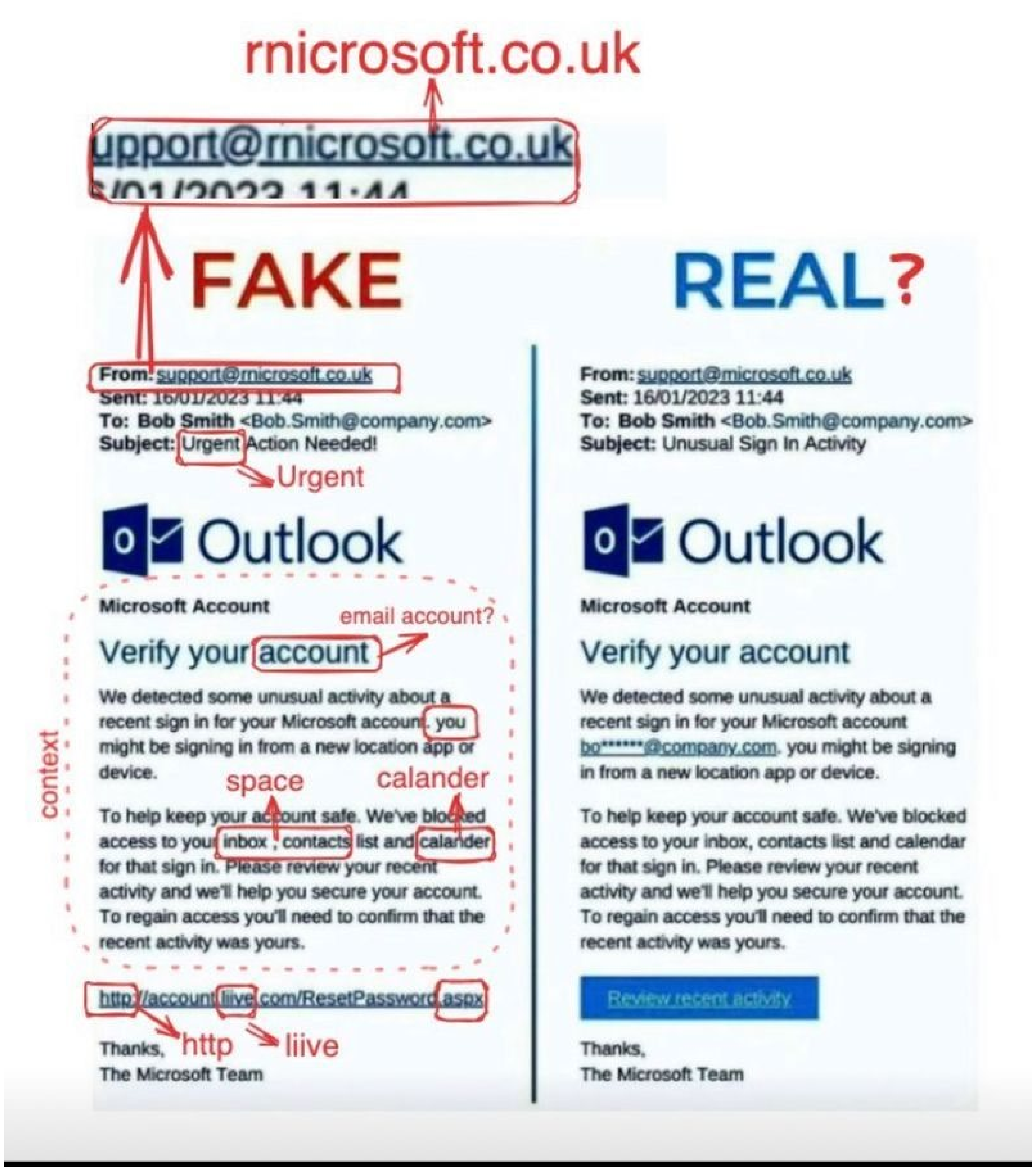
•**Dark Web**: A hidden space where criminals buy/sell illegal cyber tools and data.

# Phishing & Spear-Phishing

**Phishing:** Random, widespread fake messages (e.g., fake bank emails).

**Spear-Phishing:** Targeted at specific people or groups, often well-researched.

These emails look real and may contain fake links or attachments to install malware or steal data



**FAKE**

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

**Microsoft Account**

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account, you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

**REAL?**

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

**Microsoft Account**

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com, you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Thanks,
The Microsoft Team

# Ransomware & Malware

**Ransomware**: Encrypts files and demands money for the key.

*Examples*:

**lankaThe Cargills Bank Data Leak: Uncovering Sri Lanka's Largest Breach and the Silence Surrounding It**

*https://chanidumadalagama.medium.com/the-cargills-bank-data-leak-uncovering-sri-lankas-largest-breach-and-the-silence-surrounding-it-aefee619b0e6*

**Malware**: General term for harmful software like viruses, trojans, worms, spyware.

# Botnets and DDoS Attacks

- **Botnet**: A group of infected computers (zombies) controlled remotely.

- **DDoS**: Distributed Denial of Service attacks that flood a website/server, making it unavailable.

- Used to disrupt services, sometimes as political or financial attacks.

# Keyloggers & Dark Web

- **Keyloggers**: A keylogger (short for keystroke logger) is a type of surveillance software or hardware that records every keystroke typed on a keyboard, often without the user's knowledge. It is one of the most common tools used in cyberattacks to steal sensitive data, particularly usernames, passwords, credit card numbers, and other private information.

- **Dark Web**: Accessed using tools like Tor. It's where stolen data, malware kits, and hacking services are traded anonymously.

# Man-in-the-Middle (MitM) Attacks

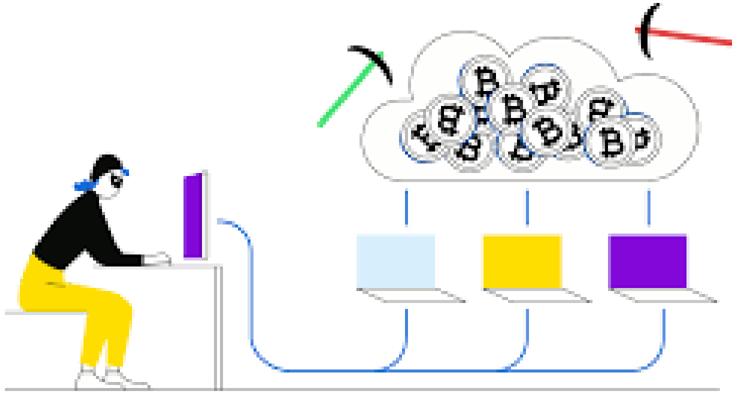
- Attacker secretly intercepts and possibly alters communication between two parties.
- Risks include login theft, unauthorized bank transfers.
- Prevention: Always use HTTPS, VPNs, and secured Wi-Fi.

# SQL Injection & Web Exploits

- SQL Injection: Exploiting poor database coding to access or change data.
- Other threats:
  - **XSS** (Cross-Site Scripting): Injecting malicious code into websites.
  - **CSRF** (Cross-Site Request Forgery): Tricks users into submitting unwanted actions.

# Cryptojacking

- Cryptojacking is a type of cyberattack where an attacker illegally uses someone else's computer, smartphone, or server resources to mine cryptocurrency—without the victim’s knowledge or consent. Instead of stealing data, the goal of cryptojacking is to steal computing power.



# ⚠️ Impacts of Cryptojacking:

- ⚡ **Reduced system performance** (slowdowns, crashes)
- 🔋 **High CPU/GPU usage**, leading to:
  - Increased electricity bills
  - Hardware overheating or damage
- 🔕 Silent operation—often hard to detect
- 🏢 In business networks, it can slow down or disrupt operations

# Insider Threats: Security Risks from Within

- An insider threat refers to a security risk posed by individuals within an organization, such as employees, contractors, or business partners, who have authorized access to systems, data, and resources—and misuse it intentionally or unintentionally.

- Insider threats are particularly dangerous because the attackers already have trusted access, making them harder to detect than external threats.

## ⚠️ Consequences of Insider Threats:

- 🛑 Data breaches and intellectual property theft
- 💸 Financial losses and regulatory fines
- 📉 Reputation damage
- 🔐 Exposure of customer or employee data
- ⚙️ Disruption of operations

## 🛡️ Preventing Insider Threats:

- ✅ **Access control**: Grant minimum necessary access (principle of least privilege)
- ✅ **Monitoring**: Use insider threat detection tools and monitor behavior
- ✅ **Employee training**: Regularly train staff on cybersecurity best practices
- ✅ **Incident response plans**: Have clear procedures for suspected internal breaches
- ✅ **Background checks**: Screen employees before hiring

# Zero-Day Exploits

- A Zero-Day Exploit refers to a cyberattack that targets a previously unknown software vulnerability, one that the software developer or vendor has had zero days to fix—hence the term “zero-day.
- ”These vulnerabilities are typically not publicly known, so no patch or defense exists at the time of the attack, making them highly dangerous.

# Social Engineering Techniques

Social engineering is a psychological manipulation technique used by attackers to trick individuals into giving up confidential information, such as passwords, bank details, or access credentials—bypassing technological defenses entirely.

Instead of hacking computers, social engineers exploit human behavior—trust, fear, urgency, or curiosity.

Types:

- **Baiting**: Offering something enticing (like a free USB drive or download) to trick the victim into downloading malware.
- **Pretexting**: Impersonating someone with authority.
- **Tailgating**: Physically following someone into a restricted area.
- **Phishing**: Trick via emails or calls to get sensitive info.

# Cybercrime-as-a-Service (CaaS)

- Criminals rent out cyberattack tools.
- Ransomware kits, phishing templates, botnets sold on the dark web.
- Enables even non-technical users to launch attacks.

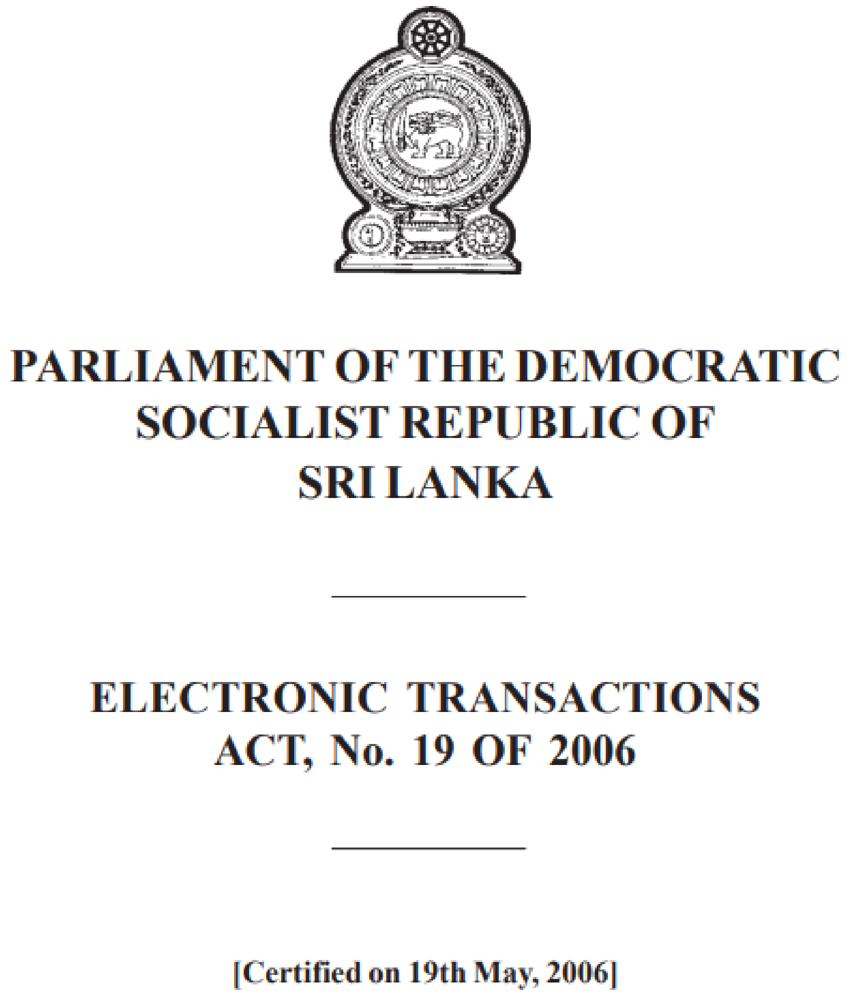
# Dark Web Marketplaces

**Dark web marketplaces** are underground e-commerce platforms operating on the **dark web**, where users can **buy and sell illegal goods and services anonymously**, often using **cryptocurrencies like Bitcoin or Monero**. These marketplaces are a core part of the **cybercriminal ecosystem**.

They are accessible only through special anonymizing software like **Tor (The Onion Router)**, which hides IP addresses and user identities.

# Sri Lanka’s ICT Legal Framework

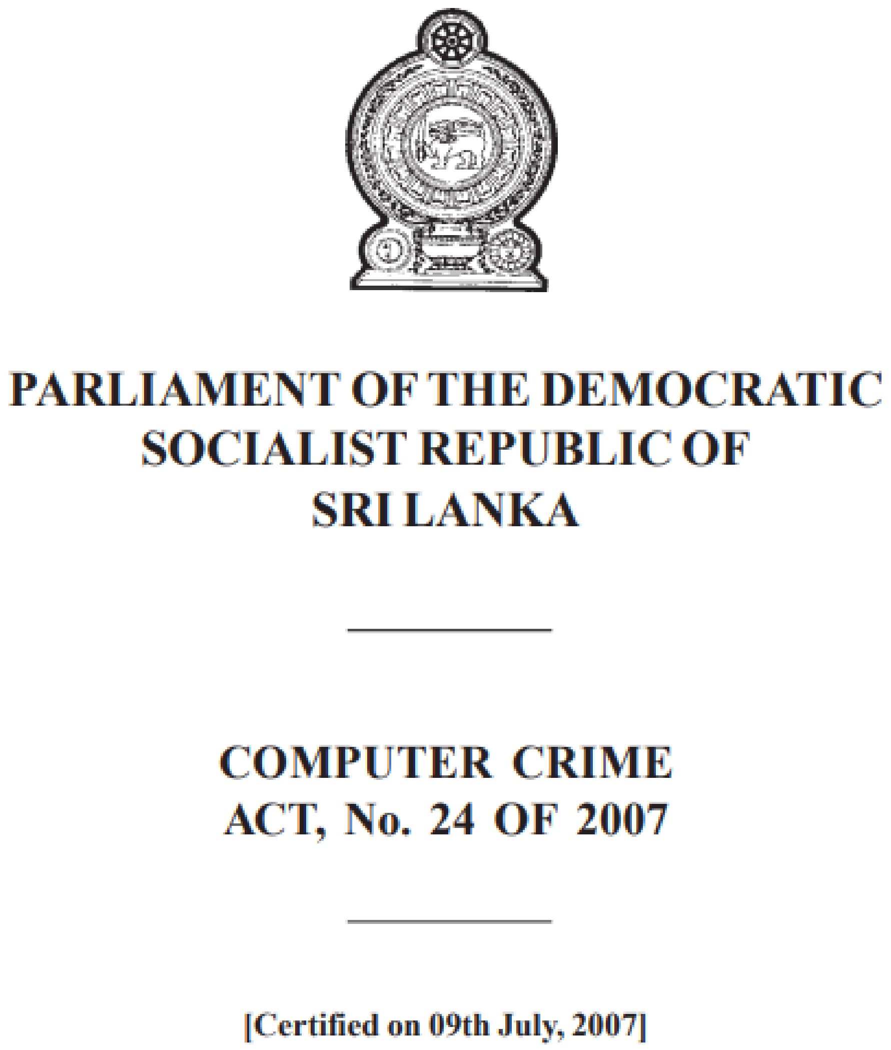
- Computer Crimes Act (2007): Covers hacking, data theft, DoS attacks.
- Electronic Transactions Act (2006): Validates digital documents.
- Payment and Settlement Systems Act: Ensures safe digital financial systems.



PARLIAMENT OF THE DEMOCRATIC
SOCIALIST REPUBLIC OF
SRI LANKA

ELECTRONIC TRANSACTIONS
ACT, No. 19 OF 2006

[Certified on 19th May, 2006]



PARLIAMENT OF THE DEMOCRATIC
SOCIALIST REPUBLIC OF
SRI LANKA

COMPUTER CRIME
ACT, No. 24 OF 2007

[Certified on 09th July, 2007]

# Sri Lanka CERT|CC

- National Computer Emergency Readiness Team.
- Responds to cyber incidents, conducts awareness programs, and offers training.
- Central role in national cybersecurity.
- Website: www.cert.gov.lk

# Budapest Convention on Cybercrime

- Also known as: Convention on Cybercrime or ETS No. 185

- The Budapest Convention on Cybercrime is the first international treaty aimed at combating cybercrime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was adopted by the Council of Europe in Budapest, Hungary, on November 23, 2001, and came into force on July 1, 2004.

**Main Objectives:**

1. 🔐 **Harmonize national criminal laws** related to cybercrime and digital evidence.
2. 👮 **Empower law enforcement** with the legal tools to investigate and prosecute cybercrime.
3. 🌐 **Promote international cooperation** across borders in real-time.
4. 🛡️ **Protect human rights** during the investigation and prosecution of cybercrime.

# Global Cybersecurity Collaboration

- Interpol, Europol, regional CSIRTs share data and lead joint investigations.
- ***Example: Tracking ransomware gangs across countries.***
- Partnerships with tech companies help in quick threat detection and takedown.

# GDPR and Data Protection Laws

- **GDPR (EU):** Requires data consent, rights to users, and breach reporting.
- Similar laws:
  - **CCPA** (California Consumer Privacy Act)
  - **India’s PDP Bill** (Personal Data Protection Bill)
- Purpose: Protect personal data in a digital world.

# Challenges in Enforcing Cyber Laws

- **Jurisdictional Issues**: Crimes cross national boundaries, complicating law enforcement.
- **Rapid Tech Changes**: Law struggles to keep pace.
- **Lack of Skilled Personnel**: Many enforcement agencies lack technical capacity.

# Penalties Under Sri Lankan Law

- **Unauthorized access:** Up to 5 years**.**
- **Data interference:** Up to 7 years.
- **Forgery, fraud:** Heavily penalized.
- Cybercrime is treated seriously under the law.

# Cybersecurity Best Practices

- **Strong Passwords & MFA:** Prevent unauthorized access.
- **Updates & Backups:** Fix vulnerabilities, and recover from attacks.
- **Caution:** Avoid clicking unknown links or sharing private info on social media.

# The Role of IT Professionals

- IT pros are guardians of digital infrastructure.
- Tasks: Secure design, risk assessments, and continuous monitoring.
- Must act ethically and educate others on cyber safety.

# Conclusion: Combatting Cybercrime

- Cybercrime is dynamic and widespread.
- Combating it needs:
  - **Laws** to punish offenders.
  - **Technology** to detect attacks.
  - **Ethics** and **awareness** to reduce human risk.
- Collaboration between individuals, organizations, and governments is crucial.

END