



Cybercrime and Cybersecurity

— Mauritius Police Force

Cybercrime Unit
Central Criminal Investigation Department



Focus Area

Awareness & Sensitisation

April 2026

Contents

01

Understanding Cybercrime

What is cybercrime and why should you care?

03

Phishing & Online Scams

Recognizing and protecting yourself from fraud

05

Cyber Safety Guidelines

Practical do's and don'ts for staying safe online

07

Reporting & Prevention

How to report cybercrime and protect yourself

02

Social Media & AI Threats

Identity theft, deepfakes, and fake profiles

04

Serious Cybercrimes

Understanding the most severe digital offences

06

Mauritian Legislation

Understanding the legal framework and penalties

01

Understanding Cybercrime

What is cybercrime and why should you care?

What is Cybercrime?

Cybercrime refers to criminal activities carried out using computers, networks, or digital devices.

As technology advances, cybercriminals are finding new ways to exploit unsuspecting users. Understanding cybercrime is the first step toward protecting yourself in the digital age.



Criminals

Use technology to commit crimes anonymously



Global Reach

Can target victims from anywhere in the world



24/7 Threat

Attacks can happen at any time, day or night



Protection

Awareness and vigilance are your best defenses



Social Media Awareness

Social media platforms have become an integral part of our daily lives, but they also present **significant security risks**. Cybercriminals use these platforms to gather personal information, impersonate others, and launch various attacks.

Identity Theft

Criminals steal your personal information to create fake accounts and commit fraud

Oversharing

Posting too much personal information makes you vulnerable to targeted attacks

Social Engineering

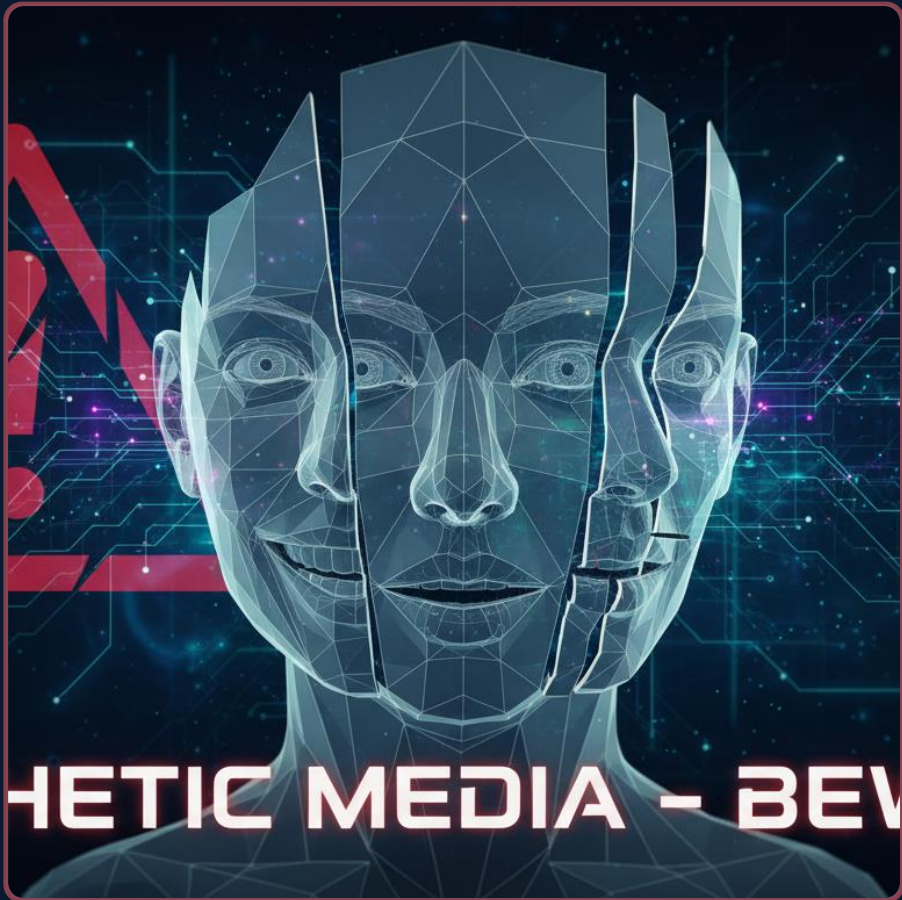
Manipulating users into revealing confidential information through deception

Fake Contests

Scams disguised as contests and surveys designed to harvest your personal data



AI-Generated Content Threats



Artificial Intelligence has made it easier than ever to create **convincing fake content**. These technologies can be misused for fraud, blackmail, and misinformation.



Deepfake Videos

Realistic fake videos that can damage reputations, spread false information, and be used for blackmail



Voice Cloning

AI-generated voices used for impersonation scams, fraudulent phone calls, and voice-based fraud



Fake Images

Generated photos used to create false identities, fake social media profiles, and deceptive content

Misuse of Fake Profiles

Creating and using fake profiles to deceive, defraud, or harm others is a **serious cybercrime**. Under Mauritian law, this offence carries severe penalties.

Romance Scams

Fake profiles used to build romantic relationships and extract money

Financial Fraud

Impersonating others to commit investment and financial scams

Cyberbullying

Anonymous profiles used to harass and intimidate victims

Defamation

Impersonating real people to damage their reputation



Penalty: Fine up to Rs 1,000,000 + Up to 20 years imprisonment



02

Phishing & Online Scams

Recognizing and protecting yourself from digital fraud

Phishing Attacks

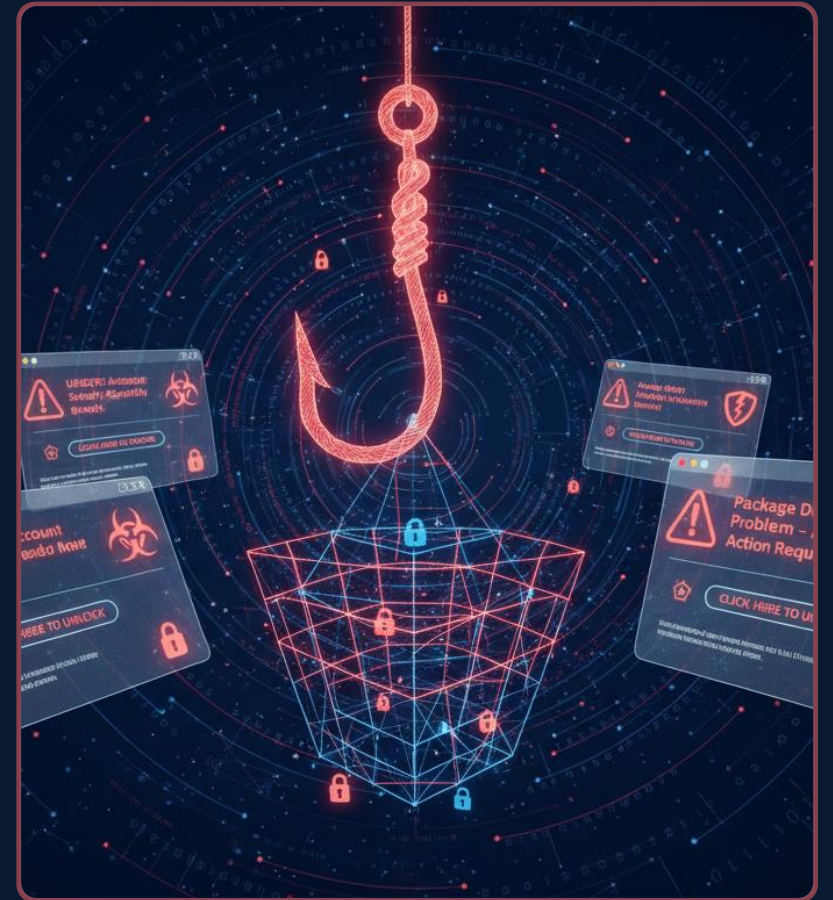
Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity. These attacks typically come via email, SMS, or fake websites.

⚠ Common Phishing Signs

- ✗ Urgent or threatening language
- ✗ Suspicious sender addresses
- ✗ Requests for passwords or PINs
- ✗ Spelling and grammar errors
- ✗ Unexpected attachments
- ✗ Links that don't match the text

🛡 How to Protect Yourself

- ✓ Never click suspicious links
- ✓ Verify sender identity
- ✓ Check website URLs carefully
- ✓ Use multi-factor authentication
- ✓ Keep software updated
- ✓ Report suspicious emails



Investment Scams



Online investment scams promise **high returns with little or no risk**. These schemes often use fake testimonials, professional-looking websites, and pressure tactics to convince victims to invest money.



Guaranteed High Returns

"Get rich quick" promises with minimal risk – if it sounds too good to be true, it probably is



Pressure Tactics

Urgent calls to invest before "missing out" – legitimate investments don't pressure you



Unregistered Investments

Not licensed by Financial Services Commission (FSC) Mauritius – always verify registration

Other Common Online Scams



Online Shopping Scams

Fake websites selling products at unbelievably low prices. They take your money but never deliver the goods.

Protection: Always verify seller reputation and use secure payment methods



Tech Support Scams

Callers claiming your computer has a virus and offering to fix it for a fee. They may install malware or steal data.

Protection: Legitimate companies never call unsolicited – hang up immediately



Lottery & Prize Scams

Notifications of winning prizes you never entered. They ask for fees to "release" your winnings.

Protection: Never pay fees to claim prizes – legitimate lotteries don't ask for money



Romance Scams

Online relationships that lead to money requests. Scammers build trust over time before asking for financial help.

Protection: Be cautious with online acquaintances – never send money to someone you haven't met

03

Serious Cybercrimes

Understanding the most severe digital offences

ALERT

Child Pornography Offences

The production, distribution, and possession of child pornography are among the **most serious cybercrimes**. These offences cause irreparable harm to children and carry severe penalties under Mauritian and international law.

Creating & Producing

Creating explicit images or videos of minors

Distributing

Sharing such content through any platform

Possessing

Having child sexual abuse material

Grooming

Building relationships to exploit minors

Reporting Child Exploitation

- ✓ Report immediately to Police: 999 / 148
- ✓ Do NOT share or forward material
- ✓ Child Development Unit: 113
- ✓ Preserve evidence for investigators



Revenge Pornography



Revenge pornography involves **sharing intimate images or videos without consent**, typically by former partners. This is a criminal offence under the Cybersecurity and Cybercrime Act 2021.



Without Consent

Sharing intimate images without the person's consent is illegal and punishable by law



Intent to Share

Even possessing such content with intent to share is a criminal offence



Victim Rights

Victims can seek removal of content and take legal action against perpetrators



Penalty: Fine up to Rs 1,000,000 + Up to 20 years imprisonment

Cyberbullying

Cyberbullying involves using digital platforms to **harass, threaten, or intimidate others**. This includes posting harmful content, spreading rumours, sending threatening messages, and creating fake profiles to humiliate victims.



Harassing Messages

Sending threatening or abusive messages repeatedly



Spreading Rumors

Sharing false information to damage someone's reputation



Sharing Embarrassing Photos

Posting photos or videos to humiliate someone



Fake Profiles

Creating fake accounts to mock or impersonate victims



Exclusion

Deliberately excluding someone from online groups



Doxxing

Sharing private information without consent



If You Are Being Cyberbullied

Don't respond

Save evidence

Block perpetrator

Report to platform

Talk to someone

Report to police



04

Cyber Safety Guidelines

Practical do's and don'ts for staying safe online



Cyber Safety: Do's

✓ Strong Passwords

Use strong, unique passwords for each account

✓ Two-Factor Auth

Enable 2FA wherever possible

✓ Keep Updated

Keep software and apps updated

✓ Antivirus

Use reputable antivirus software

✓ HTTPS Security

Verify HTTPS before entering data

✓ Backup Data

Regularly backup important data

✓ Log Out

Log out of accounts when finished

✓ Privacy Settings

Review privacy settings on social media

✓ Public Wi-Fi

Be cautious with public Wi-Fi networks

✓ Verify Requests

Verify requests for money or personal info

✓ Report Activity

Report suspicious activity to authorities

✓ Educate Children

Educate children about online safety

✓ Read Terms

Read terms and conditions before agreeing

✓ Secure Payments

Use secure payment methods online

✓ Monitor Finances

Monitor financial statements regularly

Cyber Safety: Don'ts

✗ Share Passwords

Don't share passwords with anyone

✗ Click Suspicious Links

Don't click on suspicious links

✗ Overshare

Don't overshare personal information

✗ Public Computers

Don't use public computers for sensitive transactions

✗ Ignore Warnings

Don't ignore security warnings

✗ Untrusted Sources

Don't download from untrusted sources

✗ Unsolicited Messages

Don't respond to unsolicited messages

✗ Reuse Passwords

Don't use the same password across sites

✗ Leave Unlocked

Don't leave devices unlocked and unattended

✗ Accept Strangers

Don't accept friend requests from strangers

✗ Post Location

Don't post your location in real-time

✗ Share Intimate Photos

Don't share intimate photos, even with trusted partners

✗ Ignore Identity Theft

Don't ignore signs of identity theft

✗ Delay Reporting

Don't delay reporting cybercrime incidents

✗ Believe Everything

Don't believe everything you see online

Password Security Best Practices

🔑 Create Strong Passwords

- ✓ At least 12 characters long – longer passwords are harder to crack
- ✓ Mix character types – uppercase, lowercase, numbers, and symbols
- ✓ Avoid personal information – don't use names, birthdays, or addresses
- ✓ Use passphrases – e.g., "Mauritius@2024!Beach"

🔒 Password Manager Benefits

- ✓ Generates strong passwords – creates complex, unique passwords
- ✓ Securely stores all passwords – encrypted vault for all credentials
- ✓ Auto-fills login credentials – convenient and secure access
- ✓ Alerts for compromised passwords – notifies if passwords are leaked



05

Cybercrime Laws

Understanding the legal framework and penalties in Mauritius



Key Legislation

Mauritius has established **comprehensive legislation** to combat cybercrime and protect citizens in the digital space. Understanding these laws helps you know your rights and the consequences of cyber offences.



Cybersecurity and Cybercrime Act 2021

This is the **primary legislation** addressing cybercrime in Mauritius, replacing the Computer Misuse and Cybercrime Act 2003. It covers a wide range of offences with updated penalties.



Data Protection Act 2017

Governs the collection, processing, and protection of personal data in Mauritius, aligned with international standards including **GDPR principles**.



ICT Act 2001 (Amended 2018)

Addresses offences related to electronic communications, including harassment and offensive content distributed through digital channels.

Penalties for Cybercrime Offences

Offence	Penalty
Unauthorized access to computer data	Fine up to Rs 1,000,000 + Up to 10 years penal servitude
Access with intent to commit offences	Fine up to Rs 1,000,000 + Up to 20 years penal servitude
Unauthorized modification of computer data	Fine up to Rs 1,000,000 + Up to 20 years penal servitude
Cyberbullying	Fine up to Rs 1,000,000 + Up to 20 years imprisonment
Misuse of fake profiles	Fine up to Rs 1,000,000 + Up to 20 years imprisonment
Revenge pornography	Fine up to Rs 1,000,000 + Up to 20 years imprisonment
Cyber extortion	Fine up to Rs 1,000,000 + Up to 20 years imprisonment
Unauthorized disclosure of passwords	Fine up to Rs 1,000,000 + Up to 10 years penal servitude
Unlawful possession of hacking devices	Fine up to Rs 1,000,000 + Up to 10 years penal servitude
Copyright infringement	Fine up to Rs 1,000,000 + Up to 10 years imprisonment
Data Protection Act violations	Fine up to Rs 200,000 + Up to 5 years imprisonment

Offences involving Critical Information Infrastructure **Fine up to Rs 2,000,000 + Up to 25 years imprisonment**

06

Reporting & Prevention

How to report cybercrime and protect yourself

EMERGENCY CONNECT:
SUPPORT & ASSISTANCE



Emergency and Reporting Contacts

If you are a victim of cybercrime or witness suspicious online activity, **report it immediately**. Early reporting increases the chances of apprehending criminals and preventing further harm.



Police Emergency

999 or 112

For immediate emergencies and urgent cybercrime incidents



Police Hotline

208-7015 / 7016

For non-emergency cybercrime reporting and inquiries



Cybercrime Reporting

cybercrime@police.govmu.org

Email for detailed cybercrime reports and evidence submission



Data Protection Office

460-0251 | dpo@govmu.org

For data privacy violations and personal data protection issues



Financial Services Commission

403-7000

For investment scams and unregistered financial schemes



Child Development Unit

113

For child exploitation, online grooming, and child pornography

What to Include in Your Report

Evidence to Preserve

- ✓ Screenshots of messages/posts
- ✓ Website URLs
- ✓ Phone numbers used
- ✓ Date and time of incidents
- ✓ Email headers and content
- ✓ Transaction records
- ✓ Usernames and profile links

Reporting Steps

- 1 Document everything immediately
- 2 Do not delete any evidence
- 3 Contact relevant authorities
- 4 File a formal police report
- 5 Notify your bank (if financial)
- 6 Change compromised passwords
- 7 Monitor accounts for further activity



Prevention is Better Than Cure

By following the guidelines in this presentation, you can **significantly reduce your risk** of becoming a victim of cybercrime.



Think Before You Click

Verify links and attachments before opening them



Protect Personal Info

Share personal information only when necessary



Stay Informed

Cyber threats evolve constantly – keep learning



Trust Your Instincts

If something feels wrong, it probably is



Report Incidents

Help protect others by reporting cybercrime – your report could prevent others from becoming victims



Remember: Your online safety is in your hands



SECURE YOUR TOMORROW

Stay Safe, Stay Secure

Your online safety is in your hands. Stay vigilant, stay informed, and stay safe in the digital world.

Cybercrime Unit
Central CID
Mauritius Police Force
Tel: 2104653 / 2105384
Email: ccu.mpf@govmu.org