Cape Peninsula
University of Technology

PO Box 1906, Bellville, 7535
Symphony Way, Bellville, South Africa
+27 21 959 6767 info@cput.ac.za
www.facebook.com/cput.ac.za www.cput.ac.za

Cyber Security Awareness Guideline

Introduction

Organizations often invest significantly in security technologies, but human factor remains the most vulnerable. Cyber threats frequently target end-users, exploiting a lack of awareness and training. This guideline outlines key security practices every employee must follow to understanding the importance of Cyber Security Awareness and its role in safeguarding personal and organizational assets.

Why is Cyber Security Awareness Important?

The Cyber Security Awareness Program is designed to educate employees and students about their role in mitigating cyber threats. It equips them with knowledge about:

- Social engineering tactics
- Phishing attacks
- Password management
- Protecting data in motion
- Core cyber security concepts, etc.

Key Benefits:

- Identifying potential cyber threats
- Protecting sensitive information
- Reducing risk and associated costs
- Ensuring personal and organizational safety
- Cultivating a culture of cybersecurity awareness

Who Needs It:

- Everyone connected to the internet.

Understanding Cyber Security

Cyber security involves safeguarding systems, networks, processes, devices, programs, and data from malicious attacks. It minimizes risks such as unauthorized information disclosure, theft, and service disruption.

Data That Requires Protection:

- Personally Identifiable Information (PII)
- Education Records
- Financial Information
- Health Records, etc.

Covering the Basics:

Password Hygiene and Authentication Practices

- Select strong, unique passwords (Longer, Numbers, Special Characters)
- Never reuse passwords across multiple platforms
- Enable Multi-Factor Authentication (MFA), where applicable
- Never share your passwords (including with Colleagues, Family, IT Staff, etc.)

Email and Phishing Awareness

- Treat emails from unknown senders with caution, especially those containing links and unexpected attachments
- Verify suspicious messages by contacting the sender through official channels
- Report phishing emails immediately (e.g. Fake V.C emails, Professor emails, etc)

Acceptable Use of Computing Resources

- CPUT computing resources are for staff, students, guests, and service providers (where necessary) for authorised work purposes only.
- CPUT users may not possess, distribute, or send unlawful communications of any kind, or participate or facilitate communications in furtherance of other illegal activities that may bring the establishment into disrepute.
- Unauthorised access or use of university computing resources or data is strictly prohibited.

Device and Workspace Security

- Ensure your screen is locked when leaving your workstation
- Ensure sensitive data is handled and stored securely
- Refrain from installing unauthorised software on CPUT devices
- Keep all computer systems and software updated (incl. portable devices)

Safe Use of Internet and Social Media

- Browse safely and avoid suspicious links
- Verify the website address is correct and secure before making any transactions
- Protect confidential and proprietary information related to CPUT
- Limit the amount of work-related and personal information shared via social media

Working Remotely

- Use VPN when connecting to the university systems (remote desktop where applicable)
- Avoid using public Wi-Fi without protection
- Use university approved tools for collaboration, e.g. Microsoft Teams
- Keep your home router firmware and passwords updated

Combating Cyber Threats

Practical Steps:

- Exercise caution with emails from unfamiliar sources.
- Scrutinize email addresses and sender authenticity.
- Validate urgent requests through official channels.
- Be sceptical of unsolicited offers.
- Stay updated on the latest cyber threats and tactics.

Building Resilience:

- Participate in regular security awareness training.
- Report suspicious activity promptly to the CTS-CSIRT or Service Desk.
- Embrace a culture of vigilance and accountability.
- Enable multi-factor authentication (MFA) for all sensitive accounts.
- Establish protocols to verify payment requests, such as verbal confirmation from the requesting party.

Conclusion

Cybersecurity is not solely a technological challenge but a shared responsibility. By fostering awareness, caution, and staying vigilant, individuals and organizations can effectively counter cyber threats and build a secure digital environment.

Remember: You are the first line of defence, let's work together to ensure a safer future!

Security Incidents Reporting

Report all and any cyber security related incidents to the following:

Cyber security related incidents:

- CTS-CSIRT@cput.ac.za

IT related incidents:

- Tel: 021 959 6407
- CTSSDStaff@cput.ac.za

Institutional Governance Policies

For more on the policies referenced:

1. Information Security Policy: Policy Library - Information Security Policy .pdf - All Documents
2. Acceptable Usage Policy: Policy Library - Acceptable Usage Policy.pdf - All Documents
3. Anti Malware Policy: Policy Library - Anti Malware Policy .pdf - All Documents
4. Social media Policy: Policy Library - SOCIAL MEDIA POLICY.pdf - All Documents

All institutional governance policies are available at:

Policy Library - Documents - All Documents