



Cybersecurity Awareness Month Message to the LSU Community

Think Before You Click: Stop Prioritising Convenience Over Security

By: Director, Information and Communication Technology Services (ICTS)

Lupane State University

October 2026

(a) Introduction: Our Security Is in Our Everyday Choices

As Lupane State University (LSU) joins the global community in commemorating Cybersecurity Awareness Month 2026, it is an opportune moment for every member of the University community to reflect on how our everyday digital decisions affect the security of our institution. This year, our message is simple but powerful: **Think Before You Click: Stop Prioritising Convenience Over Security.**

Universities increasingly depend on digital technologies to support teaching, learning, research, administration, financial management, student services and institutional communication. At LSU, digital systems enable staff and students to access information, collaborate, share knowledge and conduct essential university business. However, the same technologies that create these opportunities also expose the University to cyberattacks, data breaches, fraud, identity theft and other digital risks.

Cybersecurity is therefore not merely a technical responsibility assigned to the ICTS department. It is a shared institutional responsibility that requires informed decisions, responsible behaviour and a commitment to protecting information. Every email opened, link clicked, password entered, document shared and application installed can either strengthen or weaken our collective security.

While ICTS continues to play a central role in safeguarding the University's digital environment, technology alone cannot eliminate cyber risks. The choices we make as users remain a critical line of defence.

(b) The Hidden Danger of Prioritising Convenience Over Security

One of the most persistent cybersecurity challenges is the tendency to prioritise convenience over security. In our busy working and academic environments, we often seek the quickest way to complete a task, sometimes without considering the potential consequences.

We may reuse the same password across several platforms because remembering multiple passwords seems inconvenient. We may share login credentials with a colleague to save time, postpone software updates because they interrupt our work, disable security controls because they appear restrictive, or send confidential documents through personal email or unauthorised messaging platforms because these are readily accessible.

Although these shortcuts may seem harmless, they can create opportunities for cybercriminals to gain unauthorised access to institutional systems and information.

Consider an employee who shares their password with a colleague to facilitate access to a university system. If that password is subsequently compromised, it may be difficult to determine who accessed the system or performed a particular action. Similarly, a student who uses the same password for university services and an unrelated online platform may expose their university account if that external platform suffers a data breach.

Convenience can also influence how we respond to suspicious messages. A message claiming that an account will be suspended unless a link is clicked immediately may trigger panic and lead a user to disclose their credentials. An unexpected request for urgent payment or confidential information may appear legitimate, particularly when it seems to come from a senior university official.

Cybercriminals understand these human tendencies and deliberately exploit urgency, fear, curiosity, trust and the desire to get things done quickly.

At LSU, we must recognise that a few seconds saved through an insecure shortcut can result in significant financial losses, compromised personal information, disrupted university services and reputational damage. Security must therefore be considered an essential part of getting work done, rather than an obstacle to productivity.

(c) Artificial Intelligence: Opportunities Accompanied by New Risks

Artificial intelligence (AI) is transforming education, research, communication and administration. It offers opportunities to improve productivity, support teaching and learning,

analyse information and automate routine tasks. Nevertheless, the growing adoption of AI also introduces cybersecurity, privacy and ethical challenges that require careful management.

Cybercriminals can use AI tools to create convincing phishing messages, impersonate trusted individuals, automate scams and produce misleading content on a scale that would previously have been difficult to achieve. Messages that contain correct grammar, professional language and personalised information can no longer be assumed to be genuine simply because they appear well written.

Members of the LSU community should also exercise caution when using publicly available AI platforms. Uploading student records, staff information, examination materials, research data, financial records, passwords or confidential institutional documents into an unapproved AI tool may expose information to unauthorised processing or disclosure.

Before using an AI application, users should consider whether the information they intend to submit is confidential, whether the tool is approved for the intended purpose, and whether its use complies with university policies and applicable data protection requirements.

AI-generated information must also be reviewed for accuracy, bias and reliability. AI systems can produce incorrect facts, misleading explanations and fabricated references. In academic and administrative settings, accepting such information without verification can undermine the quality and integrity of institutional work.

AI should be used to support human judgement, not replace it. The responsible adoption of AI requires users to understand both its benefits and its limitations.

(d) Deepfakes: When Seeing and Hearing Are No Longer Enough

Deepfakes are digitally manipulated or AI-generated images, videos and audio recordings designed to make people appear to say or do things they never said or did. These technologies can imitate a person's face, voice or mannerisms with increasing realism.

For a university community, deepfakes present serious risks because they can be used to impersonate university management, lecturers, students, finance officers or other trusted individuals.

Imagine receiving a voice message that appears to come from a senior university official instructing you to make an urgent payment. Alternatively, imagine watching a video that appears to show a university leader announcing a major policy change or disclosing confidential information. Without independent verification, a recipient may accept the content as authentic and act on it.

Deepfakes can facilitate financial fraud, misinformation, reputational attacks, harassment and identity theft. They can also be used to manipulate public opinion, damage professional relationships and undermine confidence in legitimate institutional communication.

Members of the LSU community must therefore develop a habit of verifying unusual requests, even when they appear to come from familiar people. A phone call, voice note, video or email should not automatically be treated as proof of identity.

Where a request involves money, passwords, sensitive information or unusual instructions, verify it through a separate, trusted communication channel. Do not rely solely on the contact details or links contained in the suspicious message.

We must also avoid creating, sharing or distributing manipulated images, recordings or videos of others without appropriate authorisation. The ability to create convincing digital content does not remove our responsibility to respect privacy, dignity and truth.

(e) Emerging Cyber Threats: Staying Alert in a Changing Digital Environment

Cyber threats continue to evolve as institutions adopt cloud services, online collaboration platforms, mobile applications and interconnected digital systems. While traditional threats remain relevant, users must also be alert to changing attack methods :

- **Phishing and targeted impersonation:** Cybercriminals send fraudulent messages designed to steal passwords, obtain personal information or persuade recipients to perform unauthorised transactions. Some attacks are carefully tailored to a particular individual, department or institution.
- **Ransomware:** Malicious software can encrypt files or disrupt access to systems, with attackers demanding payment for recovery. Such incidents may interrupt examinations, e-learning, admissions, payroll and other essential university operations.
- **Account takeover and identity theft:** Stolen credentials can enable criminals to access email accounts, impersonate legitimate users, obtain confidential records or conduct fraudulent transactions.
- **Business email compromise and payment fraud:** Attackers may impersonate university officials, suppliers or business partners to manipulate staff into changing payment details, disclosing sensitive information or transferring funds to fraudulent accounts.
- **Malicious applications and unsafe downloads:** Installing unauthorised software, opening suspicious attachments or connecting unknown storage devices can introduce malware into personal devices and institutional networks.
- **Social engineering and messaging scams:** Fraudulent requests can arrive through email, SMS, WhatsApp, social media or telephone calls. A familiar communication platform does not guarantee that a message or sender is trustworthy.
- **Cloud and third-party risks:** Weak passwords, inappropriate sharing permissions and insecure external services can expose institutional information beyond its intended audience.

These threats demonstrate why cybersecurity cannot depend on recognising a single type of suspicious email. Users must adopt a consistent approach to verification, access control, secure information handling and incident reporting.

(f) Digital Ethics and the Responsible Use of Technology

Cybersecurity is not only about protecting computers and networks; it is also about how we treat people, information and technology in the digital environment. Digital ethics requires us to consider the consequences of our online actions and to respect the rights and responsibilities of others.

At LSU, responsible digital conduct means protecting personal information, respecting confidentiality, using university systems for authorised purposes and avoiding activities that compromise the security or integrity of institutional resources.

Staff and students must not access records without authorisation, share confidential information indiscriminately, misuse another person's account, interfere with institutional data or use digital platforms to harass, threaten or defame others.

The responsible use of technology also requires respect for intellectual property, academic integrity and the privacy of colleagues and students. AI tools should not be used to facilitate plagiarism, fabricate evidence, misrepresent authorship or generate deceptive content.

Before sharing information online, users should ask themselves three questions:

1. **Is it appropriate?** Do I have a legitimate reason and the necessary authority to access or share this information?
2. **Is it secure?** Am I using an approved platform and appropriate safeguards to protect the information?
3. **Is it ethical?** Could my action violate another person's privacy, mislead an audience or harm the University?

Our digital behaviour should reflect the same standards of professionalism, honesty and accountability that guide our conduct in the physical workplace and learning environment.

(g) Practical Steps Every LSU Community Member Should Take

Building a secure digital culture begins with practical actions that each person can adopt immediately :

- i. **Use strong, unique passwords.** Avoid predictable passwords and do not reuse passwords across different accounts. Use an approved password manager where available, and enable multi-factor authentication whenever supported.
- ii. **Never share passwords or verification codes.** Legitimate colleagues should use their own authorised accounts. No request for convenience should justify compromising account security.
- iii. **Think before clicking.** Check unexpected links, attachments and requests for information. Verify unusual messages through trusted channels before taking action.
- iv. **Keep devices and software updated.** Install authorised security updates promptly. Updates often address vulnerabilities that attackers may exploit.
- v. **Use approved systems and applications.** Avoid unauthorised software, unapproved cloud storage and insecure methods of transferring institutional information. Consult ICTS when uncertain about the suitability of a tool.
- vi. **Protect personal and institutional information.** Share information only with authorised recipients and only when necessary. Double-check email addresses, recipients and attachments before sending messages. Lock devices when unattended and secure portable storage.
- vii. **Apply caution when using AI.** Do not submit confidential or personal information to unapproved AI services. Verify AI-generated content before relying on it or sharing it.

- viii. **Verify identities and unusual requests.** Independently confirm requests involving payments, changes to banking details, access credentials or sensitive information, even when the sender appears familiar.
- ix. **Report suspected incidents promptly.** If you click a suspicious link, disclose credentials, lose a device or suspect that information has been exposed, notify ICTS through the University's designated reporting channels without delay. Early reporting can limit the damage. Do not conceal incidents out of embarrassment or fear.
- x. **Respect university policies and data protection requirements.** Handle personal information lawfully and securely, limit access to authorised users, retain information appropriately and dispose of it securely.

These measures are not intended to make digital work unnecessarily difficult. They are intended to ensure that our use of technology remains productive without exposing ourselves or the University to avoidable risks.

(h) The Role of ICTS in Strengthening Cybersecurity at LSU

The ICTS department recognises that sustainable cybersecurity requires a combination of appropriate technical safeguards, clear institutional practices and continuous user awareness. It is therefore important that cybersecurity becomes part of the University's everyday working culture rather than an issue considered only after an incident occurs.

As part of its commitment to strengthening cybersecurity awareness, ICTS is promoting a more proactive and shared approach to protecting LSU's digital environment. This includes encouraging responsible user behaviour, reinforcing secure information-handling practices and highlighting the importance of compliance with institutional requirements and Zimbabwe's Cyber and Data Protection Act (CDPA) and Cyber and Data Protection Regulations (CDPR).

A key planned initiative is the **training of Cybersecurity and Data Protection Champions across the University community.**

The proposed champions initiative is intended to strengthen awareness beyond the ICTS department by developing a network of informed individuals who can help promote good cybersecurity and data protection practices within their respective departments, faculties, units and student communities, as appropriate.

Through this initiative, champions are expected to help colleagues and fellow students recognise common threats, understand their responsibilities, handle information securely and appreciate the importance of reporting suspicious activity. They can also help reinforce awareness messages and encourage responsible technology use in everyday university activities.

The initiative will support the development of a culture in which cybersecurity and data protection are understood as shared responsibilities rather than duties belonging exclusively to technical personnel.

ICTS will continue to encourage users to seek guidance when uncertain about security requirements and to report potential incidents promptly through designated institutional channels. The effectiveness of these efforts, however, depends on the willingness of every staff member and student to participate actively and apply what they learn.

Cybersecurity awareness must be continuous. As threats evolve, our knowledge, habits and institutional responses must evolve with them.

(i) Cybersecurity and Data Protection: A Shared Institutional Responsibility

The University's information assets include student records, staff information, examination data, research outputs, financial information, login credentials and confidential institutional documents. Protecting these assets is essential to maintaining trust, safeguarding privacy, ensuring continuity of operations and preserving LSU's reputation.

Zimbabwe's Cyber and Data Protection Act and its associated Regulations reinforce the importance of responsible handling and protection of personal information. Negligent or unlawful practices may expose individuals and institutions to investigations, regulatory consequences, financial losses, disciplinary action and reputational harm, depending on the circumstances and applicable requirements.

Compliance should not be viewed merely as a legal obligation. It is an expression of our commitment to respecting the people whose information we collect, use, store and share.

Every member of the University community has a role to play in ensuring that personal and institutional information is accessed only for legitimate purposes, disclosed appropriately and protected against unauthorised access, alteration, loss or destruction.

By combining responsible individual behaviour with effective institutional safeguards, LSU can reduce avoidable risks and build confidence in its digital services.

(j) Conclusion: Make Security Part of Every Decision

As we commemorate Cybersecurity Awareness Month 2026, let us recognise that the security of Lupane State University depends not only on the technologies we deploy but also on the decisions we make every day.

Prioritising convenience over security may save a few moments, but the consequences of an insecure shortcut can be far-reaching. A shared password, an unverified payment request, an unsafe application or a careless disclosure of personal information can create opportunities for cybercriminals and expose the University to significant harm.

Artificial intelligence, deepfakes and emerging cyber threats make vigilance more important than ever. At the same time, digital ethics and responsible technology use must guide how we interact with information, systems and one another.

Through the efforts of ICTS, the planned training of Cybersecurity and Data Protection Champions, and the active participation of staff and students, LSU can continue building a stronger culture of cybersecurity awareness, accountability and trust.

Let us make a conscious choice to verify before we trust, protect before we share, update before we postpone, and report before a small incident becomes a major crisis.

Remember: Cybersecurity is everyone's responsibility. Convenience is optional; security is essential. Think before you click. Protect your account. Protect personal information. Protect LSU.

A handwritten signature in purple ink, appearing to read 'M. Sibanda', with a small red mark above the first 'M'.

Eng. M. Sibanda