UNISA

CYBERSECURITY EDUCATION & AWARENESS TRAINING

CYBER ALERT! STAY SAFE THIS BLACK FRIDAY & CYBER MONDAY!

As we enter the busy online shopping season, Black Friday and Cyber Monday present a golden opportunity—not just for shoppers, but also for scammers. Cybercriminals are increasingly targeting individuals with **phishing emails**, **fake online stores**, and **malicious links**. The increase in online purchases and time-sensitive deals elevates the risks, underscoring the importance of being watchful and practicing effective cybersecurity.

WHAT DOES THIS MEAN FOR THE UNISA COMMUNITY?

Staff, students, and faculty are urged to remain vigilant in protecting their personal information, financial data, and university systems. A lapse in attention might result in identity theft, compromised accounts, or malware breaches within the networks.

	1. **Verify website authenticity:** Only interact with websites that are officially trusted websites. Look for **HTTPS** in the **URL** and double-check the domain.
	2. **Enable MFA:** Activate MFA on all accounts to add an extra layer of security, ensuring that even if login credentials are compromised, unauthorized access is prevented.
	3. **Use Long & Complex Passwords:** Consider using **16 characters**, the longer the better, never reuse or store passwords on websites, and reset your password monthly. Ensure that MFA is enabled wherever possible.
http://www.	4. **Avoid Clicking Suspicious Links:** Never click links in unsolicited emails or social media ads. Instead, navigate directly to the **retailer's** official site.
	5. **Keep software and devices updated:** Ensure software is up to date to mitigate vulnerabilities that attackers may exploit.

REPORT SUSPICIOUS ACTIVITY

If you suspect fraud or need assistance, contact:

Maximo Log: Self-service ☎ 012 429 4125

You can access the Terranova training platform via this link.