BUSINESS TIPS FOR Black Friday CYBER SECURITY

WHY ITS RISKY:

- Spike in transactions: Increased payment processing creates more opportunities for fraud.
- Phishing surge: Cybercriminals exploit the season with fake deals and emails.
- Website vulnerabilities: Heavy traffic can expose weaknesses.

WATCH OUT FOR:

- Too good to be true offers: Often a lure for phishing scams.
- Unusual login attempts: Especially from unfamiliar locations or devices.
- Fake customer service requests: Attackers may impersonate customers to gain access.

BUSINESS TIPS & BEST PRACTICES

Educate your team: Train staff to spot phishing emails and suspicious links. It is important in these discussion:

- Explain common malicious contact tactics, such as urgency and fear mongering in emails, slight URL variations, attachments and links.
- Teach verification steps, checking sender details and red flags in content.
- Encourage reporting and sharing as soon as something seems wrong. If a team member has noticed an issue, ensure staff have an active elevation plan and make sure they know who to communicate with.

Update systems: Ensure all software, plugins, and payment gateways are patched and up to date.

Enable Multi-Factor Authentication (MFA): Add an extra layer of security for logins.

Monitor transactions and secure your website: Use fraud detection tools to flag unusual activity, https, firewalls, and vulnerability scans.

Backup critical data: In case of ransomware or outages, backups keep you operational.