CyberShield SME Assistant - Frequently Asked Questions

🔐 Basic Security Setup

Q: What are the essential cybersecurity measures every SME should implement immediately?

A: Start with these five critical steps:

1. Enable multi-factor authentication (MFA) on all business accounts
2. Install and maintain updated antivirus software on all devices
3. Implement a robust backup strategy (3-2-1 rule: 3 copies, 2 different media, 1 offsite)
4. Train employees on basic cybersecurity awareness
5. Keep all software and systems updated with latest security patches

Q: How much should a small business budget for cybersecurity?

A: SMEs should allocate 3-7% of their IT budget to cybersecurity, or approximately $500-2000 per employee annually. Start with free/low-cost solutions and scale up as your business grows.

Q: What's the difference between antivirus and anti-malware software?

A: Antivirus protects against traditional viruses, while anti-malware covers broader threats including spyware, ransomware, and trojans. Modern solutions often combine both. For SMEs, comprehensive endpoint protection suites are recommended.

📧 Email Security

Q: How can SMEs protect against phishing attacks and email-based threats?

A: Implement these email security measures:

- Use email filtering and anti-phishing solutions
- Train employees to identify suspicious emails
- Implement DMARC, SPF, and DKIM email authentication
- Never click links or download attachments from unknown senders
- Verify requests for sensitive information through separate communication channels

Q: What should I do if an employee clicks a phishing link?

A: Take immediate action:

1. Disconnect the affected device from the network
2. Change passwords for all accounts accessed from that device
3. Run a full system scan for malware
4. Monitor accounts for unusual activity
5. Report the incident to your IT support or cybersecurity provider

Q: How do I secure my business email accounts?

A: Follow these steps:

- Enable two-factor authentication (2FA)
- Use strong, unique passwords
- Regularly review and remove unused email accounts
- Configure email encryption for sensitive communications
- Set up email retention policies

💰 Budget-Friendly Solutions

Q: What are cost-effective cybersecurity solutions for small businesses with limited budgets?

A: Focus on these affordable options:

- Free antivirus solutions (Windows Defender, Avast Business)
- Cloud-based backup services ($5-15/month)
- Password managers ($3-8/user/month)
- Employee training through free online resources
- Basic firewall (often built into routers)
- Regular software updates (free but critical)

Q: Can I get enterprise-level security without an IT department?

A: Yes! Use managed security services:

- Cloud-based security platforms with 24/7 monitoring
- Managed detection and response (MDR) services
- Security-as-a-Service providers
- Automated security tools with minimal configuration required

Q: What free cybersecurity tools should every SME use?

A: Essential free tools include:

- Microsoft Defender (Windows)
- Google Workspace security features

- Have I Been Pwned (breach monitoring)
- VirusTotal (file scanning)
- OpenVPN (secure remote access)
- KeePass (password management)

🚨 Incident Response & Recovery

Q: What should I do if I suspect a data breach?

A: Follow this incident response plan:

1. **Immediate containment**: Isolate affected systems
2. **Assessment**: Determine scope and impact
3. **Notification**: Inform stakeholders, customers, and authorities as required
4. **Documentation**: Record all actions taken
5. **Recovery**: Restore systems from clean backups
6. **Prevention**: Implement measures to prevent recurrence

Q: How do I recover from a ransomware attack?

A: Never pay the ransom. Instead:

1. Disconnect infected systems immediately
2. Report to law enforcement and cyber authorities
3. Restore from clean, verified backups
4. Patch vulnerabilities that allowed the attack
5. Strengthen security measures before going back online

Q: Do I need cyber insurance for my small business?

A: Highly recommended. Cyber insurance helps cover:

- Data recovery costs
- Business interruption losses
- Legal fees and regulatory fines
- Customer notification expenses
- Reputation management Cost ranges from $500-3000 annually for most SMEs.

🔒 Data Protection & Privacy

Q: How do I protect customer data and comply with privacy regulations?

A: Implement these data protection measures:

- Data encryption (at rest and in transit)
- Access controls and user permissions
- Regular data audits and inventory
- Privacy policy and consent management
- Secure data disposal procedures
- Employee training on data handling

Q: What is the minimum data I should encrypt?

A: Always encrypt:

- Customer personal information (PII)
- Financial data and payment information
- Employee records and HR data
- Business-critical intellectual property
- Any data stored on portable devices

Q: How long should I keep customer data?

A: Follow these guidelines:

- Keep only data necessary for business purposes
- Establish clear retention periods (typically 3-7 years for financial records)
- Regularly purge outdated information
- Comply with industry-specific regulations
- Document your data retention policies

👥 Employee Training & Awareness

Q: How often should I conduct cybersecurity training for employees?

A: Implement ongoing training:

- Initial comprehensive training for new hires
- Quarterly refresher sessions
- Monthly security tips and updates
- Immediate training after security incidents
- Annual phishing simulation tests

Q: What topics should employee cybersecurity training cover?

A: Essential training topics:

- Password security and management
- Phishing and social engineering recognition

- Safe internet browsing practices
- Mobile device and remote work security
- Incident reporting procedures
- Data handling and privacy practices

Q: How do I create a security-conscious culture in my small business?

A: Foster security awareness through:

- Leadership commitment and example
- Regular communication about security importance
- Recognition for good security practices
- Easy reporting of security concerns
- Integration of security into daily operations

🌐 Remote Work & Mobile Security

Q: How do I secure remote workers and mobile devices?

A: Implement remote work security:

- VPN for secure network access
- Mobile device management (MDM) solutions
- Endpoint security software on all devices
- Secure cloud storage and collaboration tools
- Clear remote work security policies

Q: What are the security risks of BYOD (Bring Your Own Device) policies?

A: BYOD risks include:

- Uncontrolled access to company data
- Mixing personal and business information
- Difficulty enforcing security policies
- Challenges in remote device management Mitigate with MDM solutions and clear usage policies.

🏢 Industry-Specific Questions

Q: Are there specific cybersecurity requirements for my industry?

A: Many industries have specific regulations:

- **Healthcare**: HIPAA compliance

- **Finance**: PCI DSS for payment processing
- **Legal**: Attorney-client privilege protection
- **Manufacturing**: Industrial control system security
- **Retail**: Customer payment data protection Consult industry-specific guidelines and compliance requirements.

Q: How do cybersecurity requirements differ for e-commerce businesses?

A: E-commerce requires additional focus on:

- Payment card industry (PCI DSS) compliance
- SSL certificates and secure payment processing
- Customer account security
- Website security and regular penetration testing
- Secure customer data storage

🔍 Threat Detection & Monitoring

Q: How can I monitor for cyber threats without dedicated IT staff?

A: Use automated monitoring solutions:

- Security information and event management (SIEM) tools
- Network monitoring services
- Endpoint detection and response (EDR) solutions
- Cloud-based threat intelligence services
- Managed security service providers (MSSPs)

Q: What are the warning signs of a potential cyberattack?

A: Watch for these indicators:

- Unusual network activity or slow performance
- Unexpected pop-ups or system messages
- Files appearing, disappearing, or being modified unexpectedly
- Unauthorized access attempts in logs
- Employees reporting suspicious emails or activities

💡 Advanced Security Measures

Q: Should small businesses use AI-powered cybersecurity tools?

A: AI-powered tools offer benefits:

- Automated threat detection and response
- Behavioral analysis for anomaly detection
- Reduced false positives
- 24/7 monitoring capabilities Many affordable AI-based solutions are now available for SMEs.

Q: How do I implement zero-trust security in a small business?

A: Start with basic zero-trust principles:

- Verify every user and device before access
- Implement least-privilege access controls
- Monitor and log all network activity
- Use multi-factor authentication everywhere
- Segment your network and systems

🔄 Maintenance & Updates

Q: How do I maintain cybersecurity over time?

A: Establish regular maintenance:

- Monthly security updates and patches
- Quarterly security assessments
- Annual penetration testing or security audits
- Continuous employee training
- Regular backup testing and recovery drills

Q: What should be included in a cybersecurity policy for SMEs?

A: Your policy should cover:

- Acceptable use of company technology
- Password requirements and management
- Email and internet usage guidelines
- Incident reporting procedures
- Remote work security requirements
- Data classification and handling procedures

Contact Info

Bot:
Please **report the incident immediately** to the Communications Authority of Kenya:

+254 703 042 700
incidents@ca.go.ke www.ca.go.ke