

HOW TO PROTECT YOUR \$H1T

A BUSINESSES GUIDE TO CYBERSECURITY



KTI
KEARNS TECHNOLOGY INC

BUSINESS CYBER SECURITY CHECKLIST

Protecting your business from cyber threats doesn't have to be complicated or overwhelming. This comprehensive cybersecurity checklist is your roadmap to safeguarding your digital assets, giving you peace of mind and a solid defense against potential online risks. We've designed this resource to be straightforward and actionable, breaking down complex security concepts into clear, manageable steps that any business can implement.

[Quick Tips for Using This Checklist](#)

- Review each section carefully and check off items as you complete them
- Don't feel pressured to implement everything at once - progress is progress!
- Pay special attention to areas like employee training, device security, and backup systems

[Need extra support?](#)

Our team at Kearns Technology Inc is always here to help. If you find yourself feeling uncertain about any aspect of cybersecurity or want a professional review of your current protections, we're just a **call (866 853 2767)** or **email (cybersafe@kearnstechnology.com)** away.

Our experts can provide personalized guidance tailored to your specific business needs, ensuring you have the most robust defense possible



BUSINESS CYBER SECURITY CHECKLIST



Asset Management

- Create an inventory of all physical and digital assets



Incident Response

- Develop and regularly update an incident response plan



Access Control

- Review and update user accounts and security groups
- Limit access to sensitive data on a need-to-know basis
- Implement strong password policies and use a password manager



Data Protection

- Encrypt sensitive data both at rest and in transit
- Implement Data Loss Prevention (DLP) tools
- Regularly backup data using the 3-2-1 rule



Software and Device Management

- Keep all software and operating systems up-to-date
- Install and maintain antivirus/anti-malware software
- Secure mobile devices used for business



Email Security

- Implement email encryption and threat scanning tools
- Train employees to recognize phishing attempts



Network Security

- Install and maintain firewalls
- Secure your Wi-Fi network



Employee Training

- Establish clear security policies and procedures
- Educate staff on cybersecurity best practices

