CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

The 14 Critical Cyber Mistakes Small Business Owners Make

Every day, small business owners and decision-makers face a myriad of security and resiliency challenges. From natural disasters like fires and hurricanes to public health crises such as COVID-19, these threats are often top of mind. However, one of the most significant risks to their business lies in a less obvious place: the digital devices they use daily. The 2×4 inch screen in their pocket or the 1×1.5 foot slab of circuits beside their desk can pose a far greater threat than any old-school thief breaking into a storefront. Cyberthieves operate from anywhere in the world, using just their fingers and laptops, often leaving no trace and facing little chance of being caught. In an era where digital security is paramount, many small business owners fail to utilize even the basic cybersecurity measures available to them, leaving their businesses vulnerable to attack. This article highlights the 14 critical cyber mistakes that most small business owners make and offers practical advice on how to avoid them.

Using Simple Passwords or the Same Password Everywhere

A common mistake is using simple or repetitive passwords across multiple accounts. Cybersecurity experts recommend creating complex passwords—ideally, 14 characters or longer, incorporating a mix of letters, numbers, and symbols. This approach significantly increases the difficulty for hackers attempting to breach accounts through brute force attacks. Additionally, each account should have a unique password. This precaution ensures that if one account is compromised, the others remain secure.

Not Configuring Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring two or more verification factors to gain access to an account. This could include something you know (like a password), something you have (like a phone), or something you are (like a fingerprint). Enabling MFA on email, social media, banking, and other critical accounts greatly reduces the risk of unauthorized access, even if a password is compromised.

Conducting Business on Open Public WiFi

Using open public WiFi for business transactions, especially those involving sensitive information, exposes your data to potential interception by cybercriminals. It’s akin to broadcasting your confidential information. Whenever possible, use secure, private networks and consider utilizing a Virtual Private Network (VPN) to encrypt your internet traffic.

Skipping Antivirus Software

Antivirus software is a fundamental line of defense against malware and viruses. Ensuring that all business computers have current antivirus software installed and operational is crucial for detecting and neutralizing threats before they can cause damage.

Ignoring Updates

Software and hardware manufacturers regularly release updates that include security patches to fix vulnerabilities. Failing to install these updates leaves systems exposed to known exploits that hackers can use. Setting monthly reminders to check and apply updates can help maintain security.

Failing to Back Up Data

Data loss can be catastrophic for a business. Regular data backups are essential for protecting against data loss due to cyberattacks, hardware failures, or accidental deletions. Cloud-based backups are an affordable and efficient solution, offering easy recovery options in the event of a disaster.

Falling for Phishing Scams

Phishing remains the primary method cybercriminals use to steal information. These scams often involve deceptive emails or websites designed to trick users into providing sensitive information. Business owners and employees should be trained to recognize phishing attempts, such as scrutinizing email addresses, avoiding clicking on unknown links, and verifying the authenticity of requests for information.

Overlooking Security Training for Employees

Employees are often the first line of defense against cyber threats. Regular training sessions on cybersecurity best practices can help prevent many common security breaches. This training should cover the importance of strong passwords, recognizing phishing attempts, and the proper handling of sensitive information.

Neglecting to Secure Mobile Devices

Mobile devices, like smartphones and tablets, are frequently used for business purposes and often contain sensitive data. Ensuring these devices are secured with strong passwords, encryption, and the ability to remotely wipe data in case of loss or theft is crucial.

Using Outdated Software

Outdated software can contain vulnerabilities that are well-known to hackers. Regularly updating all business software, including operating systems, applications, and plugins, helps protect against these vulnerabilities.

Not Implementing a Firewall

A firewall serves as a barrier between your internal network and external threats. It helps prevent unauthorized access and can be configured to block suspicious activity. Implementing a robust firewall solution is a fundamental step in protecting your business network.

Sharing Passwords

Sharing passwords increases the risk of them being compromised. If password sharing is necessary, it should be done using secure methods, such as a reputable password manager, which can store and share passwords securely.

Not Monitoring Network Activity

Regularly monitoring network activity can help detect unusual patterns that may indicate a security breach. Early detection is crucial for mitigating the impact of an attack, allowing for swift action to contain and resolve the issue.

Ignoring Cyber Insurance

Cyber insurance can provide a safety net in the event of a cyberattack, covering costs related to data breaches, business interruption, and recovery efforts. While it’s not a substitute for robust cybersecurity measures, it is an essential component of a comprehensive risk management strategy.

In today’s digital age, the threats posed by cybercriminals are ever-present and evolving. Small business owners must prioritize cybersecurity, not just as a technological necessity but as a critical component of business resilience. By avoiding these 14 common cyber mistakes, businesses can significantly reduce their risk of falling victim to cyberattacks. Implementing strong passwords, enabling MFA, securing mobile devices, and staying vigilant against phishing attempts are just a few of the many steps that can safeguard your business. With the right measures in place, small businesses can protect their valuable assets and maintain customer trust in an increasingly interconnected world. Stay proactive, educate your team, and make cybersecurity a priority to ensure the long-term success and safety of your business.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060

© Copyright 2025 Cannabis Risk Manager. All Rights Reserved