UNCUT LAB | YOUR DIGITAL SPACE FORCE

MAY 2022

8 STEPS TO BETTER CYBERSECURITY

A MESSAGE FROM THE UNCUT LAB TEAM

The rules of business in all industries have already been rewritten in the age of COVID-19. When it comes to small-scale brick and mortar retail along with big-box retailers, the decline is very apparent.

According to Ibis Industry Reports, specialty retail and cannabis are weathering the storm brought on by COVID 19 better than the aforementioned sectors of retail. So what does that mean for you if you are a specialty retailer or cannabis business? Well, the future is brighter for you, but still unclear.

So to weather the next wave of economic upheaval, you must persevere and stand out! In this unbelievably brutal market, you must adapt to a new set of rules to stay on top. In this ebook, we have laid out some helpful tips that we have learned from our partners, through extensive market research, and case studies. We compiled the following information to help specialty and cannabis retailers harness the power of this moment in history.

This ebook of hacks covers a wide range of topics related to technology, eCommerce, and software management for small-scale retailers in the cannabis industry specifically, and specialty retail, generally. For a deeper dive into some of the topics outlined in this ebook, visit our blog for updated articles and spirited debates. Thank you for taking the time to check out the resource.

8 STEPS TO BETTER CYBERSECURITY

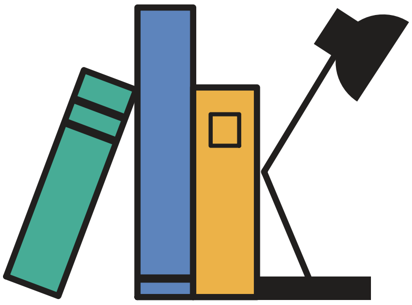
As of 2021, the average cost of a data breach for any company is $4.24 million. In a global recession and for newer or smaller cannabis businesses, this could mean an incredible financial disaster. A business can not only end up losing customers' personal information, but it would have to pay obscene amounts of money to regain access to their systems or fix the breach.

Cyber threats are no longer an aspect of business you can ignore, especially if you are in the cannabis industry. Why? Because most of the cybercriminals love the cannabis operations since they are fairly young and the businesses are simply unprepared in the worst cases, or unprepared in the best cases, for cyberattacks.

In light of this, we've devised this list of basic cybersecurity strategies to make it more difficult for hackers and criminals to steal vital data from your business.

STEP 1: Educate Yourself & Your Employees About Cybersecurity

The first step is to educate yourself and your employees about the nature of these threats so they are aware of the cyber risks all around them. The more you knows about cyber security, the better equipped you will be to protect your cannabis or specialty retail business.



It may seem like a daunting task at first glance, but this single step can help you stay protected and informed.
Make sure everyone in your company knows how to spot a phishing attack, for example, and knows how to deal with suspicious emails or attachments.

STEP 2: Put Antivirus Software on All Devices

This should be a basic step not just for cannabis retail owners, but private citizens as well. Every device you own should have antivirus software or an antivirus app on it. Antivirus programs can scan every file for viruses, adware, spyware, ransomware, and more. They can also provide real-time protection from such threats, preventing cyber criminals from entering your systems.

Luckily, there are plenty of business plans from antivirus app developers and software providers that are fairly affordable. You might even get antivirus protection on all your devices, such as laptops, tablets, and smartphones.

STEP 3: Keep all your cybersecurity software up-to-date and scan regularly

Updating your software can be inconvenient, but as often as we figure out ways to defend ourselves from cybercriminals, those same criminals come up with new viruses and new ways to steal and destabilize business operations and private life.

Security experts recommend that keeping your security systems up-to-date can protect you from all the latest threats.
A weekly or bi-monthly scan of your entire system should also be in order so that you can detect any malware that made it past your first line of security.

STEP 4: Use Strong Passwords

Though it might be easier, do not use a single password across all the websites you use. Also do not include details like your birthday, favorite food, favorite animal, and other such details in your password.

However, this doesn’t mean that you should use a random jumble of symbols, letters, and numbers. On the password difficulty scale, choose one that is less difficult to guess than a random phrase or collection of words.

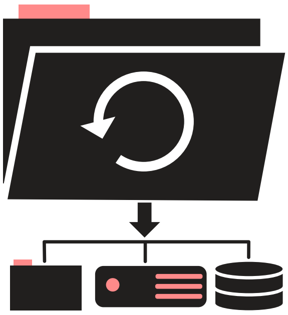
!2gh546/leo is a good password. It is not easy for scripts and other password-hacking software to guess. So is HorseFindChillChicken79841. The latter, however, is also much more easily remembered.

STEP 5: Enable Two-Factor Authentication (2FA)

This line of security requires you to complete two steps before you get into your accounts. After inputting your username and password, you would be required to input a randomized code or respond to an access request to your phone or email. This factor alone is enough to deter many criminals who have only managed to guess your password.

STEP 6: Back Up Your Data Regularly in Case of a Cyberattack

Data backup is one of the most important steps businesses can take to protect themselves from ransomware attacks. By having a recent copy of all their data, businesses can minimize the damage that is done in the event of a hack



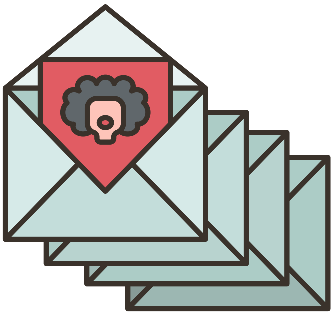
A recent study found that 60% percent of small businesses that suffered a cyberattack went out of business within six months.

8 STEPS TO BETTER CYBERSECURITY

Thus having a data backup is extremely vital for you to stay in business.

Data backup helps businesses recover more quickly if they are hit with a cyber attack. In addition to having a recent copy of your data, it is important to have a plan for restoring that data in the event of an attack.

STEP 7: Avoid Spam Emails



E-mail is still the most common way that people communicate electronically today despite its limitations, despite its dangers.
An email can easily be spoofed to appear as if it's from a trusted source, and this can lead to a cyberattack. In fact, studies show that small businesses receive 94% of their detected malware by email.

One of the most common types of cyberattacks is a phishing attack. In a phishing attack, the attacker sends an email that looks like it's from a trusted source, such as your bank or your employer. The goal of the attack is to get you to click on a link or open an attachment in the email. When you do this, you may give the attacker access to your computer or your account information.

STEP 8: Access Management

Access management is a term used in information technology to describe the control of access to systems and data.

Access management includes the definition of who is authorized to access which systems and data, as well as the enforcement of those permissions

One of the main ways that access management can help against cyberattacks is by limiting access to certain parts of your business's network. This can help to prevent unauthorized individuals from gaining access to sensitive information or systems.

Additionally, having restricted access also helps keep track of who is accessing the information and when, so if something does happen, authorities can more easily investigate and find the perpetrator.

Summing it all Up

Cannabis and specialty retail cybersecurity is an ever-looming issue, but if you incorporate it into your standard operating procedures. Once this is done, cyber security becomes something you never worry about at all. Cyber security does require a bit of investment, but it is definitely a worthwhile expense. After all, the protection in the form of the right cybersecurity measures will always cost less than the potential damages from a data breach. If you're an app developer or just work in the digital space in any way, your security is absolutely something you cannot leave to chance.

THANK YOU FOR DOWNLOADING THIS EBOOK.

Connect with us!

facebook.com/uncutlab

linkedin.com/company/uncutlab

uncutlab.com

info@uncutlab.com