SKYVIEW
TECHNOLOGY

A Cybersecurity Survival Guide
to Help Protect Your Business

According to Verizon’s 2019 Data Breach Investigation Report, 43% of breaches impacted SMBs. But Why do cyberhackers go after small businesses? Business News Daily states that when it comes to starting a small business, new owners have many decisions to make and often leave cybersecurity measures by the wayside. Unless they focus on shoring up their defenses, they may inadvertently end up leaving points of entry wide open for hackers. A Large Enterprise will have many more security protocols in place than a small to medium sized business and SMB’s have many more digital assets available to a cyber criminal than an individual will have online.

Let’s Look At The Facts:

- 43% of cyber attacks are targeted at small businesses.

- 60% of SMB’s companies go out of business within six months of a cyber attack.

- 95% of data breaches occur due to employee error.

Survival Tips:

1. Follow the basics:

- Keep your software up-to-date
- Keep your Antivirus up-to-date
- Understand your Assets, Risks and Resources

2. Train and Educate Your Employees

We cannot stress this enough!! According to an IBM study, 95% of data breaches are caused by employee mistakes.

Provide Your Employees With A Security Policy

Did you know that 48% of employees disable their employer required security settings on their mobile devices? Having a security policy in place with consequences in place to enforce will drastically reduce the possibility for a data breach.

Educate , Educate, Educate

Teach your employees about the different ways cybercriminals can infiltrate your systems. Advise them on how to recognize signs of a breach and educate them on how to stay safe while using the company's network.

Dark Web and Password Rules

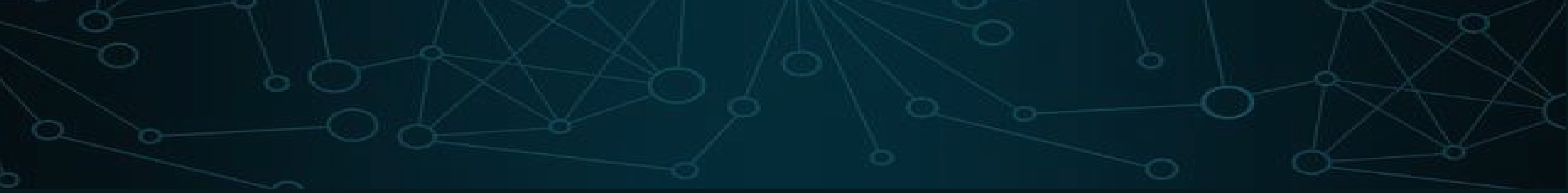
Educate your employees on the Dark Web. Passwords should be different on all logins. It is easy for a hacker to decipher a password that closely resembles another password.

Invest In Security Awareness

This can be the single most effective security measure that a business owner can take. By working with your staff, you can raise awareness of issues such as phishing email. A recent study showed that 21% of phishing emails to employees were opened and 16% of recipients opened an attachment3 —both of which greatly increase chances of data breach and information theft.

3. Know Which Firewalls Your Business Needs

Whether it’s protecting your network, your employees’ devices, or your company website, know which kind of firewalls need to be in place in your organization. For example, an IPS, network firewall, and web application firewall are all different. This also means being educated about new types of cyberattacks that exist so that you and your business are better armed to combat them. Cybersecurity doesn’t need to come with the high price tag. Many cybersecurity vendors offer discounted prices for small businesses so that they can continue serving their customers without the worry of cyberattacks. It’s also important to find a solution that minimizes the resources needed to manage the security in the first place.



4. Be on the Lookout

One of the best ways to prepare for an attack is to understand the different methods that a Hacker will use to gain access to your business information. Cybercrime is at an all time high and their criminal tactics are constantly evolving. Business owners should, at the very least, be aware of the following:

- APT: Long-term targeted attacks in which hackers break into a network in multiple phases to avoid detection. Once an attacker gains access to the target network, they work to remain undetected while establishing their foothold on the system.

- DDoS: A server is intentionally overloaded with requests until it shuts down the target's website or network system.

- Inside attack: This is when someone with administrative privileges, purposely misuses his or her credentials to gain access to confidential company information.

- Malware: This is an umbrella term for any program introduced with the intent to cause damage or gain unauthorized access. Includes; viruses, worms, Trojans, ransomware and spyware.

- Man in the middle (MitM) attack: This is generally done when one or more parties conduct a transaction through an unsecured public Wi-Fi network, where attackers have installed malware that helps sift through data.

- Password attack: This can include; guessing at passwords, a program to try different combinations of words; and keylogging, which tracks a user's keystrokes, including login IDs and passwords. Once a password is maintained; it is easy to gain additional access, since many users use the same passwords or a variation of that password.

- Phishing: Collecting sensitive information like login credentials and credit card information through a legitimate-looking website, often sent to unsuspecting individuals in an email.

- Ransomware: Infects your machine with malware and demands a ransom. Typically will either lock you out of your computer/network and demand money in exchange for access, or it threatens to publish private information if you don't pay a specified amount.

5. Understanding The Available Tools:

By now you know that Strong passwords, up-to-date antivirus and Firewalls are just a few tactics you should employ as part of an overall cybersecurity solution but SMB's should not just focus on these surface level tools. SMB's should consider investing in these three additional important security measures.

- 2FA (2 Factor Authentication): This is a second step to authenticate that it is indeed you are logging in and will reduce the likelihood of password cracking. Many of the breaches made public in recent months could have been prevented by having 2FA in place. Even if attackers had managed to infect a computer and steal a password, they would not have been able to access the account associated with it since they didn't know the one-time access code. Adding 2FA to your current security solution not only protects data; it meets compliance requirements for multi-factor authentication and prevents access to lost or stolen laptops and other devices.

- Data Backup and Disaster Recovery Plan: Having a detailed, step by step procedure for, not only, restoring data and infrastructure but should also specify, which personnel will perform which disaster recovery tasks, how quickly recovery tasks need to be completed in order to meet requirements, how disaster recovery procedures might vary between different facilities or sites and whether disaster recovery operations for hardware need to be performed independently. Keep in mind the costs of downtime- so timing is everything.

- Encryption Software: An Extra security measure to protect sensitive data such as employee records, financial statements and customer information.

6. Control Access:

Use your controls to enforce the policy you have put in place by monitoring access to company systems and control administrative rights and access to important data to only those employees who require access to complete their jobs. Remember that you must have consequences in place for failure to follow to security policy and remove access to anyone who no longer works for your business.

7. Consultations from a well known Computer/Network Security Provider:

Cybersecurity is going to continue to be an on-going process for any business, large or small. To stay up-to-date on security threats and network weaknesses the best thing you can do is hire an educated Managed Service Provider. This takes all the worry out of your IT. To start, look for one who has a free or low cost security assessment. You may also refer to our guide: 5 Insider Tip For Hiring The Right I.T. Service Provider For Your Business. The link can be found here: **https://offer.skyviewtechnology.com/5-hiring-tips**

SKYVIEW
TECHNOLOGY

About Us:

SkyView Technology provides IT packages which are custom tailored to our clients' business needs, including enterprise storage, server upgrades and migrations, data center consolidation, storage optimization, network integration, MSP, MSS, and many others.

SkyView Technology has been providing our award winning services for nearly two decades. With offices in Charleston, Charlotte and Chicago we specialize in delivering proactive IT support and services to businesses like yours with friendly, knowledgeable, 100% certified techs and 24/7 support.

SkyView Technology, as well as our President/CEO Michael Camodeca, have both been awarded and recognized as experts by a number of national media outlets including Fox News and the LA Times.

We optimize your processes, streamline for efficiency and minimize your risk exposure. SkyView Technology will give you; easy file sharing on multiple devices in The Cloud, quick access for all techs in the field, data security, easy inventory control, emergency back up and restoration. We offer Quarterly Technology reviews with fixed priced services and remain vendor neutral- allowing you the best price for our award winning services.

Charleston * Charlotte * Chicago