

BEST PRACTiCE



Best Practices

Although criminals are targeting SMBs, employing best practices can help protect your company against cyberattacks and data breaches.

The following are best practices that you can take to minimize the chance of data breaches.

SKYVIEW
TECHNOLOGY

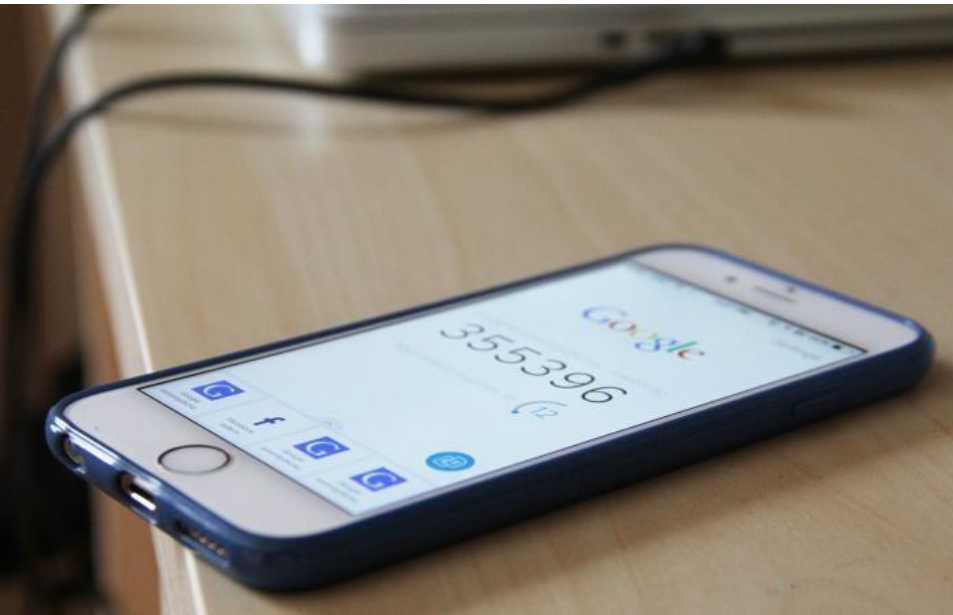
Secure passwords

Passwords are the key to networks, customer information, online banking and social media.

Password best practices include:

Use strong passwords.

- ✓ Make the password at least 8 characters long. The longer the better. Longer passwords are harder for thieves to crack.
 - ✓ Consider using passphrases. When possible, use a phrase such as “I went to Lincoln Middle School in 2004” and use the initial of each word like this: “lw2LMSi#2004”.
 - ✓ Include numbers, capital letters and symbols.
 - ✓ Don’t use dictionary words. If it’s in the dictionary, there is a chance someone will guess it. There’s even software that criminals use that can guess words used in dictionaries.
- Change passwords. Passwords should be changed every 60 to 90 days.
 - Don’t post it in plain sight. This might seem obvious, but studies have found that a lot of people post their password on their monitor with a sticky note.
 - Consider using a password manager. Programs or Web services let you create a different very strong password for each of your accounts, but you only have to remember the one password to access the program or secure site that stores your passwords for you.
 - Consider using multi-factor authentication. Set up multi-factor authentication that requires a code that is displayed on your phone. This way hackers cannot access an account without having physical access to your phone.



SKYVIEW
TECHNOLOGY

Encrypt data

Lost laptops, smartphones and USB drives continue to cause data breaches.

Many businesses don't realize how much sensitive information is on mobile devices. Sensitive information could be in emails, spreadsheets, documents, PDF files and scanned images.

The best way to protect sensitive information is to use encryption. Under many federal and state regulations, encryption is a "safe harbor". This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a reportable breach. Customers and affected individuals would not need to be notified.

Types of Encryption

Mobile device encryption. Laptops, smartphones and USB drives can all be encrypted. This will protect any data that is on these devices.

Email encryption. Emails could contain sensitive information and should be encrypted. Secure email will protect the data that is sent.

Workstation encryption. Like laptop encryption, desktops and workstations can be encrypted to protect any data stored on them. Workstation encryption is very important in the event of a break-in and theft of workstations. Without encryption, a stolen workstation may result in a data breach.

SKYVIEW
TECHNOLOGY





Employee Security Training

95% of data breaches are caused by employee mistakes. It is critical to ensure that employees understand the risks to sensitive information and the threat of data breaches.

Phishing and ransomware are leading methods of attacks. Employees need to know how to spot phishing emails, phishing websites and the dangers of email attachments.

Training needs to take into account the dangers of hacking, stolen mobile devices, posting sensitive information on social media and other causes of data breaches.

A good training program will continually remind employees about the dangers of data breaches and how to avoid becoming a victim. Cybercriminals are developing new scams and attacks everyday and employees should be made aware of these scams.

“95% of data breaches are caused by employee mistakes”

SKYVIEW
TECHNOLOGY

Data backup and disaster recovery

Backing up data will protect your business from data loss due to damaged servers or malicious code such as ransomware.

A fire, flood, explosion or natural disaster can destroy systems that contain valuable information. Having up-to-date data backups and a disaster recovery plan will help recover and restore valuable information.

Many businesses go out of business after a data breach because they can't continue to operate without having access to customer information, business process documents, financials and other necessary information. Data backups ensure that data is recoverable.

It is recommended that automated backups occur that securely copy data offsite.

Data backups should be periodically tested to ensure the data is able to be recovered.

www.skyviewtechnology.com

info@skyviewtechnology.com

877-818-3247



“Only 6% of companies survive longer than 2 years after a significant data loss”

SKYVIEW
TECHNOLOGY

Perform a security risk assessment

A security risk assessment (SRA) is a critical step to understanding the risk to your business and sensitive information.

An SRA will inventory customer, employee, vendor and sensitive data, identify how you are currently protecting the data and make recommendations on how to lower the risk to the data.

An SRA will help you to understand your risk of phishing scams and ransomware, the dangers of lost mobile devices, the risk of insider threats and how prepared you are in the event of a disaster.

Without a thorough understanding of risk, it is difficult to implement the safeguards needed to protect your business. Cybersecurity is a business risk and needs to be evaluated and mitigated just like other business risks.



“Many SMBs don’t know where their critical data is, how it is being protected or what the risks are to the data. Cybersecurity is a business blind spot.”

SKYVIEW
TECHNOLOGY

www.skyviewtechnology.com

info@skyviewtechnology.com

877-818-3247

www.skyviewtechnology.com



SKYVIEW TECHNOLOGY

SkyView Technology offers nearly 2 decades of proactive support with an average customer retention of over 10 years. We employ only reliable and certified engineers and offer 24/7 support with a quick response time. We are customer service based and offer customized solutions based on your individual company needs. Please call us for more information 877-818-3247 or email us at Info@skyviewtechnology.com

877.818.3247