CHECK POINT™

YOU DESERVE THE BEST SECURITY

# TOP 10 SECURITY BEST PRACTICES FOR SMBS

Today's cyber-landscape is tough for small and medium businesses. Cybercriminals have dramatically improved their attacks, resulting in a higher frequency of attacks and sophistication. SMBs struggle with the expertise, manpower, and IT budget needed to succeed in this day and age. We're here to help you every step of the way with these security best practices that you can implement now.

## 01 COMMON PASSWORDS ARE BAD PASSWORDS

Passwords are your first line of security defense. Cybercriminals attempting to infiltrate your network will start by trying the most common passwords.

BEST PRACTICE: Ensure use of long (over 8 characters) and complex passwords (include lower case, upper case, numbers, and non-alpha characters).

## 02 SECURE EVERY ENTRANCE

All it takes is one open door to allow a cybercriminal to enter your network. Just like you secure your home by locking the front door, the back door and all the windows, think about protecting your network in the same way.

Consider all the ways someone could enter your network, then ensure that only authorized users can do so.

## 03 SEGMENT YOUR NETWORK

A way to protect your network is to separate your network into zones and protect the zones appropriately. One zone may be for critical work only, where another may be a guest zone where customers can surf the internet, but not access your work network.

Segment your network and place more rigid security requirements where needed.

## 04 DEFINE, EDUCATE, AND ENFORCE POLICY

Actually HAVE a security policy (many small businesses don't) and use your Threat Prevention device to its full capacity. Spend some time thinking about what applications you want to allow in your network and what apps you do NOT want to run in your network.
Educate your employees on acceptable use of the company network. Make it official. Then enforce it where you can. Monitor for policy violations and excessive bandwidth use.

## 05 BE SOCIALLY AWARE

Social media sites are a goldmine for cybercriminals looking to gain information on people, improving their success rate for attacks.

Attacks such as phishing, spearphish, or social engineering all start with collecting personal data on individuals.

## 06 ENCRYPT EVERYTHING

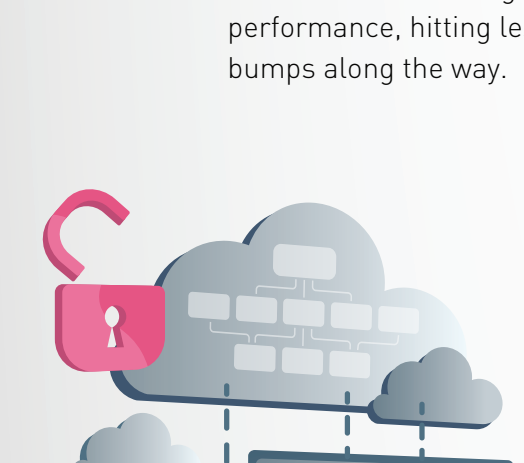
One data breach could be devastating to your company or your reputation. Protect your data by encrypting sensitive data and make it easy for your employees to do so.

Ensure encryption is part of your corporate policy.

## 07 MAINTAIN YOUR NETWORK LIKE YOUR CAR

Your network, and all its connected components, should run like a well oiled machine.

Regular maintenance will ensure it continues to roll along at peak performance, hitting less speed bumps along the way.



## 08 CLOUD CAUTION

Cloud storage and applications are all the rage, but be cautious. Any content that is moved to the cloud is no longer in your control.
And cybercriminals are taking advantage of weaker security of some cloud providers.

## 09 DON'T LET EVERYONE ADMINISTRATE

Laptops can be accessed via user accounts or administrative accounts.

Administrative access allows users much more freedom and power on their laptops, but that power moves to the cybercriminal if the administrator account is hacked.

## 10 ADDRESS THE BYOD ELEPHANT IN THE ROOM

Start with creating a Bring-Your-Own-Device policy. Many companies have avoided the topic, but it's a trend that continues to push forward.

Don't avoid the elephant in the room!
It all comes back to educating the user.

***Feel free to download the full white paper here***

***Schedule a quick demo for your SMB here***

***Get more resources and information here***