YOU DESERVE THE BEST SECURITY

TOP 10 SECURITY BEST PRACTICES FOR SMALL BUSINESS

Practical Guide to Protecting Your Business Today

Why Are Small Businesses Targeted?

LARGE BUSINESS

Significant expertise,
IT staff and budget.

Advanced security with
continuous monitoring.

SMALL & MEDIUM BUSINESS

Valuable information but
weaker protection.

Less people and less investment
in security.

As more large businesses and corporations invest in cybersecurity tools, hackers are increasingly targeting small and medium-sized businesses

— Michael Sohn, FBI Supervisory Special Agent

42% of SMBs blame their security issues on lack of trainings

— SMB Security Report 2022, Datto

Ways Your Office Can be Threatened

Phishing is the leading threat action for SMBs
— Verizon DBIR

70% of SMB Employee Passwords Stolen, Lost
— Global State of Cybersecurity in SMB, Keeper Security and the Ponemon Institute

85% Ransomware is the biggest SMB threat
— Datto's Global State of the Channel Ransomware Report

Why don't SMBs focus on security?

Believe they are too small to be a target

Believe they have sufficient protection in place?

Perception that security is too expensive, complex, and demanding

Nearly 75% of SMBs say that a ransomware attack would be a death blow

— SMB Security Report 2022, Datto

TOP SECURITY BEST PRACTICES #1

1

#1: Common Passwords Are Bad Passwords

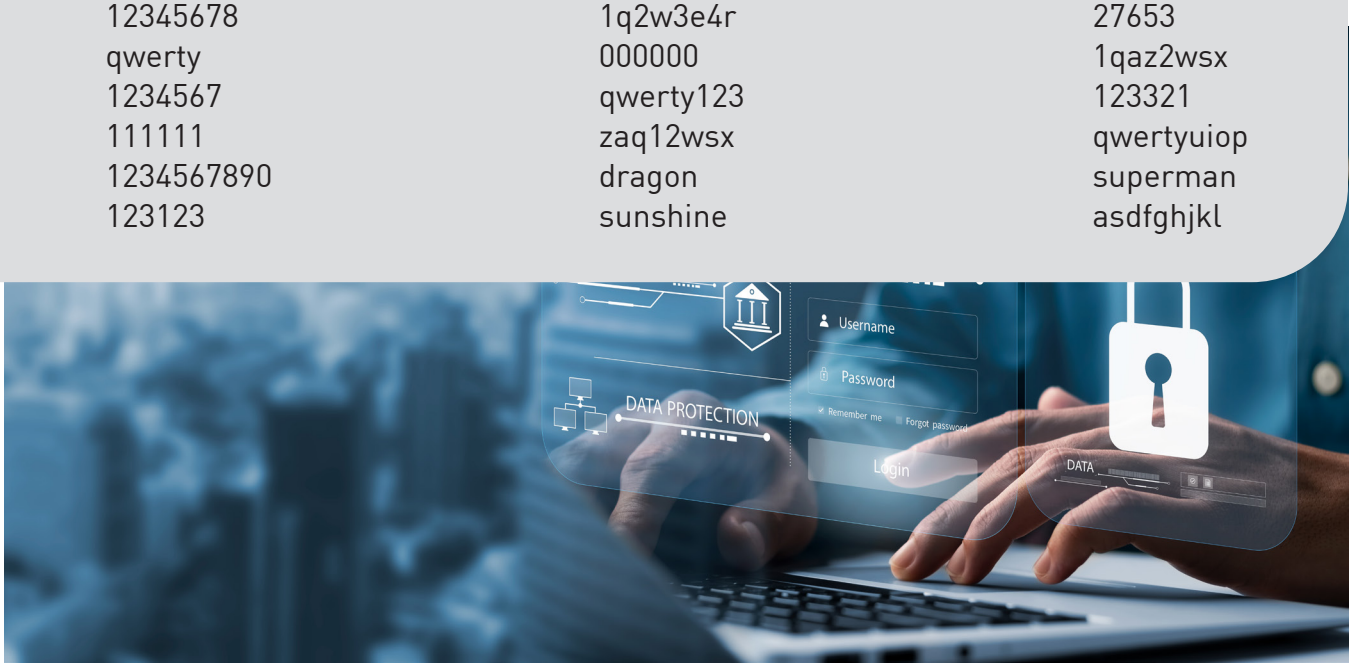
Passwords are your first line of security defense. Weak passwords and access management continue to remain in the top 5 issues for SMBs when it comes to security. Cybercriminals attempting to infiltrate your network will start by trying the most common passwords. The folks over at Safety Detectives captured the top 30 most used passwords in the world. See those below.

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

The 30 Most Common Passwords

(If you have one of these, change it NOW!)

123456	abc123	princess
password	1234	letmein
123456789	password1	654321
12345	iloveyou	monkey
12345678	1q2w3e4r	27653
qwerty	000000	1qaz2wsx
1234567	qwerty123	123321
111111	zaq12wsx	qwertyuiop
1234567890	dragon	superman
123123	sunshine	asdfghjkl



TOP SECURITY BEST PRACTICES #2

2

#2: 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.

- Ensure strong passwords on laptops, smartphones, tablets, and WIFI access points.
- Use a Firewall with Threat Prevention to protect access to your network (like the Check Point 1500 Appliance).
- Secure your endpoints (laptops, desktops) with security software such as Anti-virus, Anti-SPAM and Anti-Phishing.
- Protect from a common attack method by instructing employees not to plug in unknown USB devices.

TOP SECURITY BEST PRACTICES #3

3

#3: 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.

- Public facing web servers should not be allowed to access your internal network.
- You may allow guest access, but do not allow guests on your internal network.
- Consider separating your network according to various business functions (customer records, Finance, general employees).

TOP SECURITY BEST PRACTICES #4

4

#4: 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. 42% of SMBs blame their security issues on lack of training. It's evident that education and training MUST improve.

- Set up an Appropriate Use Policy for allowed/disallowed apps and websites.
- Do not allow risky applications such as Bit Torrent or other Peer-to-Peer file sharing applications, which are a very common methods of distributing malicious software.
- Block TOR and other anonymizers that seek to hide behavior or circumvent security.
- Think about Social Media while developing policy.

TOP SECURITY BEST PRACTICES #5

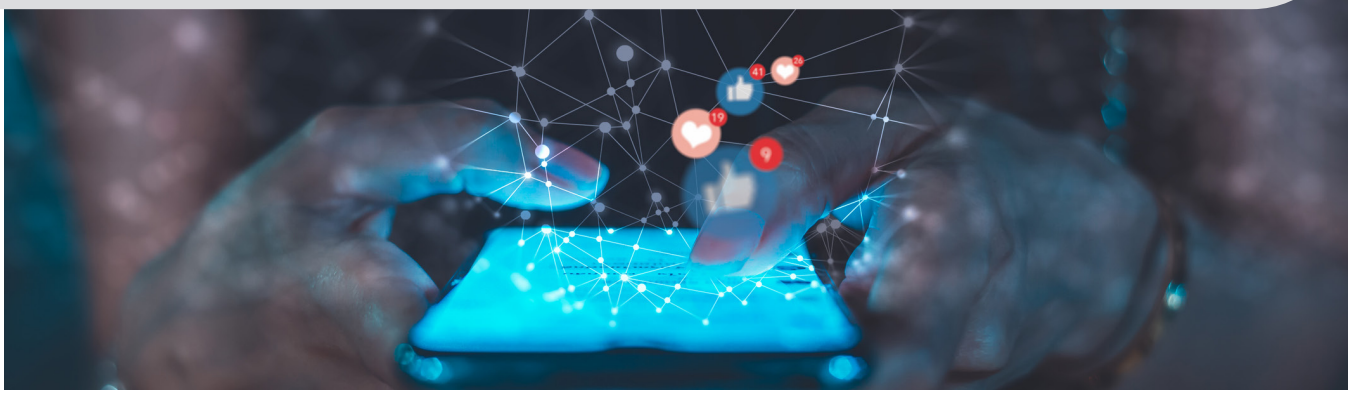
5

#5: Be Socially Aware

Social media sites are a gold mine 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.

- Educate employees to be cautious with sharing on social media sites, even in their personal accounts.
- Let users know that cybercriminals build profiles of company employees to make phishing and social engineering attacks more successful.
- Train employees on privacy settings on social media sites to protect their personal information.
- Users should be careful of what they share, since cybercriminals could guess security answers (such as your dog's name) to reset passwords and gain access to accounts.



TOP SECURITY BEST PRACTICES #6

6

#6: 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.

- Sleep easy if laptops are lost or stolen by ensuring company owned laptops have pre-boot encryption installed.
- Buy hard drives and USB drives with encryption built in.
- Use strong encryption on your wireless network(consider WPA2 with AES encryption).
- Protect your data from eavesdroppers by encrypting wireless communication using VPN (Virtual Private Network).

TOP SECURITY BEST PRACTICES #7

7

#7: 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 and hit few speed bumps.

- Ensure operating systems of laptops and servers are updated (Windows Update is turned on for all Systems).
- Uninstall software that isn't needed so you don't have to check for regular updates (e.g., Java).
- Update browser, Flash, Adobe and applications on your servers and laptops.
- Turn on automatic updates where available: Windows, Chrome, Firefox, Adobe.
- Use an Intrusion Prevention System (IPS) device like the Check Point 1500 Appliance to prevent attacks on non-updated laptops.

TOP SECURITY BEST PRACTICES #8

8

#8: Don't Underestimate the Need to Secure Your Cloud

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.

- When using the Cloud, assume content sent is no longer private.
- Encrypt content before sending (including system backups).
- Check the security of your Cloud provider.
- Don't use the same password everywhere, especially Cloud passwords.

TOP SECURITY BEST PRACTICES #9

9

#9: 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.

- Don't allow employees to use a Windows account with Administrator privileges for day-to-day activities.
- Limiting employees to User Account access reduces the ability for malicious software (better known as malware) to do extensive damage at the "administrator" privileged level.
- Make it a habit to change default passwords on all devices, including laptops, servers, routers, gateways and network printers.

TOP SECURITY BEST PRACTICES #10

10

#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 comes back to educating the user.

- Consider allowing only guest access (internet only) for employee owned devices.
- Enforce password locks on user owned devices.
- Access sensitive information only through encrypted VPN.
- Don't allow storage of sensitive information on personal devices (such as customer contacts or credit card information).
- Have a plan if an employee loses their device.

Prevention is Key

Small businesses need enterprise level protection without the complexity, cost and expertise. This means they need security that consolidates the functions to achieve a high level of protection, security that doesn't require a large staff or deep expertise and security that just works, right out of the box. But how does that work?

• Above all else preventing the next cyberattack is key. Solutions that detect an infection has occurred are helpful, but they're a bit like hearing "Fire" in a crowded movie theater.

• When you see or hear the alert, then you know you have to take action, i.e. move quickly to the nearest exit or disconnect the infected system from the network.

• An alert that the fire is out or the attack was prevented means you can continue doing what you were doing.

Securing the Network

Check Point security gateways are enterprise-grade, meaning they've been tested, approved and deployed by thousands of enterprises worldwide. The Check Point Quantum Spark™ Series security gateways are an all-in-one solution for securing small to medium size businesses.

Protection from every threat

Easy to deploy and manage

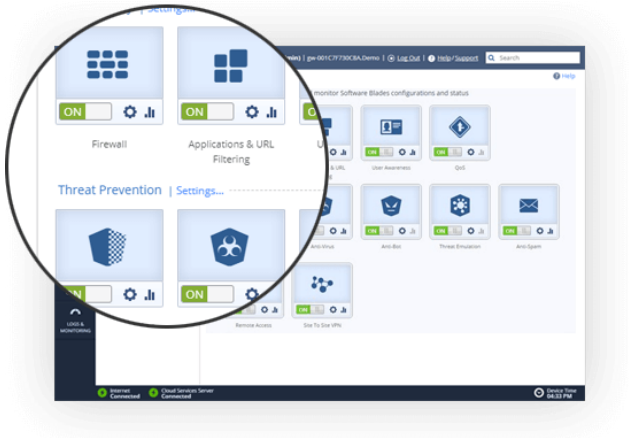
"All-in-One" solution

- **Easy setup** - Plug it in, follow a simple set-up wizard and your network is secure
- **Out of the box protection** – security policies are included that deliver protection immediately, and adjustments can be made to tailor policies for your business.
- **Low price** - the Quantum Spark family delivers protection with a modest investment. Check Point Quantum Spark security gateways could also be offered by your local Internet service provider as a monthly subscription. Asked for your service provider for Check Point.
- **Easy management** - Ongoing management and upkeep is simple with a mobile app to monitor and mitigate any security issues while on the go.
- **Network and security package in one** – Models are available with the latest and greatest internet connectivity options, including 5G Cellular, Wi-Fi 6, and more. These gateways can support multiple internet service providers and monitor them for quality of service, so you can get the best bandwidth for each application.

Enterprise Capabilities in a Small Package

The security functions of the Quantum Spark Next Generation Firewall family enable you to control who accesses your network, prevents attacks and threats, and secures communications with your business from remote employees or additional business locations. Having the tools is important. Knowing how to use them simply and effectively is critical.

Just like enterprises, small businesses need to ensure that only authorized traffic and users are allowed to access the network. They must also ensure that only appropriate websites are accessed by users. Policies span various capabilities that are used to protect the network.



• Next-Gen Firewall - Ensures only the traffic that should be allowed on the network traverses the network. Prohibited traffic is blocked before it ever enters the network.

• Application Control and URL Filtering - these capabilities work together to ensure that only allowed applications are used on the network and that only allowed websites can be visited.

• User Awareness - Allows an organization to have polices in place that will allow or prohibit what specific people can do, based on their identity or role in the business.

• QoS - Quality of Service allows you to give priority to your most important traffic.

Prevent Attacks and Threats

Large enterprises use high levels of protection to defend the business from threats. Small businesses now can leverage these threat prevention technologies to defend their business.

• IPS - Intrusion Prevention Systems search traffic for attacks targeting business computers and devices. Computers and devices that do not have the latest patches are protected by the IPS.

• Anti-Virus - Malware such as viruses and worms are prevalent and can cause major damage. Anti-Virus blocks malware before it can get into the network.

• Anti-Spam - unwanted email is an issue for any business. Anti-Spam blocks SPAM email messages that can also often deliver malware or lead users to malicious sites.

• Anti-Bot - Bots collect information to send to their command and control center for further malicious activity. Anti-Bot will detect and block that communication.
• Sandboxing - prevents infections from undiscovered exploits, zero-day and targeted attacks by launching suspicious files in a virtual sandbox, discovering malicious behavior and then preventing malware from entering the network.

Protect Business Data

When computers communicate with other computers or remote users, the information can be captured by attackers if it is not encrypted. Virtual Private Networks (VPN) encrypt data traversing the network, allowing only the intended receivers to read the information.

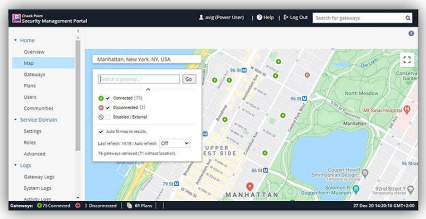
• Remote Access - Encrypts traffic from PC's and user devices to the network, whether they are in the office or on the road.
• Site-to-Site VPN - If a business has multiple offices, this VPN encrypts all communications between multiple office locations.

Easy and Intuitive Cloud and Mobile Management

SMBs have a variety of easy to use choices for managing Quantum Spark security gateways including a Cloud web portal and WatchTower ™ mobile app.

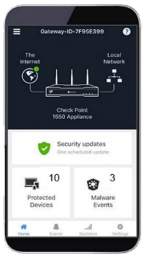
Cloud-Based Security Management Portal

Check Point's intuitive cloud-based management portal enables easily manager your security gateway settings and alerts onsite or remotely saving time, effort, and cost.



Mobile App for Management On-the-Go

Check Point's WatchTower mobile application provides a security operations center in the palm of your hand. From your mobile phone, you can remotely monitor the security status of your network including who is accessing it, and quickly mitigate any threats directly from the mobile device.



Complete Protection for Remote employees and Cloud Applications

In addition to the network protection Quantum Spark gateways provide, businesses can protect all laptops and PCs against threats such as malware, ransomware and phishing with Check Point endpoint protection, and secure employees' smartphones with Check Point mobile protection. Email and docs can be protected with Check Point email security.

Help is Available

Nearly two-thirds of small to medium businesses say they lack the in-house skills to deal with cyber-security issues – so it's no surprise that SMBs are urgently looking for solutions to prevent cyber-threats from damaging their business.

Help is available from Managed Security Providers (MSP) who sell security services specifically designed for the growing SMB market. To put the size of that opportunity in perspective, it's forecast that SMBs' spend on security worldwide will almost double between now and 2024 (from around $50 billion currently). Businesses are willing to pay a 34% premium to service providers that deliver the right cybersecurity services, and 91% of SMBs would consider moving to a new IT service provider if it offered the right security solutions.most important traffic.

Why Check Point?

The Fortune 100 relies on Check Point for security. Other providers don't bring the level of expertise and experience delivering high levels of protection. Only Check Point delivers enterprise-grade security in a compact, easy to manage package, designed to meet the needs of a small business.

"Security is not an option for retailers. We hold the details of millions of customers' credit cards; hacking those details can have a catastrophic impact on our corporate reputation. Check Point allows us to work smarter. "

— Smart & Final

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com

© 2023 Check Point Software Technologies Ltd. All rights reserved.