SECUR-SERV

Small Business Cybersecurity Playbook:

How to Train Your Team & Stop Costly Attacks

One click can cost you thousands — here's how to turn your employees into your strongest defense.

secur-serv.com

TABLE OF CONTENTS

INTRODUCTION

Why Your Employees Are Your Strongest (and Weakest) Link

Big companies spend millions on cybersecurity tools. But for small businesses, it only takes one click on a fake link or a stolen password to bring everything to a halt.

Hackers know this. That's why they target your people first — because a busy employee is more likely to open a suspicious email or use the same password everywhere.

86%

According to a PricewaterhouseCoopers survey, 86% of business executives expressed concern about cyberthreats and lack of data security.

The good news? You don't need a huge IT budget to stay protected. Training your team to spot red flags and follow simple best practices can block most threats before they do any damage.

This playbook breaks down practical, no-jargon tips to help you:

- Keep sensitive data out of the wrong hands
- Make cybersecurity part of your daily work culture
- Protect your reputation (and your bottom line)

Your people really are your best defense — if they know what to watch for.
Let's get started.

CHAPTER 1

Physical Security Precautions

Physical Security - The Basics Still Matter

You'd be surprised how many breaches start with something as simple as a messy desk. A sensitive file left out. A laptop that's not locked when you grab a coffee.

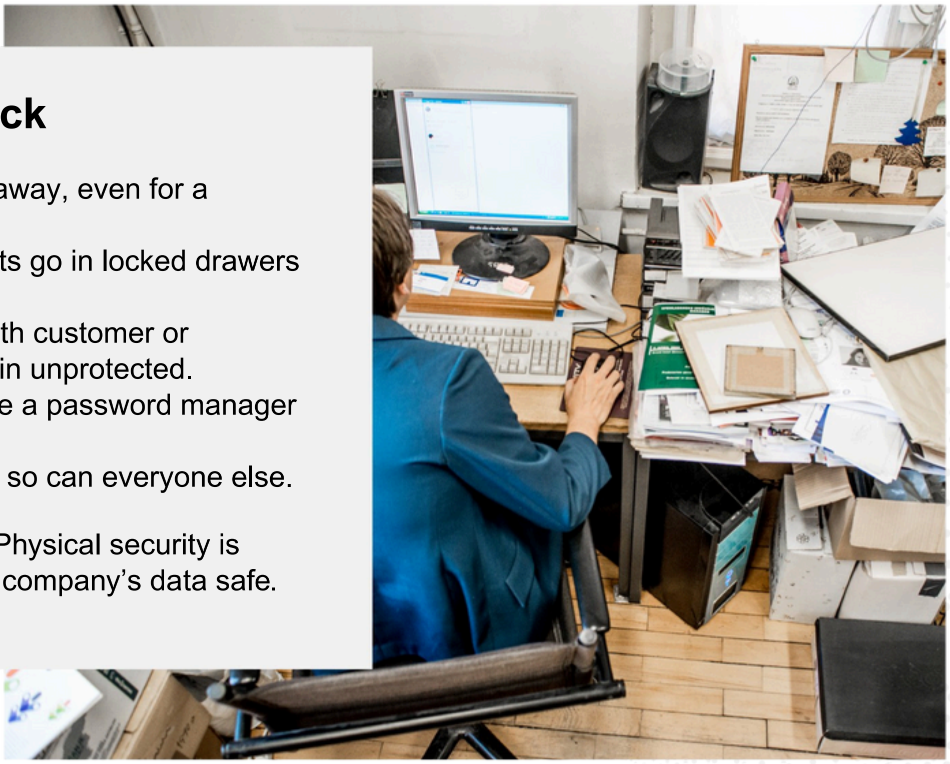
In a small business, it's easy to think, "It won't happen here." But physical security slip-ups are the low-hanging fruit for anyone looking to steal data — whether it's a disgruntled ex-employee, a visitor, or just someone being nosey.

A clean desk isn't just tidy — it's protection. When you keep workspaces clear of papers, USB drives, or sticky notes with passwords (yes, it still happens), you're cutting off easy targets for theft.

Daily Desk Security Check

- Lock screens whenever you step away, even for a minute.
- Secure files — sensitive documents go in locked drawers or cabinets.
- Shred it, don't trash it. Anything with customer or business info shouldn't go in the bin unprotected.
- No passwords on sticky notes. Use a password manager instead.
- Think like a thief. If you can see it, so can everyone else.

A little habit change goes a long way. Physical security is the first, simplest step in keeping your company's data safe.



Email Threats

Social engineering is when scammers manipulate people — not computers — to steal information and break into your systems. They often pretend to be someone you trust, like a coworker, vendor, or customer.

> An example of social engineering is an email where an employee is asked to contact a tech support hotline and is tricked into giving up credential information.

Phishing Email Compromises

If there's one thing hackers count on, it's that your people are busy and distracted. That's why phishing emails are still their #1 trick — and they keep getting better at fooling us.

One click on a fake link, and a scammer can get your passwords, install malware, or even trick you into sending money to the wrong account. It happens every day to businesses just like yours.

Spotting a phishing email takes vigilance and practice.

Common Phishing Techniques

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these email tactics:

- Embedding links that redirect users to an unsecured website requesting sensitive information
- Installing Trojans via a malicious attachment
- Spoofing the sender address to appear as a reputable source and requesting sensitive information

CHAPTER 2

How to Spot Suspicious Emails

Check the sender

Does the email really come from who it says? Look closely at the address — hackers often swap one letter or use a lookalike domain.

Attachments can hide trouble

If you weren't expecting it, verify first. Don't open mystery files.

Don't blindly trust links

Hover over links before you click. If it looks fishy or unfamiliar, don't bite.

Verify urgent email requests

"Act now or else" is a classic scam move. Take a breath and confirm through another channel.

Keep your machine clean

Regular updates and good antivirus software help catch what slips through.

!

90+%

According to CISA.gov, over 90% of cyberattacks arrive by email.

CHAPTER 3

Username & Password Management

If you want an easy win for your company’s security, start with stronger passwords. Weak or reused passwords are an open door for hackers — and yes, “password123” is still way too common. The names of popular sports such as “football” and “baseball” are also on the list, in addition to quirky passwords such as “qwerty” and even the word “password” itself.

Cybercriminals don’t guess passwords by hand — they use powerful tools that can try billions of combinations in seconds. Short, predictable passwords are the first to to be compromised.

Emphasis should also be placed on the importance of avoiding common usernames. In analysis conducted by the information security firm Rapid7, hackers most often prey upon these 10 usernames:

Username	administrator	Administrator	User1	Admin
Alex	Pos	Demo	db2admin	Sql

CHAPTER 3

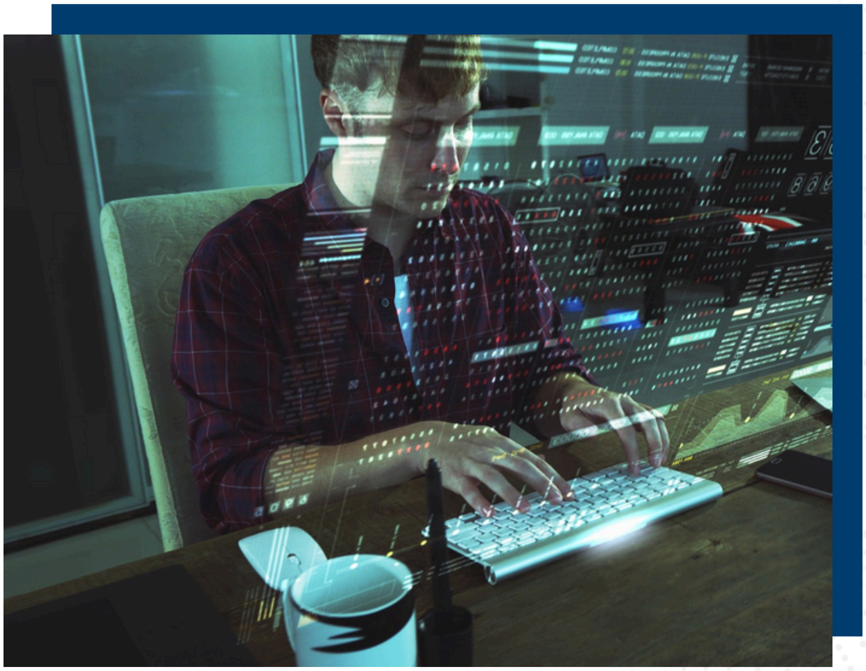
How Attackers Exploit Weak Passwords

While most websites don't store your actual password, they do store what's called a password hash — an encrypted version of your password. Hackers know how to target these hashes, and if your password is weak, it's much easier for them to reverse-engineer it.

Attackers also use common tricks to guess passwords they think they're close to cracking. For example, they'll try different word variations like:

- Capitalizing the first letter
- Swapping between upper and lowercase combinations
- Inserting numbers randomly inside the word
- Adding numbers to the beginning or end
- Replacing letters like "o" and "l" with "0" and "1"
- Adding punctuation at the end (like "!")
- Doubling letters in the word
- Combining two words into one
- Adding spaces or symbols between words
- Using "@" instead of "a"

All of these mutations are easy for hacking tools to test automatically. That's why using longer, complex passphrases — instead of short, predictable words — is the best way to keep your logins secure.



CHAPTER 3

Tips to Strengthen Password Security

- Longer is better: Aim for at least 12 characters. Short passwords get cracked first.
- Mix it up: Use upper and lowercase letters, numbers, and special characters.
- Keep them unique: Never reuse the same password for multiple accounts.
- Skip the sticky notes: Use a secure password manager instead.
- Turn on two-factor authentication (2FA): Always add that extra step when it’s available. It makes a huge difference.
- Check regularly: Do a quick password audit every few months. Shut down old accounts and fix weak logins.

!

For an extra layer of protection, always use two-factor authentication (2FA) whenever possible. With 2FA, logging in requires not just a password, but also a one-time code sent to the user’s phone or authentication app. Even if hackers steal a password, they can’t get in without that second step.

CHAPTER 4

Mobile Security

Keep Devices from Becoming Doors

Laptops and phones make work easy — but they're also prime targets for hackers. In a small business, especially with remote or BYOD (Bring Your Own Device) setups, mobile security often gets overlooked. One lost phone or one risky app can open the door to your entire network.

And public Wi-Fi? A goldmine for attackers. On an unsecured network, it's shockingly easy for someone nearby to intercept data or hijack your device.

The Biggest Mobile Device Risks

Protect Every Mobile Device

- Lost or stolen devices: If a phone with work access goes missing, sensitive info can go with it. Remote wipe and lock tools are a must.
- Mobile malware: Hackers are increasingly targeting phones with malware hidden in texts or fake apps. Android devices see this more often, but iPhones aren't immune.
- Untrusted apps: Sketchy third-party apps can be a back door into your business data

Hi!
Free to talk?
Yes. Where are you?
At home
And you?
At work. See you today?
Yes. When?
At 7 o'clock in our cafe
Ok

Pro Tip for Small Teams

If you let employees use their own devices for work, set clear rules: strong passcodes, remote wipe enabled, and company data must be removed if they leave. A few upfront policies can save you from major headaches later.

CHAPTER 4

How Employees Can Secure Their Mobile Devices

Always use a passcode

No phone should be unlocked. Some devices let you set it to wipe data after too many failed attempts.

Use remote locate tools

Tools like Apple's "Find My iPhone" or Android's Device Manager help you find lost phones and erase them if needed.

Keep devices clean

Run antivirus and malware scans regularly.

Think twice on public Wi-Fi

Avoid logging into sensitive accounts or transferring important files on open networks. Use a VPN when you have to.

Use Mobile Device Management (MDM)

An MDM solution lets you enforce security settings, manage apps, and track devices. For small businesses, this is one of the best ways to keep personal and company data separate and secure.

!

Pro Tip for Small Teams

If you let employees use their own devices for work, set clear rules: strong passcodes, remote wipe enabled, and company data must be removed if they leave. Upfront policies can save you from major headaches later.

CHAPTER 5

Secure Website Browsing

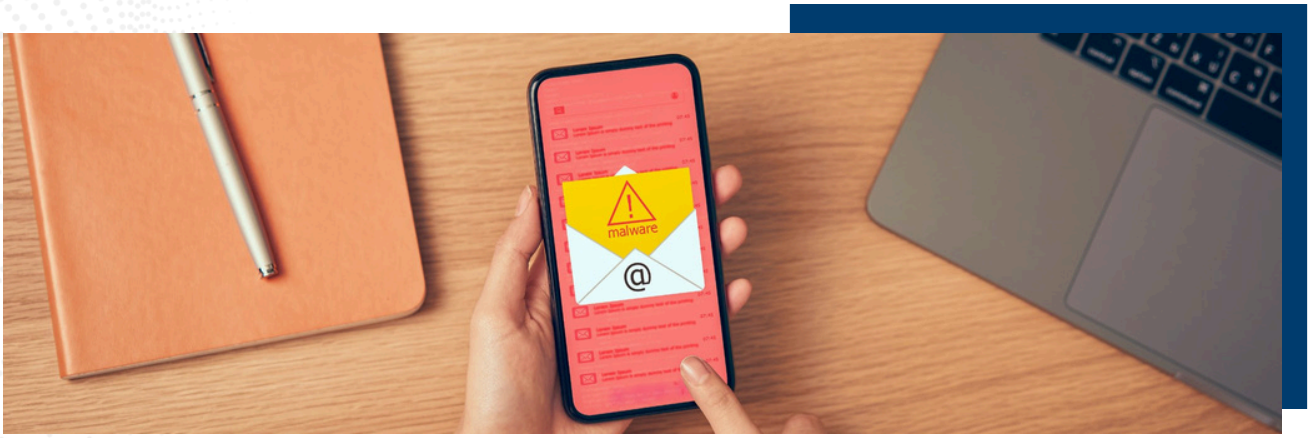
Most employees don’t think twice about clicking around online — but websites are one of the most common ways malware sneaks into your network. Even trusted sites can be compromised with dangerous ads or malicious downloads hiding in plain sight.

Malvertising is a form of malicious code that distributes malware through online advertising. It can be hidden within an ad, embedded on a website page or bundled with software downloads. This type of threat can be displayed on any website, even those considered the most trustworthy.

Another website browsing threat involves social media. According to an article in The Huffington Post, some of the most common Facebook hacks and attacks include clickjacking, phishing schemes, fake pages, rogue applications, and the infamous and persistent Koobface worm. Twitter isn’t immune to security issues either. According to CNET News, just 43% of Twitter users could be classified as “true” users. The other 57% fell into a bucket of “questionable” users.

Biggest Website Threats

- **Malvertising:** These are malicious ads — sometimes even on legit sites — that infect devices when clicked or just viewed.
- **Fake download buttons:** Some sites trick users into downloading malware disguised as software updates or helpful tools.
- **Phishing pages:** Lookalike websites (often reached through email links) are built to steal passwords, credit card info, or company credentials.
- **Social media scams:** Clickjacking, fake pages, rogue apps — these tactics are all over platforms like Facebook and Twitter.



CHAPTER 5

Browse Smarter, Stay Safer.
Best Practices for Employees

- Stick to known sites: If a site seems off, it probably is. Avoid unfamiliar sources for downloads or tools.
- Don't click links in emails: Go directly to the website yourself instead of trusting a link — even if it looks legit.
- Look for HTTPS: Always check that a site uses HTTPS (the "S" stands for secure).
- Be skeptical of pop-ups: Many are scams or attempts to download malware. Close them without clicking.
- Stay updated: Make sure your browser, plugins, and antivirus tools are current — updates often patch real security gaps.
- Use good social media hygiene: Don't click on strange DMs and avoid connecting with unknown accounts.

!

Pro Tip for Small Teams

Set your employee browser default to a secure, work-approved site. It it keeps people grounded in safe online behavior — especially if they're working from home or jumping between tabs all day.

CHAPTER 6

Cybersecurity You Don’t Have to Handle Alone

Most small businesses don’t have a full-time IT staff. It also means you're doing everything: keeping systems running, managing devices, watching for threats, and hoping nothing slips through the cracks.

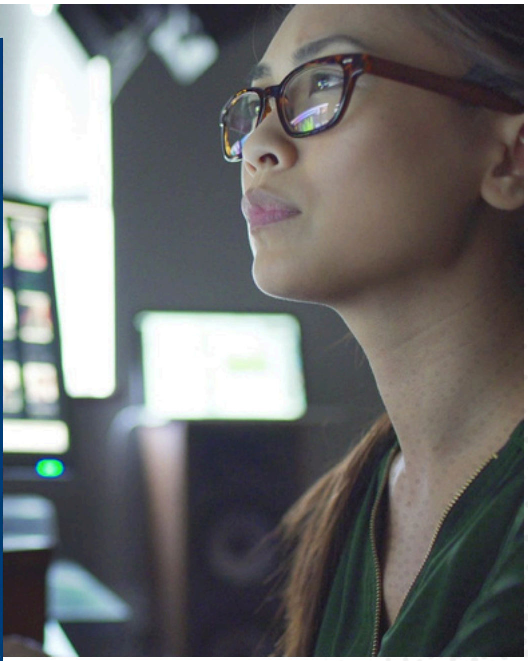
Meanwhile, hackers are counting on that gap.

That’s where a Managed Service Provider (MSP) comes in — not as a vendor, but as a partner. A good MSP works like an extension of your team. They help protect your people, your devices, and your business — without you having to stay up to date on every new cyber threat.

This isn’t about outsourcing tech problems. It’s about strengthening your defenses, closing the gaps, and getting peace of mind.

Why SMBs Work with MSPs

- **Your time is better spent running the business.** Let someone else handle the patches, updates, monitoring, and alerts.
- **Mistakes happen.** A good MSP trains your team, runs phishing tests, and helps turn your people into your first line of defense.
- **Downtime is expensive.** When something breaks, your MSP is already working on it.
- S**mall businesses are big targets**. Hackers go for the easy wins. An MSP makes sure that’s not you.



Think of cybersecurity like insurance: if you wait until something goes wrong, it's already too late. A trusted MSP helps you stay protected before anything hits — with tools, training, and real support built for small business realities.

SUMMARY

Education & Technology – a Winning Cybersecurity Combination

Cybersecurity isn't just about tools or technology, it is about people, habits, and smart decisions made daily. For small businesses, the risks are real, but so are the solutions. By training your team, locking down your devices, and partnering with the right experts, you can build a strong, flexible defense without overcomplicating your operations. The threats may be growing, but with the right strategy, your business stays one step ahead — protected, prepared, and ready for whatever comes next.

See these tips in action — book a free demo of Secur-Serv's employee cybersecurity training program.

SECUR-SERV

800.228.3628

secur-serv.com