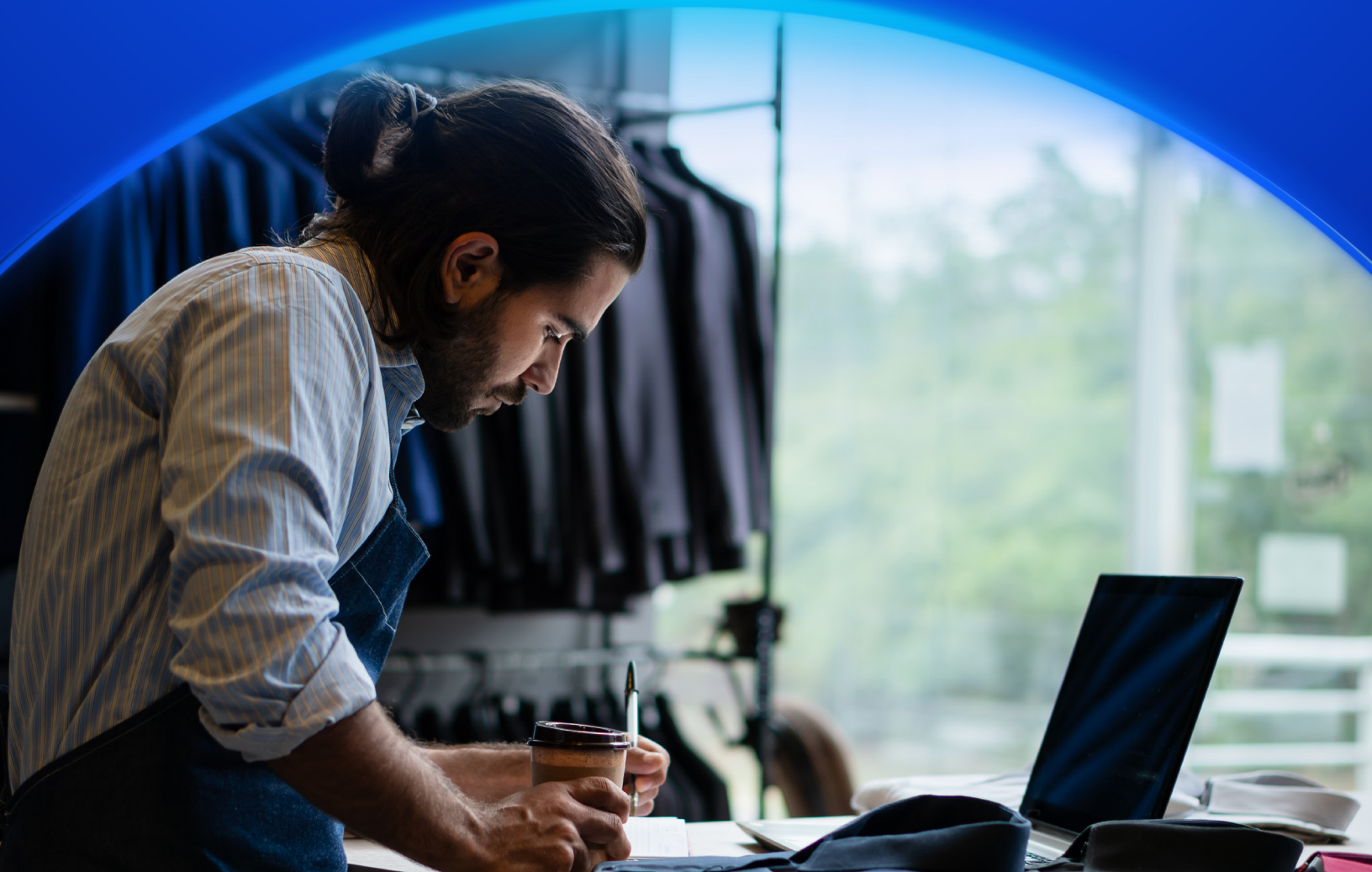
COMCAST
BUSINESS

Small Business Cybersecurity Guide



Introduction

Cyber threats don't just target large corporations. Small businesses face many of the same risks, but often with far fewer resources to defend themselves. And as small businesses become more reliant on technology, cyber threats are becoming smarter and harder to stop, especially with attackers using artificial intelligence.

The following guide shows small business owners how to adapt to these new risks by adopting practical cybersecurity tools, conducting regular employee training, and building a holistic culture of security.

This guide will help you:

- Learn how AI is changing the types of cyber threats small businesses face.
- Build a security culture that turns employees into your first line of defense.
- Avoid common mistakes that cyber-criminals exploit.
- Deploy layered technology, including firewalls, anti-virus, and threat monitoring, for stronger security.
- Establish clear cybersecurity practices for everything from password management to incident response planning.

CHAPTER 1

Why Small Businesses Are Targets for Cybercrime

Cyber threats are growing in both volume and complexity. Attackers are using increasingly sophisticated methods—including artificial intelligence—to scale operations, exploit vulnerabilities, and evade traditional defenses. And while attacks on large enterprises often make headlines, small businesses are far from immune.

In fact, small businesses are being targeted at nearly the same rate as large organizations. According to Cisco, 43% of all cyberattacks are aimed at smaller businesses. The impact, however, can be more severe. Often with fewer resources to recover, smaller businesses can face a greater risk of operational disruption, reputational damage, and financial loss.

Recent findings from the Identity Theft Resource Center show that over 80% of small businesses had been the victim of a cyberattack, data breach, or both during a 12-month period. Financial losses grew dramatically in 2024 compared to previous years, with reported losses of more than $500,000 doubling in one year.

Attackers go after small businesses because they often see them as “soft targets.” Unlike large enterprises with dedicated IT and security teams, small businesses typically have fewer security measures, less monitoring, and looser policies, making them easier to breach. They may also store valuable customer or financial data, process online payments, or act as entry points into larger supply chains, giving criminals multiple incentives to exploit them.

CHAPTER 1

Common Threats for Small Businesses

The types of threats small businesses face are varied and constantly evolving. Common attacks include:

Phishing

Deceptive emails or messages designed to trick recipients into revealing confidential information, such as login credentials, credit card numbers, financial details, or customer information.

Drive-by compromises

Visiting a compromised website triggers the download of malicious software, which can steal data, spy on activity, give attackers remote access to systems, or lock users out of systems.

Malware

Programs such as viruses or spyware used to steal or destroy data.

Ransomware

Malware that encrypts data and demands payment for its release.

Botnets

Networks of infected devices controlled by attackers and used to send spam, spread malware, or launch large-scale attacks. A single compromised device in a small business can unknowingly become part of a botnet, putting both the business and its customers at risk.

DDoS attacks

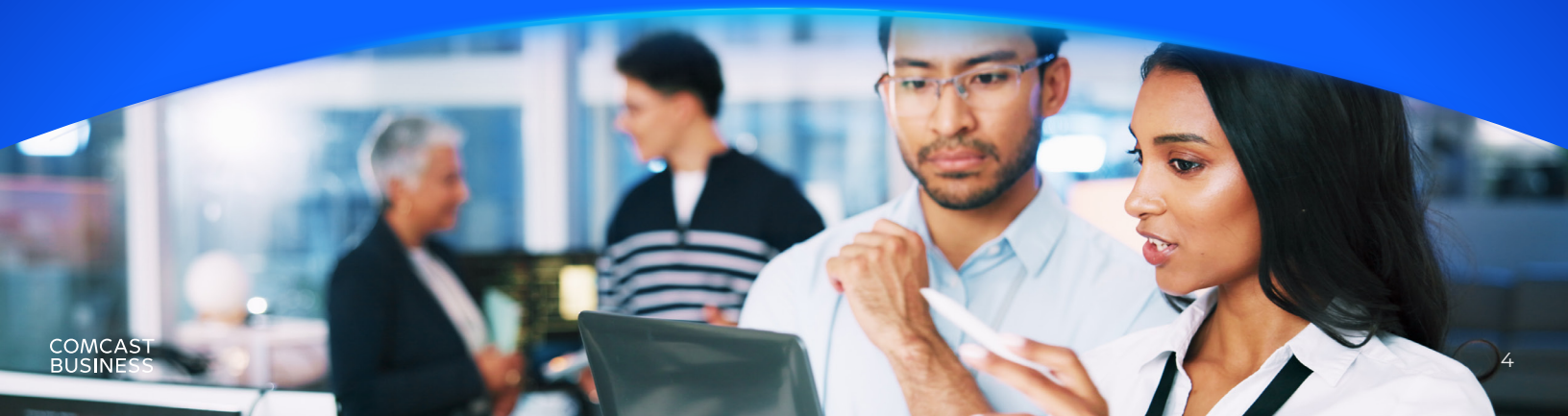
Distributed Denial-of-Service attacks (DDoS) send large volumes of traffic to a network to overwhelm systems and take down websites.

Over a 12-month time frame from June 1, 2024 to May 31, 2025 Comcast Business detected:

4.7 Billion
Phishing events

9.7 Billion
Drive-by compromise events

44,069
DDoS attacks

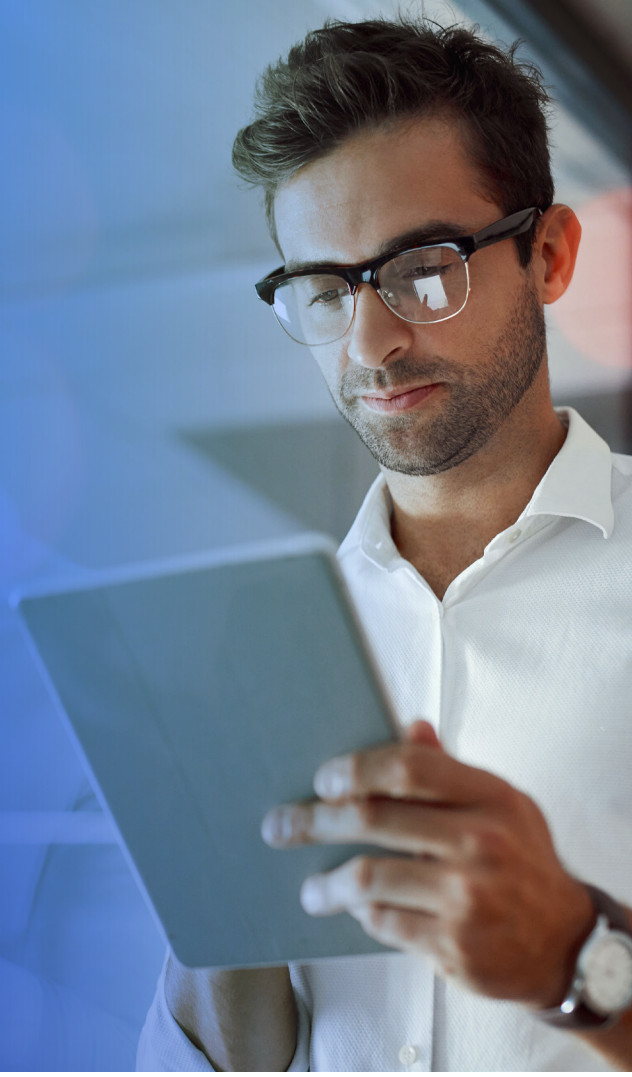


Best Practices to Reduce Risk

While no small business can eliminate every cyber threat, there are simple steps you can take to help protect against these attack types:

1. **Keep systems and software updated** to patch vulnerabilities that malware, botnets, and drive-by compromises often exploit.
2. **Educate employees on phishing recognition,** since so many attacks begin with a deceptive email or message.
3. **Use strong password practices and multi-factor authentication (MFA)** to reduce the chance that stolen credentials lead to broader compromise.
4. **Limit administrative access** so that if one device is infected, it can't easily spread across the entire network.

With the right mix of awareness, habits, and tools, small businesses can turn these risks into manageable challenges and build a stronger security foundation moving forward.



CHAPTER 2

How AI is Changing Cybersecurity for Small Businesses

Artificial intelligence is not just transforming industries—it's also changing how cybercriminals operate. Generative AI tools now allow attackers to launch faster, more convincing, and more widespread attacks with far less effort or technical knowledge than before. What once required coding, design, or writing skills can now be generated instantly with AI.

These AI-powered threats are especially dangerous because of their ability to exploit human behavior. They succeed not just by breaking through technical defenses, but by manipulating people into granting access or sharing sensitive information. Generative AI can craft messages that sound familiar, create fake profiles that look authentic, or impersonate voices that seem trustworthy.

Even cautious employees can be fooled when a scam appears to come from a colleague, vendor, or customer.

To help stay protected, your team must be able to recognize and respond to the most common forms of AI-driven threats:

Fraudulent content

With the help of generative AI, it is easier than ever to create phishing emails, fake business profiles, and websites that seem professional and convincing. According to McKinsey, phishing attacks have surged by 1,265% since generative AI platforms became widely available in 2022.

Deepfake videos and voice scams

Attackers are now using AI-generated audio and video to impersonate executives, employees, or vendors, often in urgent scenarios designed to manipulate the victim into acting quickly.

AI-generated fraudulent documents

From fake invoices to forged credentials, generative AI can help criminals create realistic-looking documents used in scams or unauthorized access attempts.

Taking a moment to evaluate and verify before acting can help stop scams. If an email, message, or request feels unusual or urgent—even if it appears to come from a trusted colleague or vendor—confirm it through another channel, like a phone call or direct conversation. Many AI-driven attacks rely on creating pressure and urgency, but pausing to double-check can stop a scam in its tracks.

CHAPTER 3

How to Get Your Team Threat-Ready

Cybercriminals rely on everyday behaviors to gain access, such as clicking on links, responding to messages, and sharing information. In fact, according to the Cybersecurity and Infrastructure Security Agency (CISA), more than 90% of successful cyberattacks begin with a phishing email. And a study by Visa found that three-quarters of small business fraud cases exploit people, not technology.

By building a culture where cybersecurity is seen as a shared responsibility, businesses can reduce risk at the earliest stages of an attack.

Establish clear, actionable cybersecurity policies that everyone in the organization understands.

These policies should be easy to follow and tailored to the specific risks your business faces. Resources like the FCC Small Biz Cyber Planner can help guide the creation of practical policies, especially for businesses without in-house expertise.

Make training an ongoing practice, not a once-a-year event

Cyber threats are evolving quickly—especially with the rise of generative AI—so it's important to keep employees informed and up to date.

Key training priorities should include:

Recognizing AI-enhanced phishing and scams
Train employees to approach every message, document, or request with healthy skepticism, no matter how professional or familiar it appears. Emphasize that they cannot trust anything on looks alone.

Identifying social engineering tactics
Help employees recognize the psychological manipulation techniques that attackers use to create urgency, confusion, or misplaced trust, such as pretending to be a colleague in distress or an irate manager.

Understanding deepfake risks
Raise awareness around fake voice messages or videos that impersonate trusted individuals.

Practicing verification and caution
Reinforce habits like verifying identities, double-checking links, and thinking twice before sharing sensitive information.

Promote Cybersecurity as a Shared Responsibility

Building a resilient small business starts with the understanding that cybersecurity is a team effort. When everyone feels ownership over keeping the business safe, your defenses become stronger from the inside out.

Make security part of daily routines and conversations
Security shouldn't be something people only think about during annual training. Small, regular reminders—such as discussing a recent phishing attempt in a team meeting or highlighting a good catch by an employee—help normalize cybersecurity as part of everyone's job.

Empower employees to report incidents without fear of blame
Mistakes happen, especially when attackers are using advanced tools to deceive people. What matters most is how quickly issues are reported. Leaders should emphasize that no one will be punished for falling for a scam if they come forward promptly. A quick report can mean the difference between stopping a breach and suffering a costly loss.

Reinforce the idea that there are no "bad questions" when it comes to staying safe
Security threats evolve quickly, and even seasoned employees might hesitate to ask for help if they're unsure. Encourage open dialogue and curiosity. A simple question, like "Does this email look right to you?", can prevent a major incident. The more supported people feel, the more likely they are to speak up before a threat spreads.

CHAPTER 4

Ensure You Have the Right Technology in Place

Even the most security-aware teams can be susceptible to cyberattacks, and business leaders need the right technology to help limit security risks. The ideal cyber solutions should be easy to implement, require no specialized expertise to manage, and deliver proactive, scalable security.

These are some essential capabilities your security solution should provide:

Endpoint device detection
Helps protect business and customer data on network connected devices from malware, ransomware, botnets, phishing, and unauthorized traffic sources. These safeguards help strengthen your first line of defense before threats reach users.

Threat intelligence
Uses regularly updated global data to identify and prevent access to known malicious websites, phishing domains, and malware sources. This helps block connections before they can cause harm.

Antivirus
Helps protect devices from malicious software by identifying and removing known threats like viruses and malware.

Password management
Simplifies the creation and use of strong, unique passwords across accounts, reducing the risk of breaches caused by weak or reused credentials.

Small businesses should consider solutions that are easy to manage and give business leaders clear visibility into malicious activity, making it easy to set policies and receive timely alerts when something looks suspicious.

For many small businesses, an effective option can be enlisting a trusted cybersecurity partner who provides enterprise-grade solutions without requiring in-house expertise. Partnering in this way ensures you have access to advanced defenses, expert oversight, and scalable security that can grow with your business.

CHAPTER 5

Creating an Incident Response Plan

Even with strong defenses in place, no system is completely immune to cyber threats. That's why every small business needs an incident response plan: a simple, clearly defined set of steps to follow when something goes wrong. The goal is to minimize disruption and restore normal operations as quickly as possible.

Most importantly, a well-prepared plan empowers your team. When a cyber incident happens, time matters. Confusion and hesitation can turn a small issue into a major disruption. In the stress of a real incident, clarity and confidence can make all the difference.

This three-step response plan is clear and simple to follow under pressure:

01. **Define what counts as a security incident**
Start by establishing what types of events should trigger a response, such as a suspected phishing email, a ransomware notice, or unusual network activity. Clear definitions prevent confusion and enable timely action.

02. **Assemble a response team and clarify roles**
Designate a small group of people to be responsible for handling incidents. Who should be notified first? Who contacts your service providers or vendors? Who communicates with employees or customers? Assigning these roles in advance ensures a faster, more coordinated response.

03. **Map out your recovery steps**
Think through how you'll isolate affected systems, preserve evidence, restore backups, and resume business operations. Include contingencies (e.g., what to do if customer data is exposed or systems are offline for several hours).

An incident response plan doesn't need to be complicated, but it does need to be documented and practiced periodically. With a clear plan in place, small businesses can tackle cyber threats quickly and confidently.

Practical Small Business Security with Comcast Business SecurityEdge®

Cybersecurity doesn't have to be complex to be effective. Solutions like Comcast Business SecurityEdge give small businesses a simple yet powerful way to help protect their networks and connected devices.

SecurityEdge® helps defend against malware, ransomware, phishing scams, and botnet attacks by using advanced global threat intelligence that updates every five minutes.

Activity can be monitored in real time through a personalized dashboard, and businesses can set custom controls—including web filters, blocked pages, access settings, and scheduled reports—all in one place. No additional hardware or complex installation required other than Comcast Business Internet and a compatible router.

By pairing human awareness with smart, scalable tools like these, small businesses can take real, measurable steps toward cybersecurity resilience.

Learn more about how SecurityEdge® can help protect your business today.

Learn more

COMCAST BUSINESS