Business Banking

The Small Business Owner's Guide to Cybersecurity

Protecting Financial Data from Hackers

PNC BANK | BRILLIANTLY BORING SINCE 1865℠

Table of contents

Decoding the modern threat landscape

Smarter Tech, Smarter Threats: Cyberattacks Targeting Small Businesses

A cybersecurity threat is any malicious act meant to disrupt digital systems, compromise sensitive information or steal data, including financial assets. As small businesses embrace smarter, cloud-based technologies, cybercriminals are keeping pace with more sophisticated attacks designed to exploit them.

The result is a threat landscape that isn't just expanding — it's evolving. Cyberattacks are now faster, harder to detect and increasingly fueled by artificial intelligence (AI).

For small businesses, this evolution may translate into heightened exposure to several cybersecurity risks.

Social Engineering Attacks

One of the most common (and effective) ways cybercriminals target small businesses is through social engineering. This broad term describes attacks that work by manipulating people, rather than directly hacking into systems, to infiltrate an organization.

These scams trick recipients into revealing confidential information, such as passwords, or into sending criminals money. Social engineering also encompasses other common cyberattacks, such as phishing and business email compromise (BEC) scams, which we'll define in detail next.

Phishing Schemes

A frequent type of social engineering, phishing schemes involve attackers posing as trusted institutions — like banks, service providers or employers — to collect sensitive information via email, text or phone.

For example, a fraudulent email may instruct staff to update their login credentials on a fake employer portal. Once the link is clicked, the attacker may collect any personal information entered, such as email addresses, account numbers, passwords or even Social Security numbers.

In 2024, there were 193,407 confirmed reports of phishing schemes, resulting in $70 million in stolen funds.[1]

Business Email Compromise (BEC) Scams

Phishing often serves as the entry point for BEC scams, which target organizations that regularly send or receive digital payments, such as suppliers, distributors, vendors, and real estate firms.

In these scams, attackers compromise legitimate business email accounts and pose as trusted contacts. They may request unauthorized payments, financial data, or personal information, or transfer company funds to their own accounts.

Generative AI

Attacks on the rise

The Federal Bureau of Investigation (FBI) warns that today's cybercriminals are using generative AI to sharpen deception tactics and scale financial fraud schemes.[2] These tools may be able to craft convincing emails, chatbot responses and even audio files that mimic real people, making it tougher than ever to spot a scam.

$6.3B

Of the 21,442 BEC scams reported in 2024, businesses lost upwards of $6.3 billion, with a median loss per incident of $50,000.[3]

Wire Fraud

BEC scams may also lead to broader schemes like wire fraud, which exploit electronic communication — such as emails and texts — to scam victims out of money or sensitive data.

Common entryways include real estate transactions, in which scammers impersonate brokers or property owners to request fraudulent transfers. Real estate wire fraud alone accounted for $173,586,820 in losses in 2024.[1]

Malware Attacks

While social engineering manipulates human behavior, malware attacks compromise systems directly. Short for malicious software, malware is designed to infiltrate a device and alter or damage the data, or spy on the user.

Most attacks require the user to click on a link or download a file, which allows the software to be installed. From here, it may spread across the victim's network.

Ransomware, a subset of malware, locks a user's systems until a ransom is paid. The financial toll of these attacks is steep. In 2024, reported ransom payments totaled $813 million worldwide.[4]

The impact also falls disproportionately on smaller organizations: Ransomware appeared in 88% of breaches at small and midsized businesses, compared with just 39% at larger organizations.[3]

Tech Support Scams

Malware may attack system health, but tech support scams do little to remedy the damage. In these schemes, cybercriminals pose as system support specialists to trick businesses into granting remote system access or sending payments.

Victims believe they're receiving help — until funds or data go missing. And missing they do go: Tech support scams generated $1.46 billion in losses last year.[1]

Denial of Service (DoS) Attacks

Some cybercriminals don't aim to steal data but to disrupt business operations instead. A Denial of Service (DoS) attack overwhelms systems with illegitimate traffic, making websites or services temporarily unavailable.

These attacks often force systems to go offline, leaving organizations vulnerable to other types of cybercrime. During the downtime, competitors may gain an advantage as customers seek services elsewhere.

Among small and medium-sized businesses, the median DoS attack size has grown by over 200% since 2018. The top targets include finance (35%), manufacturing (28%) and professional services (17%).[3]

Why Small Business Financial Data Is a High-Value Target

For most cyberattacks, the endgame is simple: **profit**. Financial data — such as payment details, bank account numbers and personal identifiers — offer hackers a direct path to cash, whether through unauthorized transactions, fraudulent purchases or resale on the dark web.

It's not just direct theft that's rising, either. Identity theft losses climbed to $174 million, credit card and check fraud reached $199 million, and investment fraud ballooned beyond $6.5 billion in 2024.[1]

Cryptocurrency-related crimes have surged to more than $9.3 billion, an astronomical leap for a crime category that wasn't even on the FBI's radar until 2017.[1] For cybercriminals, financial data is the ultimate prize. Small businesses just happen to be the prime target.

Small businesses are high on the hit list. In 2024, companies with fewer than 1,000 employees were targeted four times as much as large organizations. Of the 3,049 confirmed cyberattacks, data was exposed in 2,842 of them. The motive in 99% of the breaches? Financial.[3]

Identifying your system vulnerabilities

Common Risk Areas for Today's Small Businesses

Cybercriminals are unlocking more backdoors to business operations — and more weak points to exploit. Vulnerabilities now account for one in five successful breaches, a share that's been climbing year over year.[3] Over time, certain patterns of vulnerabilities have emerged across small businesses.

Weak passwords

More than 80% of data breaches trace back to compromised passwords, and over half of passwords are reused across accounts.[5] Passwords that are duplicated or consist of basic combinations of employees' names and birthdays simply aren't secure anymore.

Lack of employee training

Employees who aren't trained to create strong passwords and spot phishing emails, suspicious links or social engineering attempts may unintentionally open the door to hackers.

Outdated software

Nearly 30% of breaches are now linked to third-party involvement, including unpatched software. This vulnerability has doubled from the previous year.[6]

Unsecured Wi-Fi

Open or poorly secured networks often make it easier for hackers to intercept sensitive data and access confidential systems.

Self-Assessment Checklist: Is Your Business Exposed?

Uncovering potential vulnerabilities often starts with asking the right questions. The following checklist may help gauge whether there are **opportunities to strengthen protections** for company and customer financial data:

- Do employees reuse passwords across accounts?
- Are passwords updated regularly (e.g., once every four months)?
- Is multi-factor authentication (MFA) in place (i.e., email or text)?
- Is cyber threat training included in employee onboarding?
- Are vendor and third-party security practices reviewed?
- Are Wi-Fi networks encrypted and password-protected?
- Are emails from outside the organization flagged?
- Is outdated software or equipment still in use?

Insights from a checklist like this may help inform the cybersecurity measures your business chooses to prioritize.

Implementing best practices for financial data protection

Access Control and Password Hygiene

Weak or shared passwords have been the culprit in countless small business breaches. One way to help reduce this risk is by limiting system access to authorized personnel only. This may include assigning unique accounts with role-based permissions so each user may access only the functions necessary for their role.

Some organizations also limit administrative privileges to trusted IT staff, which may make it easier to track activity if a breach occurs. Others choose to lock unattended devices, such as laptops or tablets, to further reduce exposure.

When it comes to passwords, many businesses opt for strong, unique credentials of at least 16 characters. Some request password resets every 90 days, with old passwords retired and password "hints" disabled. And because passwords are only one layer of protection, other businesses tack on additional safeguards like multi-factor authentication.

Multi-Factor Authentication (MFA)

Cybercrime experts note that MFA may be a strong deterrent against certain types of attacks.[7] This extra step — whether it's a text code, app prompt or security question — makes it far harder for hackers to use stolen credentials.

Consider checking with vendors and financial institutions to see if MFA can be enabled across accounts. PNC Small Business customers, for example, have access to two-step verification and security questions to safeguard financial data.

Software Updates and Patch Management

Beyond flimsy passwords and access control, outdated software was behind a surge in last year's data breaches.[7] In response, some organizations now prioritize updates for operating systems, web browsers and security software as soon as they're available.

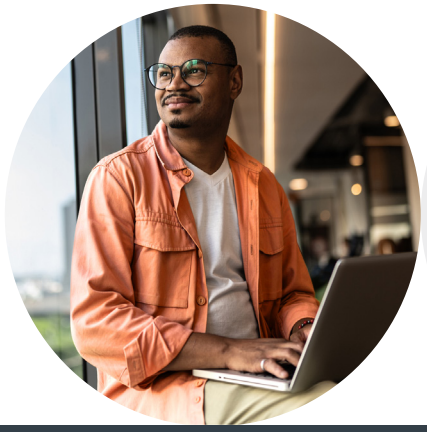
Many also set antivirus software to scan for malware and other threats after each update, and work to deploy other key patches promptly. These updates may help close security gaps — but for many businesses, protecting their network itself is another high priority.

Network Security and Firewalls

Attackers can now exploit unsecured Wi-Fi networks. To help reduce this risk, the U.S. Small Business Administration advises encrypting Wi-Fi, hiding its Service Set Identifier (SSID) and locking down router access with a strong password.[7]

Firewalls — programs designed to block outsiders from unauthorized access to systems or data — may also be enabled on all devices, especially those used by remote staff. However, their effectiveness often depends on proper configuration and ongoing management, as poorly tuned firewalls may leave gaps in protection.

Paired with device encryption, these steps help add another layer of defense against unauthorized access.



Device Encryption and Endpoint Security

Lost or stolen devices may be a common entry point for breaches. Encryption scrambles data, rendering it useless to unauthorized users. To help protect financial data, some organizations use encryption that meets the U.S. government standard of 256-bit security. Security apps may also be installed to **block unauthorized access**.

In addition, having a clear protocol for reporting lost or stolen equipment may help speed response efforts. And for businesses that store large volumes of information, secure cloud storage may act as a safety net if devices are compromised.

Secure Cloud Storage and Backups

Data loss isn't always the result of theft; sometimes, it's due to hardware malfunctions, software glitches or other unexpected system failures. These risks have prompted many businesses to seek reliable ways to store and protect their information, such as partnering with reputable cloud service providers (CSPs), which often offer strong security measures.

However, no environment is completely risk-free. Cybercriminals are becoming more advanced in their attacks on cloud technologies, and CSPs can be a target as well. This makes it important for organizations to maintain awareness and take shared responsibility for the security of their data, whether stored on the cloud or in-house systems.

Backing up critical files to both secure cloud storage and offline devices may provide an additional layer of protection. Likewise, safeguarding transactional systems and financial processes often helps keep daily operations running smoothly, even when disruptions occur.

Safeguard Payment Processing

Payment fraud remains one of the most common small business cybercrimes. To combat this, many businesses work with their bank or processor to explore anti-fraud tools such as role-based user permissions and real-time transaction monitoring.

On the staff side, some teams choose to keep payment systems isolated from general internet use to reduce potential exposure. Combined with strong access controls, network protections and reliable backup processes, these steps may help to strengthen overall financial data security.

Training employees and developing internal policy

The Importance of a Human Firewall

Think of your employees like a human firewall: the physical barrier that supplements the digital ones you've put in place. Even with strong encryption and network security, risks may remain if the people using them aren't equipped to recognize threats.

In other words, while technology may create the shield, employees may influence whether it holds. Awareness training often helps staff take on a more active role in security.

Sample Cybersecurity Policies and Protocols

Whatever tactics cybercriminals use, having documented policies in place helps give employees a clear reference point if a breach occurs. Below are a few common protocols many organizations review during training that you could consider implementing.

Password Policy

Provide a policy on how to create strong passwords and when to change them to prevent unauthorized access.

Example: Require passwords with at least 16 characters, including at least one letter, number and symbol. Passwords must be changed every 90 days.

Access Control Policy

This policy describes who can access which systems and data, and when access should be changed.

Example: Immediately remove system access for employees who leave the company (voluntarily and involuntarily) or change roles.

Acceptable Use Policy

This policy defines how employees can use company devices and networks, ensuring they avoid activities that could expose the organization to risk or legal issues.

Example: Prohibit the use of work devices for personal file downloads or to access unsafe websites.

Tips for Training Staff to Recognize Red Flags

Your team's daily habits may either strengthen or weaken your defenses. Therefore, many organizations find it useful for employee cybersecurity training to address these topics.

Identifying Phishing Emails

Spotting signs like suspicious senders (e.g., those flagged as "not in your network") and urgent, high-pressure requests

Opening Attachments Carefully

Knowing when to avoid unexpected files, especially from unknown senders or those without a preview window

Verifying Links

Hovering over links to preview and verify the destination URL before clicking to unknown or risky sites

Being Cautious with Software

Recognizing approved applications, trusted sources and the risks of unsolicited "update" prompts from unfamiliar devices

Recognizing Social Engineering Tactics

Questioning unusual requests, even from known contacts, and confirming them through another channel if unsure

Reporting Incidents Immediately

Following a clear process for escalating suspicious activity to management

Incident response: What to do if you're breached

Five Steps Small Businesses Prioritize After a Breach

If your organization experiences a breach, the first few hours matter most. A swift, coordinated response may limit damage, protect your financial data and accelerate recovery.

An incident response plan outlines exactly who does what — and when — in the event of a cybersecurity breach. Many small business plans include these five steps:

1) Identify and Contain the Threat

Many organizations start by determining how the breach occurred and isolating affected systems to prevent further spread. This may involve disconnecting compromised devices from the network and updating any passwords that may have been exposed.

2) Notify Your Bank, Your Vendors and Affected Parties

It's common to alert financial institutions and payment processors early to help block fraudulent transactions. Vendors, employees and customers whose data may have been involved are also typically informed right away.

3) Preserve Forensic Evidence

Every breadcrumb matters. Keeping a detailed record of how the incident unfolded — from error messages and suspicious files to system access logs — may be critical for determining the breach source. Even small details, such as unusual emails, may provide valuable clues.

4) Work with Cybersecurity Experts

Many businesses coordinate with qualified professionals to assess the breach, patch lingering vulnerabilities and confirm threats have been removed. Some also hire independent forensic investigators or legal counsel to review compliance with applicable federal and state regulations.

5) Minimize Damage and Restore Operations

Recovery often begins with clean backups, followed by a fresh round of antivirus scans and security updates. Keeping stakeholders informed of progress may also support trust during the recovery phase.

How banks can support your cybersecurity efforts

Stronger Together in the Fight Against Cybercrime

When it comes to protecting financial data, you're not in the fight alone. While you may turn to IT teams or cybersecurity vendors first, your bank continues to be one of your most valuable allies.

Financial institutions are on the front lines of fraud detection every day — monitoring millions of transactions, building advanced authentication tools and educating customers on evolving threats, just as we're doing now.

With financial data a prime target for cybercrime, no partner is better positioned to help protect your business than the institution that handles your money. Here's how banks like PNC may strengthen your defenses.

Business Banking Platform Security Features

Your bank's online and mobile platforms are more than just convenient; they're designed with layered safeguards to protect every small business transaction:

- Automatic session timeouts
- Role-based user permissions
- Real-time transaction tracking
- Multi-factor authentication (MFA)
- Unique security questions

Treasury Management Services

Beyond strengthening cash flow, treasury management may help reduce fraud risk. For instance, **PINACLE® treasury management solutions** from PNC allow you to monitor and manage banking activity from anywhere you have internet access, so nothing goes undetected.

Concerned about fraudulent wire transfers or unauthorized payments? Transaction limits restrict the size or frequency of transfers, while dual authorization requires two people to approve high-value transactions.

Educational Resources and Support

Banks may also serve as a trusted source of education and a partner in the event of a cyberattack. **PNC's Security & Privacy Center** is home to helpful advice for small business owners, including tips to spot impostors, online banking best practices and step-by-step instructions for **reporting fraud**.

Your PNC Relationship Manager or Treasury Management Officer may also walk you through payment fraud prevention tools and connect you to relevant resources — including ongoing articles on **PNC Insights** — to help stay informed as cybercriminals develop more sophisticated schemes.

Fraud Prevention Tools

Speaking of safeguards, banks offer a range of built-in tools, from ACH filters that block unauthorized debits to real-time account alerts and customized access controls. These tools may help spot suspicious activity early, giving you time to block hackers before they drain your accounts.

PNC Small Business customers receive access to **online fraud mitigation tools** such as:

Positive Pay Solutions

Display your check presentment information online to help proactively identify and respond to suspicious activity.

ACH Debit Authorization Solutions

Halt all ACH debits from posting to your account, or establish "rules" for filtering which ACH items post or are returned to the originator as unauthorized.

Universal Payment Identification Code (UPIC)

Hide your checking account number so your business can accept ACH credits without providing your PNC account number to the payment sender.

Building a long-term cybersecurity plan

Laying the Groundwork for Lasting Protection

Solid business defenses start with a long-term strategy. Whether you have a full IT team or are wearing the tech hat yourself, creating a clear, actionable cybersecurity plan may be helpful for identifying risks early, responding quickly and keeping sensitive financial data out of the wrong hands.

Over time, that plan should evolve alongside your business operations and the cyber threat landscape. Here are a few tips to do just that.

Scaling Smart: Partnering with the Right Experts

As your business grows, so do your vulnerabilities. It's helpful to invest in scalable security tools that may accommodate your team size and data usage.

Likewise, work closely with your bank, financial advisors and IT experts to ensure your protections match your needs — without overcomplicating your workflows.

Measuring Your Cybersecurity Maturity

It's wise to regularly evaluate your cyber defenses, from password policies to employee training programs, to identify strengths and weaknesses. Let this assessment create benchmarks that set realistic improvement goals to track progress year over year.

Following an Annual Cybersecurity Review Checklist

Want to keep defenses strong year-round? Many organizations revisit these areas as part of an annual cybersecurity review.

Incident Response Plan

Some teams run simulations to confirm every member knows their role in the event of a breach.

Employee Training Programs

Many organizations refresh materials with recent phishing examples or emerging threats to help maintain awareness.

Passwords and Account Access

Employees who periodically rotate passwords and review permissions may help ensure access stays appropriate.

Software and Security Tools

Many businesses stay current with updates to help close vulnerabilities before attackers have a chance to exploit them.

Data Backups

Several organizations test backup systems for speed and reliability to help confirm they'll perform in the event of ransomware or DoS attacks.

Bank Account Security Settings

Some business owners review MFA, transaction alerts and fraud monitoring tools as an extra layer of protection.

Proactive security powers business continuity

Cybercriminals are constantly finding new ways to access company and customer financial data — and the cost to small businesses has proven to be devastating. Staying ahead of these threats isn't easy, but you don't have to do it alone.

PNC Bank aims to be more than a place to store your money, serving as a trusted financial partner that prioritizes digital security, offers industry-leading fraud prevention tools and provides expert guidance to help you safeguard your most valuable information.

You don't have to be a tech expert to take steps toward protecting your business from cybercrime — having the right partner may help. Explore how PNC Small Business Banking may strengthen your defenses today and support your growth tomorrow. **Visit us online** to learn more.

1 Federal Bureau of Investigation Internet Crime Report 2024, Internet Crime Complaint Center, Apr. 23, 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

2 Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud, Federal Bureau of Investigation, Dec. 3, 2024, https://www.ic3.gov/PSA/2024/PSA241203

3 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot, Verizon Business, Jun. 12, 2025, https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

4 Total Annual Amount of Money Received by Ransomware Actors Worldwide from 2017 to 2024, Statista, Aug. 19, 2025, https://www.statista.com/statistics/1410498/ransomware-revenue-annual

5 FIDO Deploying Passkeys in the Enterprise, FIDO Alliance, Jun. 2023, https://fidoalliance.org/wp-content/uploads/2023/06/June-26-FIDO-EDWG-Spring-2023_Paper-1_Introduction-FINAL.docx.pdf

6 2025 Data Breach Investigations Report, Verizon Business, Jun. 12, 2025, https://www.verizon.com/business/resources/reports/dbir

7 Cyber Safety Tips for Small Business Owners, U.S. Small Business Administration, Sep. 26, 2023, https://www.sba.gov/blog/2023/2023-09/cyber-safety-tips-small-business-owners

BB PDF 0925-018-2741301