A practical cybersecurity and payments checklist

How accounting firms can build trust with each transaction

Introduction

How accounting firms can build trust with each transaction

Technologies such as artificial intelligence (AI) give firms an edge. But they also empower cyberattackers to strike faster than ever. Attackers abuse AI to send sophisticated phishing scams, crack passwords, and launch ransomware. Following security best practices and staying proactive can help protect your clients and your firm's reputation.

This practical, expert-backed checklist is designed to help your accounting firm secure its systems and data, fight fraud, and build lasting client trust.

Meet your experts

Donny Shimamoto

CPA, CITP, CGMA, Managing Director, IntrapriseTechKnowlogies LLC

Laura Redmond

Founder and CEO of Redmond Accounting Inc.

01 Configure email security

Why it's important

AI makes it easier for attackers to create phishing emails and documents that look real but are designed to trick you into sharing sensitive information, downloading malware, or making fraudulent payments.

How to get started

Enable content filters

In your email settings (e.g. Microsoft 365 or Gmail), turn on filters to block spam, malware, and phishing.

Activate phishing alerts

Ask your email administrator about alerts like "phishing email clicked" so you know when risks are detected.

Set up manual verification procedures

Never rely solely on email for payment requests or payment information changes. Set standards for cross-checking requests through a trusted, non-email method, and require that they're entered, reviewed, approved, and auditable in your AP platform.

02 Strengthen authentication

Why it's important

Attackers can steal weak passwords faster than ever with the use of AI. Options like multi-factor authentication (MFA) add an extra layer of protection to ensure only your team can access your systems.

How to get started

Enable MFA

In your important applications—such as accounting, email, and payment portals—go to settings and switch on two-factor (2FA) or multi-factor authentication (MFA). Many providers already require MFA, but confirm it’s enabled everywhere.

Choose MFA methods

MFA requires at least two of three factors: something you have (e.g., a security key or phone), something you know (like a password), and something you are (biometrics like facial recognition or fingerprint). Whenever possible, use an authenticator app instead of SMS for stronger security.

Require strong passwords

Include letters, numbers, and symbols. Avoid dictionary words and never reuse passwords across systems or apps. A passphrase, like iS!tNextToMary@Work, makes long passwords easier to remember but harder to crack.

Don’t share passwords

Prohibit password sharing.

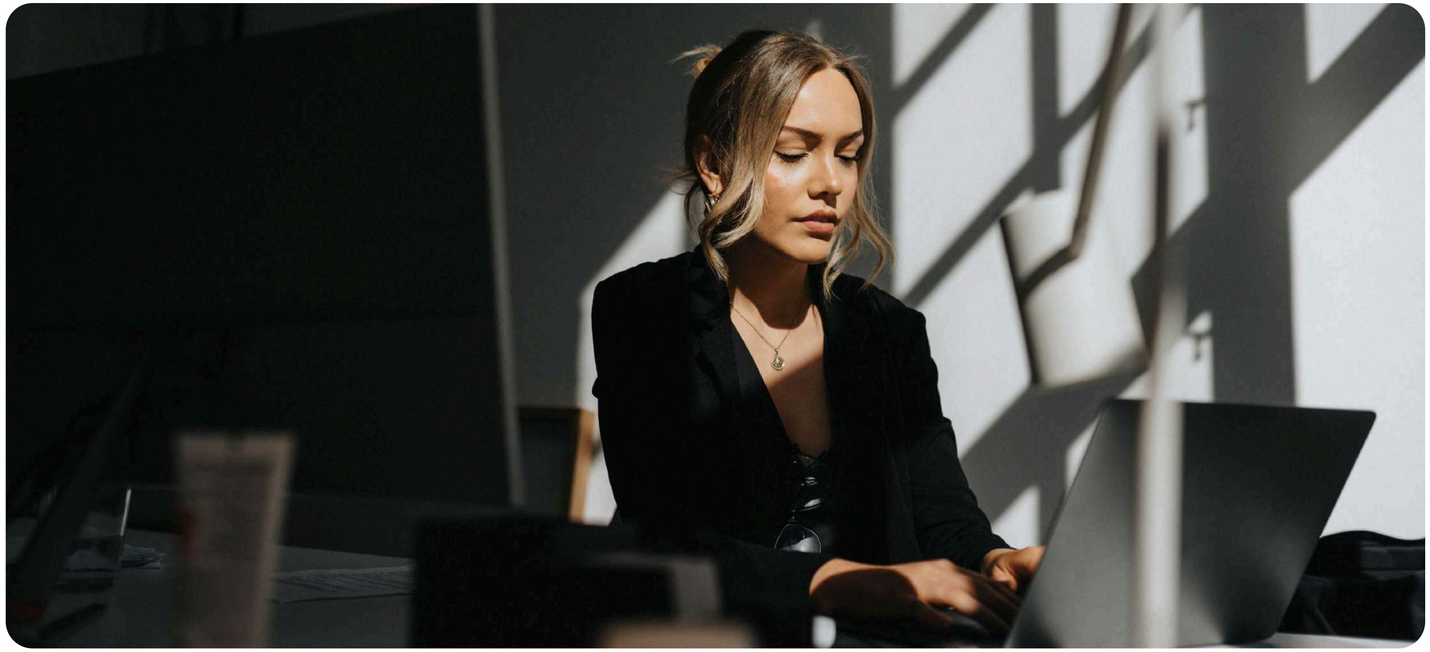
Use password management tools

Store passwords in a password manager, not in spreadsheets or text files. Managers help generate strong, unique passwords and often support MFA.

03 Restrict and monitor access

Why it's important

Limiting who can see or change critical data stops many attackers in their tracks. The fewer employees with access to critical systems, the harder it is for attackers to gain access.



How to get started

Adopt a least privilege and need-to-know policy

Give employees only the minimum access required for their role. Use role-based access control to limit permissions by job responsibilities.

Enforce separation of duties

Split responsibilities for data entry, posting, and custody of assets. For example, in accounting platforms, separate who can enter, approve, and pay bills. At minimum, ensure that staff who update vendor payment info can't also process payments—preventing them from redirecting payments to themselves.

Review access quarterly

Check permissions every quarter to ensure they still match employees' roles and adjust as needed.

Remove former employee access

Immediately deactivate accounts when staff leave.

Access auditing and logging

Check the access and activity logs in your software regularly for suspicious behavior.

04 Update software

Why it's important

Cybersecurity threats often target software vulnerabilities, so providers routinely release software updates to patch them. Apply these updates ASAP to protect your firm.

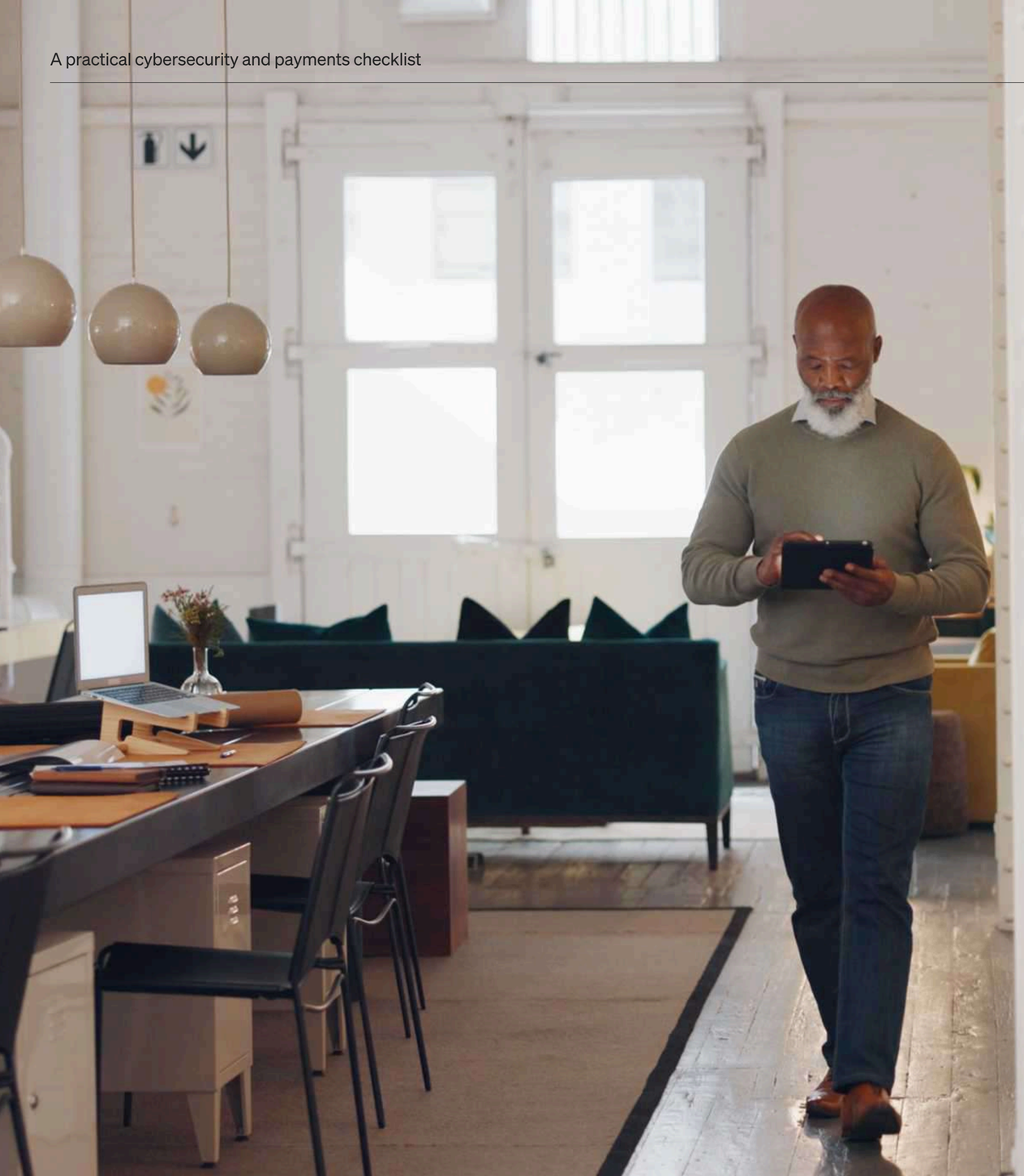
How to get started

Turn on automatic updates

Enable auto-updates for Windows, Mac, mobile devices, and software whenever possible. Make security updates mandatory and check regularly for failed updates.

Stay updated on technology

Schedule check-ins with your software providers to stay current with the latest features and updates.



05 Backup data

Why it's important

Regular backups are critical for recovering from system failures or cyberattacks like ransomware.

How to get started

Set up backups

Work with your IT team to back up all essential systems, especially those storing mission-critical data. Use built-in tools, on-site backups, and/or encrypted cloud services. If you already use cloud technology, see if additional backups are already in place. The best backup approach is the “3-2-1” rule: keep three copies of your data (the original plus two backups), on two different types of media, with one copy stored off-site.

Test restores

Twice a year, restore sample files to confirm backups work as intended.

06 Plan ahead

Why it's important

Preparedness and preventative actions limit fallout if you're the victim of a cyberattack or fraud.

How to get started

Create a concise cybersecurity policy

Use templates from reputable sources, such as the National Institute of Standards and Technology (NIST) or accounting associations.

Set data retention policies

Decide how long to keep client data, document it in a policy, and securely delete old files as the policy dictates.

Create an emergency protocol

Identify who to notify, basic triage steps (like disconnecting affected computers), and who to contact in case of a data breach or ransomware attack. Practice annually and make sure staff knows where to find the plan—both online and in print.

Look into insurance

Explore cyber insurance to help offset costs from an incident.

Have third-party vendor reviews

Set up a framework to assess vendor risks. Look at vendors' security practices, regulation compliance, and financial stability before working with them.

07 Focus on network and computer security

Why it's important

Most cyberattacks succeed because of poor network or computer security. Simple but proven security practices go a long way.

How to get started

Install antivirus and firewall

Use reputable antivirus software and confirm your operating system firewall is enabled. Modern antivirus tools detect threats by behavior, not just file signatures. Make sure every internet-connected device—even printers—runs protection.

Enable device encryption

In your computer and phone settings, turn on encryption (BitLocker for Windows, FileVault for Mac) so data stays locked if a device is lost or stolen.

Use strong network passwords

Set strong Wi-Fi and router passwords and ensure the passwords have been changed from the default/factory passwords. Limit guest access to your network. Many routers offer a guest network feature that should be used for visiting clients and employees' personal devices (e.g., phones).

08 Train employees

Why it's important

Informed staff are one of your strongest defenses.

How to get started

Provide onboarding education

Put new hires through a security orientation covering security basics and preparedness policies.

Offer training sessions

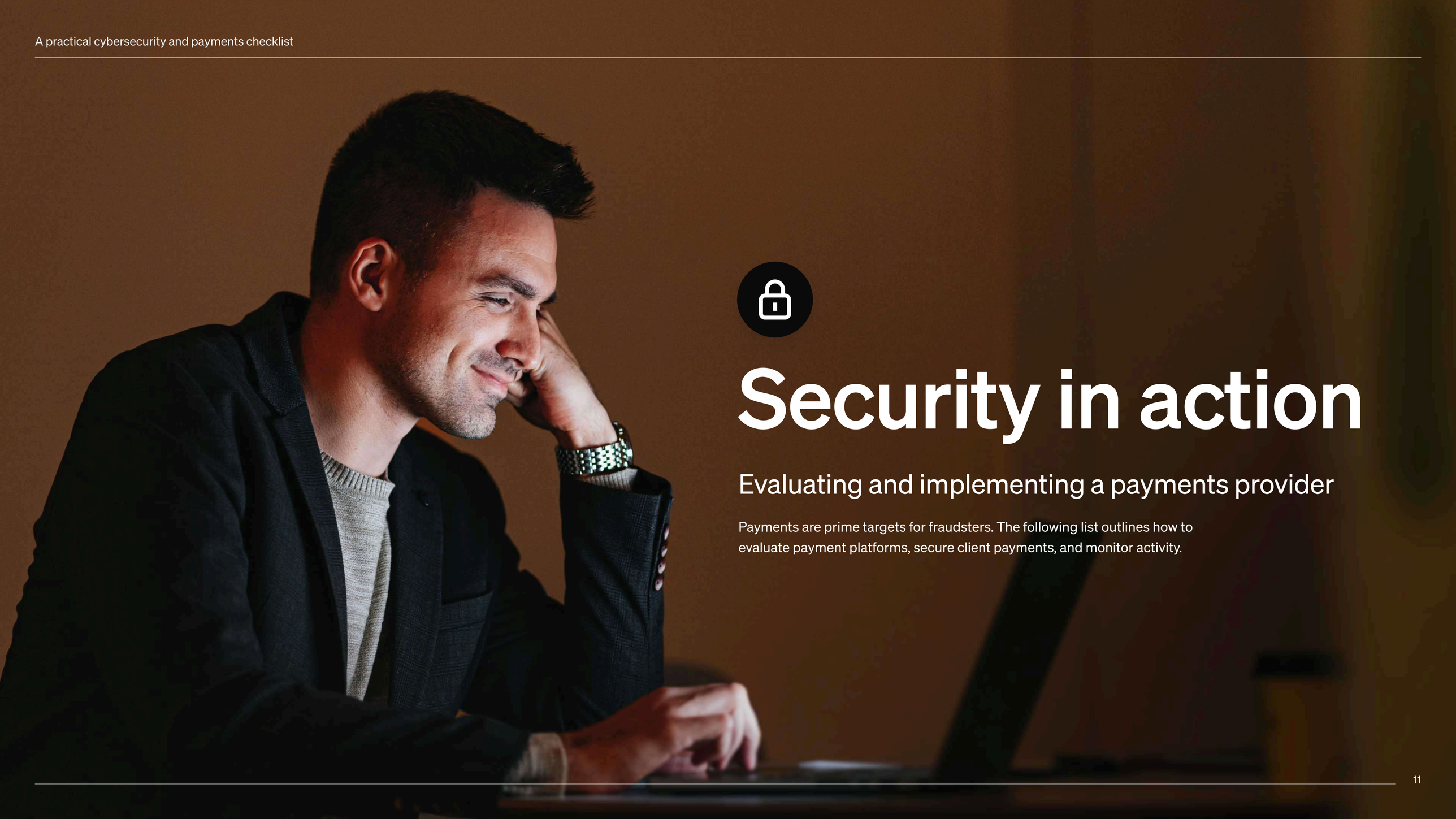
Use free resources from the National Counterintelligence and Security Center (NCSC), the Cybersecurity & Infrastructure Security Agency (CISA), or software providers to educate staff about the latest security threats and keep them updated on how they can help prevent threats.

Run periodic testing

Send phishing tests to keep staff fresh and aware year-round.

Simplify the reporting process

Tell employees how to report suspicious communications (email, phone, or secure portal). If sensitive info is ever shared by mistake, be transparent so remediation steps can follow.



Security in action

Evaluating and implementing a payments provider

Payments are prime targets for fraudsters. The following list outlines how to evaluate payment platforms, secure client payments, and monitor activity.

01 Select a secure payment platform

Why it's important

Financial operations platforms that follow industry standards can help detect and prevent fraud early.

Read the AP software selection checklist from CPA.com →

How to get started

Evaluate compliance

Providers should be compliant with SOC 1 and SOC 2, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

Review monitoring

Providers should monitor all transactions in real time and be able to spot complex fraud campaigns with speed and accuracy.

Know who issues payments

Find out if the platform processes payments in-house. Some outsource it to third-party services.

Offer physical protections

Servers and network infrastructure should be hosted at secure data center facilities managed by leading, certified data center providers.

Require encryption

Ask your provider where data is encrypted. Look for statements like “data encrypted at rest and in transit.”

Annual reviews

Put vendor reviews on your calendar each year. Ask for updated compliance reports and check for changes or incidents they may have experienced in the last year.

02 Safeguard client payments

Why it's important

Additional security measures provided by your payment platform make fraud much harder.

How to get started

Switch to digital payments

Digital payments are more secure than checks and show up in real time, so fraud gets spotted faster.

Deter check fraud

If you must send checks, use your financial operations platform. It hides client bank info and adds protections like Positive Pay.

Enforce the separation of duties

The system should ensure that each bill follows proper separation of duties before payment is authorized.

Manage corporate cards

Ensure your spend and expense software lets you deactivate and replace corporate cards quickly and easily. Set vendor and spend-category controls to reduce misuse.

Set spending guidelines

Have your spend and expense system automatically enforce your policies to prevent unapproved spending.

Use virtual cards

Assign a separate virtual card for payment to each vendor. That way, if the card is compromised, charges are limited to that one card.

Empower vendor self-management

Reduce fraud risk and ensure seamless payment accuracy by using a payment platform where vendors securely update their own delivery and banking details. This helps you avoid manual updates and exposure to sensitive data.

03 Monitor payments

Why it's important

Regular reviews catch issues before they grow.

How to get started

Review payment logs

Your platform should create an audit trail of transactions from review to payment.

Bank reconciliation

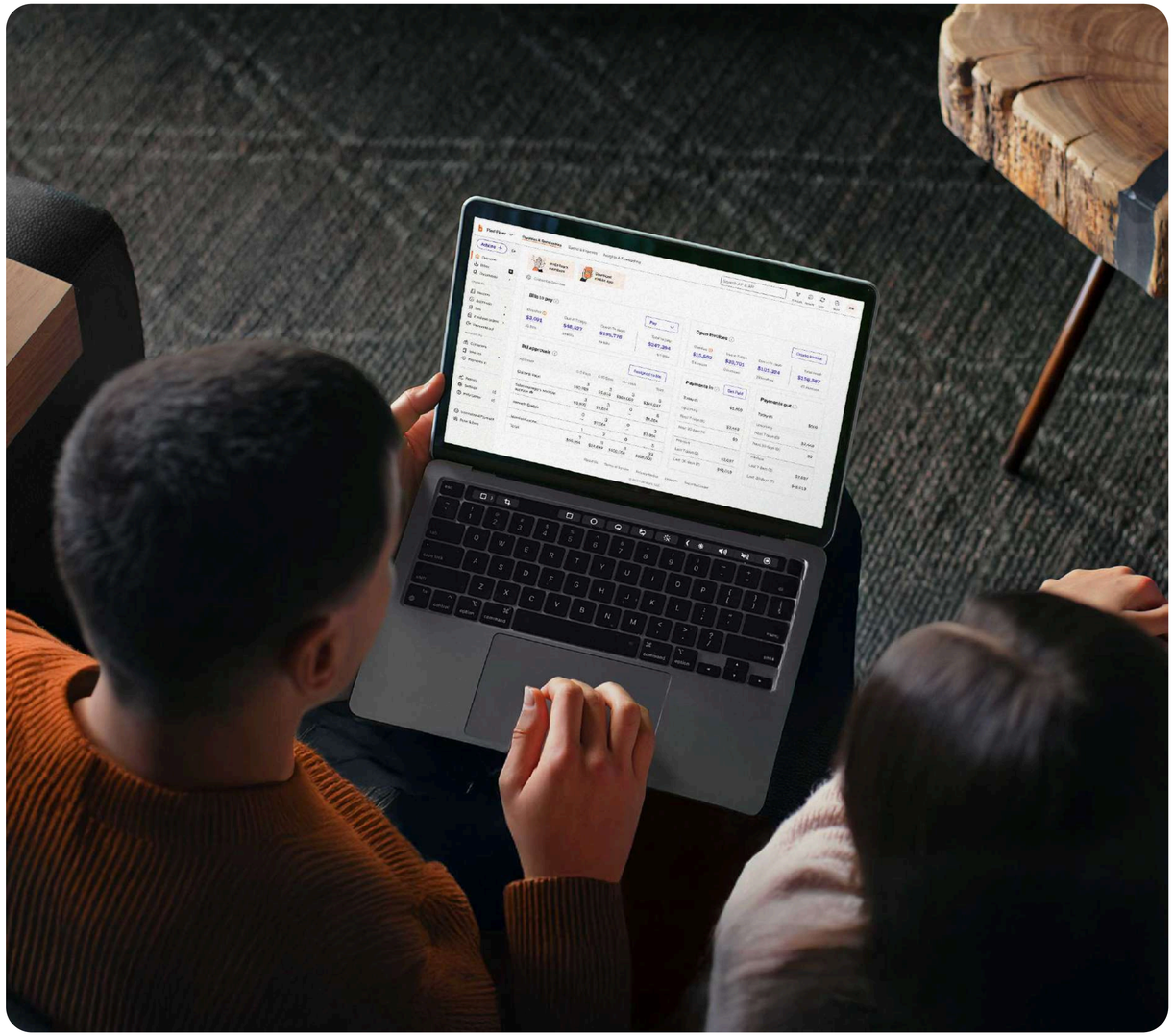
Compare your accounting system's payments to your bank feed weekly to catch unauthorized transactions fast.

Know your emergency contacts

Post your providers' fraud hotline and account manager details where staff can find them.

Conclusion

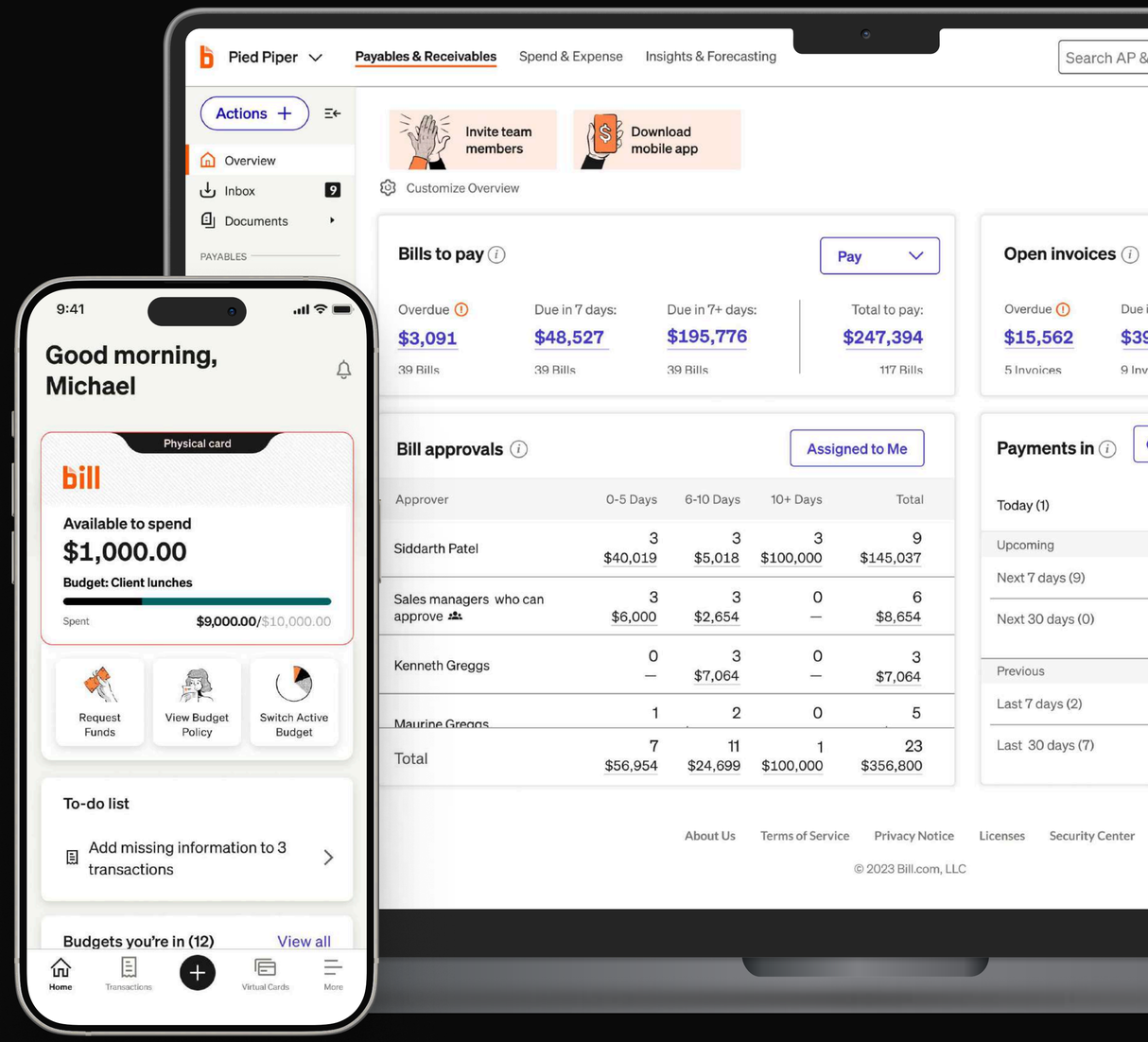
Staying secure in today's digital world takes vigilance, adaptability, and teamwork. Put these expert-driven steps into action to build strong defenses against cyberthreats and fraud to keep your business, employees, and clients safe. Remember, cybersecurity isn't one-and-done or a one-person job. Review, evolve, and train regularly.



Reduce risk, combat fraud, and keep your data secure with BILL Accounts Payable, Accounts Receivable, and Spend & Expense.

Learn more about BILL security, try a risk-free trial or request a demo.

Get started



Results from using the BILL platform may vary according to each company's goals, size and other conditions specific to them.