THREAT WATCH

Know the playbook before they call.

Most attacks on small businesses aren't clever. They're familiar. Here are the five patterns we see again and again, and the specific things that stop them.

01

Invoice and bank-detail fraud

A supplier emails to say their bank details have changed.

MOST COSTLY

The email looks like your supplier. It may come from their real address if their mailbox was compromised, and it may quote a real invoice number. The only change is the account the money lands in. By the time anyone notices, the payment has been forwarded and the money is gone.

RED FLAGS

- A supplier suddenly changes bank details, especially mid-project
- The email is slightly off: different tone, odd greeting, reply-to address changed
- Pressure to pay today because of a deadline or 'account review'
- New details arrive as a PDF attachment or in a thread that started normally
- The phone number in the signature is different from the one you already have

IF IT HAPPENS

- Call your bank immediately and ask them to recall the payment, speed matters more than anything else
- Call the real supplier on a number you already had, not one from the email
- Preserve the email and headers; don't forward it as an attachment to everyone
- Report it to the police / fraud reporting service and tell your insurer

STOP IT

- One rule: any change to bank details gets a callback to a known number
- Put the rule in writing and give it to whoever pays invoices

- Use dual approval for payments above an agreed threshold
- Ask suppliers at onboarding to confirm how they will ever communicate changes

02

CEO and gift-card impersonation

The boss needs gift cards, quietly, before a meeting.

FAST AND CHEAP ✕

A message appears to be from the owner or a senior manager: new number, urgent request, don't call because they're in a meeting. It asks for gift cards, a bank transfer or sensitive payroll data. The urgency and the secrecy are the whole trick.

RED FLAGS

- A senior person contacts you from a new number or personal email
- The request is urgent, unusual and asks you to keep it quiet
- They can't take a call, but can text or email freely
- Payment is requested in gift cards, crypto or a personal account
- The display name matches, but the actual email domain doesn't

IF IT HAPPENS

- Stop. Do not buy anything or send money
- Contact the person on a number you already have
- Tell a colleague, impersonation relies on isolation
- If money has gone, call the bank and report it immediately

STOP IT

- Agree that no urgent money request is actioned without a voice call
- Publish a simple approval rule for payments and purchases
- Train staff that 'the boss asked me to keep it quiet' is a red flag
- Use MFA and DMARC so your own domain is harder to impersonate

03

Fake IT support and MFA fatigue

"Hi, it's IT. We're seeing a problem with your account."

ACCOUNT TAKEOVER ✕

The caller knows your name, your company and maybe your manager's name. They want you to read out a code, approve a push notification or install a remote-support tool. Sometimes they skip the call and simply spam MFA prompts until you tap approve out of irritation.

RED FLAGS

- An unsolicited call about a security problem you didn't report
- A request to read out a code, approve a login or install remote software
- A number that looks internal but can't be called back
- Repeated MFA prompts you didn't trigger
- Pressure to act now and not to tell anyone

IF IT HAPPENS

- Hang up and call IT on a number you already have
- Deny any MFA prompt you didn't start; then change your password
- If remote software was installed, disconnect the machine and tell IT
- Check email rules and forwarding for anything you didn't create

STOP IT

- Agree that IT will never ask for your password or a code
- Use number matching or passkeys to stop prompt fatigue
- Use a helpdesk number published internally, not one from a message
- Give staff permission to hang up and verify, no blame

04

Payroll and direct-deposit diversion

An employee asks for their salary to go to a new account.

INSIDER-STYLE ×

The request looks routine: a change of bank details from a member of staff. It can arrive from the employee's real mailbox if that mailbox is compromised, or from a lookalike address. Payroll runs, the money leaves, and the real employee notices at the end of the month.

RED FLAGS

- A bank-detail change arrives by email only
- The request is urgent or timed just before payroll
- The writing style or signature differs from previous emails
- The reply-to address is different from the sender
- A new starter asks for an early payment to an unusual account

IF IT HAPPENS

- Pause the change and call the employee on a known number
- If paid, ask the bank to recall the transfer immediately
- Check the employee's mailbox for forwarding rules and sent items
- Reset their credentials and review any other payment changes

STOP IT

- Verify payroll changes in person or by phone, every time
- Require a second approver for payroll runs
- Tell staff you will never ask for bank changes by email alone
- Review payroll master data quarterly

05

The urgent document that isn’t

“Please see the attached remittance, password in the body.”

RANSOMWARE ×

A plausible business email carries an attachment or link: an invoice, a delivery note, a CV, a voicemail. Opening it runs malware that encrypts files, steals saved passwords or quietly installs remote access. The password in the email is there to get past email filters, not to protect you.

RED FLAGS

- An unexpected attachment, especially a ZIP, ISO or HTML file
- A password-protected archive from someone you don’t know
- A link to a login page that isn’t quite the right address
- A message about an unpaid invoice, delivery or CV you weren’t expecting
- A QR code used to ‘verify’ or ‘log in’

IF IT HAPPENS

- Disconnect the device from Wi-Fi and the network, don’t shut it down
- Tell IT or your provider immediately; don’t try to clean it yourself
- Use a different device to change important passwords
- Check whether backups are intact and offline before restoring anything

STOP IT

- Turn on automatic updates and endpoint protection everywhere
- Keep an offline or immutable backup and test a restore
- Disable Office macros from internet files by default
- Train staff to report unexpected attachments rather than open them

Check your own exposure →