THE INTERNET SURVIVAL GUIDE

for small business owners



What you'll find in this guide:

- Know Your Surroundings
- Your Survival Kit
- Your Biggest Threats
- Emergency Response

Powered by PHIN

KNOW YOUR SURROUNDINGS

What do these mean?

When your business relies on email, online banking, cloud software, customer information, and/or connected devices, there are a few things worth knowing.

- **MFA** (Multi-Factor Authentication): An extra security check at login, like a code sent to your phone.
- **Phishing:** A fake email that tricks someone into clicking, sharing info, or sending money.
- **Malware:** Harmful software that steals info, spies, or damages devices.
- **Ransomware:** Malware that locks your files so criminals can demand money.
- **BEC** (Business Email Compromise): Criminals impersonate or take over a business email to trick someone into sending money or data.

Major red flags to look out for:

🚩 **Urgency:** A payment, password reset, or request suddenly needs handling immediately.

🚩 **Changed payment details:** A supplier or customer asks you to use a new bank account.

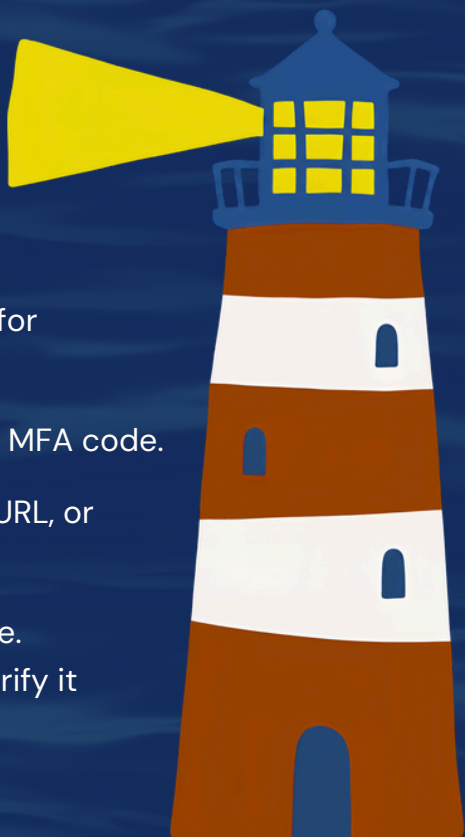
🚩 **Unusual requests:** Your employee, accountant, or supplier asks for something out of the ordinary.

🚩 **Passwords and codes:** Someone asks for login credentials or an MFA code.

🚩 **Something looks off:** A slightly different email address, strange URL, or unexpected attachment.

🚩 **Secrecy:** You're told to act without discussing it with anyone else.

If money, access, or sensitive info is involved and it feels unusual, verify it before acting.



YOUR SURVIVAL KIT

For help setting anything up, reach out to your IT provider or someone you trust.

Have a verification process. Decide how you'll verify payment requests, bank-detail changes, and password resets. A quick call beats an expensive email.

Use strong, unique passwords for every account. One stolen password shouldn't unlock your email, accounting software, social media, and everything else.

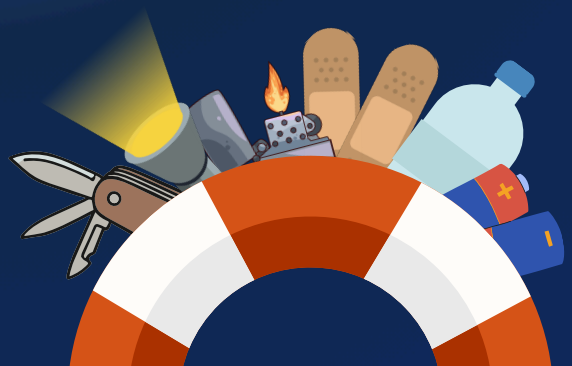
Keep everything updated. Turn on automatic updates. They fix weaknesses criminals exploit.

Use a password manager. It creates and stores strong passwords, and is far safer than a spreadsheet called passwords.xlsx.

Limit access. People should only have access to the accounts, systems, and information they need for their jobs. When somebody leaves the business, remove their access promptly.

Back up important data. Keep regular backups of the files and information your business couldn't operate without.
Make sure at least one backup can't easily be altered or deleted if your normal systems are compromised.

Set up MFA wherever possible, especially for email, banking, accounting, cloud storage, social media, and admin accounts. A stolen password is far less useful if it isn't enough to log in.



Before you click, pay, share, download, or approve:

ALWAYS PAUSE & PONDER

☐ Who sent this?

Check the *actual* email address, not just the display name.

☐ What are they asking for?

Money? Login credentials? Customer info? An MFA code? System access? The more valuable the request, the more carefully you should verify it.

☐ Why is this happening, and does it make sense?

- Was this invoice expected?
- Does this supplier normally change payment details by email?
- Would your colleague really ask for $1,000 in gift cards out of the blue?

☐ When does this need to be done?

Urgency makes people skip steps. An "emergency" is not a reason to skip verification. It's a reason to verify more carefully.

☐ How can I verify it?

Use contact details you already trust. If a supplier emails new bank info, call the number already in your records, not the one in the suspicious message.

YOUR BIGGEST THREATS

1 "WE'VE CHANGED OUR BANK DETAILS."

A familiar supplier sends an invoice but asks you to pay into a new account. The email looks legitimate because criminals compromised a real mailbox.

What should you do? Verify payment-detail changes with a contact method you already trust, never just the email.

2 "CAN YOU TAKE CARE OF THIS FOR ME?"

An employee gets an urgent email that seems to be from the owner or a senior colleague, asking for a payment, gift cards, or information. The sender knows names, roles, and enough about the company to sound convincing (usually information easily accessible online).

What should you do? Make independent verification part of your process for unusual or high-value requests, no matter who appears to be asking.

3 "YOU NEED TO LOG IN."

An email claims to be a shared document, missed voicemail, password-expiry notice, or Microsoft 365 alert. The link leads to a convincing fake login page built to steal your password.

What should you do? Don't log in through unexpected links. Open the service directly through your usual app or website instead.



4 "YOUR FILES HAVE BEEN LOCKED."

Ransomware can prevent you from accessing important business files and systems while criminals demand payment to restore them. It can begin with something as simple as a malicious attachment, compromised account, or unpatched device.

What should you do? Keep software updated, maintain secure backups, and be cautious with unexpected files. If ransomware hits, disconnect affected devices from the network and get expert help immediately.

5 "I'M FROM IT. I JUST NEED YOUR CODE."

Someone calls or messages an employee pretending to be from IT, a software provider, bank, or another trusted organization. They may already know enough about your business to sound legitimate.

What should you do? Never provide passwords or MFA codes to an unexpected caller. End the conversation and contact the organization through a trusted method.

6 "WE'VE GOT YOUR PASSWORD."

An employee reuses a password exposed in another breach. Criminals try it on their work email, and it works. From there, they can steal data, reset passwords, or target customers and suppliers.

What should you do? Use unique passwords and MFA. If an account is compromised, change the password, revoke active sessions, and check for unauthorized changes.

WHEN IN DOUBT, VERIFY IT WITH A QUICK PHONE CALL.

OH, CRAP. WE'VE BEEN HACKED.

Now what?

The first few actions after a cyber incident can make a big difference. Don't waste time looking for someone to blame. Focus on containing the problem.

STEP 1

Stop communicating and interacting with anything suspicious. Don't send more money or information.

STEP 2

Inform whoever handles your IT or cybersecurity with as much detail as possible. If customers, employees, suppliers, or other organizations could be affected, establish what happened before deciding what communication or notification is required.

STEP 3



If money was sent, contact your bank or payment provider immediately. Ask whether the payment can be stopped or recovered.



If an account was compromised, change its password, enable MFA, and revoke unfamiliar or active sessions where possible. Check whether account recovery details or forwarding rules have been changed.



If a device was compromised, disconnect it from your network and get expert technical support.



If business data may have been accessed, preserve evidence and get appropriate professional advice. You may have legal, contractual, or regulatory obligations depending on what happened and where you operate.

STEP 4

Train your employees to ensure the same mistake doesn't happen again.