ARK Care

From the ARK Computer Repair workshop

Business safety pack

Free, plain-English guides to keep you safe online

Not sure about a message, email or call?

Call 01329 623 555

We'll tell you if it's a scam, free of charge. arkcare.uk

What's inside

When you are the business, one scam or one dead laptop can stop the work. These are the threats we see hitting tradespeople, freelancers and small shops, and the simple steps that stop them.

1. Scams to watch out for
2. Invoice fraud: "our bank details have changed"
3. HMRC and Companies House scams aimed at small businesses
4. Protecting your business email
5. Backing up your business files and accounts
6. Using your phone for work safely
7. Protecting a small business from cyber attack
8. Ransomware: how it gets in and how to survive it
9. Need a hand?

Scams to watch out for

"Our bank details have changed"

What it looks like: An email from a supplier, or a fake copy of your own invoice sent to a customer, with new bank details.

What to do: Always ring to confirm new bank details on a number you already have. Put "we never change bank details by email" on your invoices.

HMRC and Companies House demands

What it looks like: A message about a tax refund, a penalty, or a fee to "renew" your company registration.

What to do: Log in through gov.uk yourself. Forward HMRC scams to phishing@hmrc.gov.uk, or texts to 60599.

"You have a document to review"

What it looks like: An email that takes you to a Microsoft or Google sign-in page to open a shared file or invoice.

What to do: Check the address bar before typing your password. Turn on two-factor sign-in so a stolen password isn't enough on its own.

Google listing and domain renewal calls

What it looks like: A caller says your Google listing will be removed, or an invoice arrives for a website domain you don't recognise.

What to do: Google doesn't cold-call to sell listings. Check your domain renewal only with the company you actually registered it with.

Invoice fraud: "our bank details have changed"

An email arrives from a supplier you know, saying their bank details have changed. Or a customer pays your invoice, but the money never arrives, because they received a copy with different details on it.

This is payment diversion fraud. It often happens because someone has got into one of the email accounts and is quietly watching for invoices.

The one check that stops it

Whenever bank details change, ring the person on a number you already have — not one in the email — and confirm the new details before paying.

Tell your own customers that you will never change your bank details by email, and put that line on your invoices.

Warning signs

- A request to update bank details, especially with urgency
- A sender address that's one letter different from the usual one
- A customer saying they've paid when nothing has arrived
- Emails in your sent folder or rules in your mailbox you didn't create

If money has gone

Call your bank immediately — the sooner, the better the chance of recovery. Report it to Action Fraud on 0300 123 2040, then change your email password and check for forwarding rules.

HMRC and Companies House scams aimed at small businesses

If you're self-employed, your details are easy to find, and scammers know when tax deadlines fall. Messages threaten penalties, promise refunds, or ask for a "filing fee".

Common versions

- A text or email about a tax refund with a link
- A call threatening arrest or court for unpaid tax
- A letter or email asking you to pay to "register" or "renew" with Companies House or a trade directory
- A request for your Government Gateway login

How to check

Log in to your HMRC or Companies House account yourself through gov.uk. Anything genuine will be there. HMRC publishes a list of genuine contact methods on gov.uk, which is worth checking.

Never give your Government Gateway login or code to anyone who contacts you.

Reporting

Forward suspicious HMRC emails to phishing@hmrc.gov.uk and texts to 60599. Other scam emails can go to report@phishing.gov.uk.

Protecting your business email

For a one-person business, the email account holds invoices, customer details and the password reset for nearly every other account. If someone gets in, they can take over all of it.

The essentials

- Turn on two-factor authentication for your email, ideally with an app
- Use a long password that you don't use anywhere else
- Check sign-in activity every so often for logins you don't recognise
- Look for mailbox rules that forward or delete emails — criminals add these
- Keep a separate personal email for recovering the business account

Fake login pages

A common trick is an email saying "you have a document to view" or "your mailbox is full", with a link to a page that looks exactly like Microsoft or Google. Always check the address bar before typing your password, or go to the site yourself.

Use your own domain

An address at your own business name looks more professional than a free email account, and it lets you set up email security records that make it harder for others to pretend to be you.

Backing up your business files and accounts

When you're the whole business, a lost, stolen or broken laptop can stop work completely. You also need to keep business records for HMRC, usually for at least five years after the Self Assessment deadline.

What to back up

- Invoices, quotes and receipts
- Customer and supplier contact details
- Photos of jobs and work in progress
- Any accounting files kept on the computer
- A list of the online accounts and software you use

A setup that works

Keep everything in a cloud service, plus a separate backup that keeps older versions. That second copy is what saves you if ransomware or an accidental delete hits the cloud copy too. Test it now and then by restoring a file.

Phones count too

If you take job photos or quotes on your phone, make sure the phone's backup is switched on as well.

Using your phone for work safely

Many sole traders run the whole business from a phone: email, banking, invoicing apps, photos and customer messages. That makes the phone very valuable, both to you and to a thief.

Set these up today

- A screen lock with a PIN of six digits or more, plus fingerprint or face unlock
- Automatic updates switched on
- Find My iPhone, or Find My Device on Android, switched on
- Apps installed only from the official App Store or Google Play
- Automatic backup of photos and contacts

Messages and calls

Be wary of texts about missed parcels, unpaid tolls or fines, and of WhatsApp messages asking for a code. Customers' numbers can be spoofed too, so check any change of payment details by ringing a number you already have.

If it's lost or stolen

Use Find My to lock it and erase it if needed, ring your bank, and change your email password from another device. Ask your mobile provider to block the SIM.

Protecting a small business from cyber attack

Small businesses are targeted precisely because they're small: valuable enough to extort, rarely defended well enough to make it difficult. Attackers don't pick you personally — automated tooling finds exposed and unpatched systems at scale.

The good news is that the defences that work are not exotic. A handful of unglamorous measures stops the overwhelming majority of what we actually see.

How attacks actually start

Nearly every incident we deal with begins in one of a few ways.

- A convincing phishing email that harvests an email password
- A reused password exposed in someone else's data breach
- An unpatched machine or remote access tool exposed to the internet
- A malicious attachment or download opened by a member of staff
- An invoice fraud email sent from a genuinely compromised supplier mailbox

The measures that matter most

In rough order of protection gained per pound and hour spent.

- Multi-factor authentication on email, banking and remote access — the single highest-value control there is
- A password manager, so passwords are unique and nobody reuses one across accounts
- Patching operating systems and applications promptly, automatically where possible
- Managed antivirus that is licensed and monitored, not installed and forgotten
- Off-site, encrypted backup with version history, tested by actually restoring something
- Least privilege: staff work from standard accounts, not administrator accounts

Email fraud deserves its own paragraph

Invoice redirection fraud costs UK small businesses far more than ransomware does. It works by compromising a mailbox — yours or a supplier's — watching for a genuine invoice, and sending a near-identical follow-up with different bank details.

The defence is procedural, not technical: verify any change of bank details by phoning a number you already had on file, never one from the email. Make that a rule for everyone who pays invoices, and enforce it even when the request appears to come from a director.

Staff awareness, without the annual video

Long compliance training is largely forgotten. What works better is a short, specific set of rules everyone actually knows: verify bank detail changes by phone, never approve an MFA prompt you didn't trigger, report suspicious emails without fear of looking silly, and never install software because a web page said to.

Make reporting blameless. Most breaches are made worse by the hour or two someone spends hoping they got away with it.

Assume something will get through

Prevention is never complete, so judge your setup by how bad the worst day would be. Could you restore every machine? How long would it take? Would you know which data had been accessed?

That is why backup, monitoring and logging matter as much as antivirus. They are what turn a catastrophe into an expensive inconvenience.

Where ARK Care fits

ARK Care Pro covers the technical half of the list above on every device: EDR, DNS filtering, patching, monitoring and 500GB of monitored UK backup, with a monthly report so you can see it's actually working. The procedural half — MFA, password hygiene, invoice verification — is yours, and we'll happily help you set it up.

Ransomware: how it gets in and how to survive it

Ransomware encrypts your files and demands payment for the key. For a household it can mean every photo you own; for a business it can mean everything stopping for a fortnight.

It is also one of the most survivable problems there is — if one thing was in place beforehand.

How it actually gets in

Not through clever code, in the main. Through ordinary openings.

- A macro-enabled document or an attachment opened in a hurry
- Stolen credentials used on remote access that was left exposed to the internet
- An unpatched computer, server or firewall with a known flaw
- Software downloaded from a search result rather than the maker's site
- A supplier or contractor whose own network was compromised first

The first hour matters most

If files are being renamed in front of you, or a ransom note has appeared, do this straight away.

- Disconnect that machine from the network — unplug the cable, switch off Wi-Fi. Don't switch it off at the wall yet
- Disconnect any USB drive or external disk still attached, if it's safe to do so
- Check whether anyone else's machine or the shared drive is affected, and isolate those too
- Don't delete anything, don't reinstall Windows and don't run a cleanup tool — you'd destroy evidence and sometimes the only chance of recovery
- Photograph the ransom note with your phone; the strain matters for whether a free decrypter exists

Should you ever pay?

The official advice, and ours, is no. Paying funds the next attack, marks you as someone who pays, and there's no guarantee of a working key — a meaningful share of victims who pay never recover everything.

Before assuming there's no alternative, it's worth checking nomoreransom.org, a free project run with Europol that holds working decrypters for many older strains. And check your backups properly; people give up on them more often than backups actually fail.

The backup that actually survives it

Modern ransomware deliberately looks for backups and encrypts those too. A USB drive left plugged in gets taken with everything else.

- Keep at least one copy off the machine and off the network
- Use a backup with version history, so you can go back to before the encryption started
- Make sure the backup account can't be deleted by whoever holds the computer's admin password
- Test a restore occasionally — an untested backup is a hope, not a plan

For a business, plan the day itself

Decide now who you ring, who talks to staff and customers, and how you'd keep trading on paper for a couple of days. Know where the backups are and roughly how long a full restore takes.

You must also report a personal data breach to the ICO within 72 hours, so having the reporting route written down saves a scramble on a very bad morning.

Where monitoring helps

The gap between infection and encryption is often hours or days, spent quietly spreading. Monitored protection is what closes that window: the behaviour is detected, the device is isolated and someone is alerted while it's still one machine rather than all of them. ARK Care Pro pairs that monitoring with off-site backup that keeps its own version history.

Need a hand?

Is this a scam? Call us free

Ring **01329 623 555** and one of our technicians will tell you whether a message, email or call is genuine. There's no charge.

IT support without the IT department

ARK Care plans give a one-person business managed antivirus, backup, updates checked and a team to call when something goes wrong. We support you remotely anywhere in the UK. If a machine needs the workshop, post it in and we'll courier it back. No long-term commitment.

See the plans at **arkcare.uk/products**.

Repairs from anywhere in the UK

If your computer needs our workshop, you can post it to us. We can help you book a courier, and we return it to you by courier. Postage is paid by the customer.

Useful UK numbers: call 159 to reach your bank safely · forward scam texts to 7726 · email scams to report@phishing.gov.uk · Action Fraud 0300 123 2040.