ARK Care

From the ARK Computer Repair workshop

Stay Safe Online guide 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

Scam alerts, simple guides you can print and short videos, all from the technicians at our workshop. No jargon and nothing to pay.

1. Scams to watch out for
2. How to spot a scam email or text
3. Phone calls claiming to be from Microsoft or BT
4. Calls from "your bank" asking you to move money
5. "Hi Mum, this is my new number" messages
6. A pop-up says your computer is infected
7. Banking and shopping online safely
8. Passwords: the simple system that actually works
9. Two-factor authentication, explained properly
10. What to do if your email account is hacked
11. Staying safe on public Wi-Fi
12. Helping an older parent stay safe online
13. What to do if you think you've been scammed
14. Need a hand?

Scams to watch out for

Fake HMRC tax refund texts and emails

What it looks like: A message saying you're owed a tax refund, or that you owe tax, with a link to 'claim' or 'pay'.

What to do: Don't click the link. HMRC doesn't text or email about refunds with links. Forward scam texts to 7726 and scam emails to report@phishing.gov.uk.

Missed parcel delivery messages

What it looks like: A text saying a parcel couldn't be delivered and asking for a small 'redelivery fee' through a link.

What to do: Don't pay or enter card details. If you're expecting a parcel, check it on the retailer's own website or app instead.

'Microsoft' or 'BT' calling about your computer

What it looks like: A caller says your computer has a virus or your internet will be cut off, and asks you to install a program so they can 'fix' it.

What to do: Hang up. Never let a cold caller onto your computer. If you've already let them in, switch the computer off and call us.

How to spot a scam email or text

Phishing is how most people get caught out. Not a dramatic hack — an ordinary-looking email about a parcel, a bank transfer or a subscription renewal, arriving on a busy day.

Scam messages have got much better. The old clues — bad spelling, odd fonts — still catch some, but plenty of modern attempts are word-perfect. Here's what actually gives them away.

The reliable warning signs

Almost every scam message needs you to do something quickly and without checking. That need shows.

- It creates urgency: your account will be closed, a payment failed, a delivery will be returned today
- The sender's address doesn't match the company — check the part after the @, not the display name
- A link that doesn't go where it says (hover over it on a computer, press and hold on a phone to preview)
- It asks you to confirm a password, PIN, card number or one-time code — no genuine organisation does this
- An attachment you weren't expecting, especially a .zip, .html or a document that asks you to enable content
- A payment or bank detail change arriving by email alone

The convincing ones people fall for

The scams that work don't look like scams. These are the ones we see catching sensible people.

- A reply inside a real email conversation, sent from a supplier's genuinely hacked mailbox
- A renewal invoice for antivirus or a subscription you really do have, with a phone number to call to cancel
- A text from "your bank" that lands in the same message thread as their real texts — scammers can fake the sender name

- A shared document notification from a colleague's compromised account
- A text about an unpaid road toll, parcel fee or DVLA refund — small amounts, so people just pay

How to check safely

The rule is simple: never use the contact route the message gave you.

- Open a browser and type the company's address yourself, or use their official app
- Phone the number on your card, your paper statement or the company's real website
- If it's from a person, ring them on the number you already had — not one in the email
- For a delivery, check with the retailer you actually ordered from

If you've already clicked

Clicking a link is not usually a disaster on its own. Entering details is the moment that matters — and speed helps a great deal.

- Entered a password? Change it immediately on that account, and anywhere else you used the same one
- Entered card or banking details? Ring your bank now — most have a 24-hour fraud line
- Approved a code or app prompt you didn't trigger? Change the password and remove any unknown devices from the account
- Downloaded or ran something? Disconnect from the internet and get the machine checked before using it again
- Report it: forward scam emails to report@phishing.gov.uk and text scams to 7726, free on every UK network

Making yourself a harder target

Two things blunt phishing almost completely. Two-factor authentication means a stolen password isn't enough on its own. A password manager only offers to fill your details on the genuine website, so a convincing fake simply stays blank — which is a quiet, reliable warning you'll notice before you type.

Monitored antivirus adds the last layer, blocking known scam sites and malicious downloads before the page even loads.

Phone calls claiming to be from Microsoft or BT

"We've detected a problem with your computer." It remains one of the most effective scams in the UK, and the people who ring are professional, patient and well rehearsed.

No genuine company — not Microsoft, not BT, not your bank, not us — will ever phone you out of the blue about a fault on your computer.

How the call plays out

The script is consistent, because it works.

- They name a real company and claim your machine is infected or your broadband is being misused
- They walk you to a Windows screen full of ordinary warnings and present it as proof
- They ask you to install a remote support tool so they can "fix" it
- A refund or fee follows — and the bank screen you're shown is fake
- Some finish by locking the machine so you'll ring back

What they're actually after

Rarely the computer itself. The real targets are online banking, saved passwords and a payment — sometimes months later, when a second caller rings "to process the refund you were owed".

Anyone who has paid once is added to a list and called again. That repeat contact is why it matters to report the first call, even if you lost nothing.

What to do during the call

There's no need to be polite about it. Hang up. You cannot lose anything by ending a genuine call, and you can lose a great deal by staying on a fake one.

- Don't confirm your name, address, bank or any account details
- Don't install anything, however harmless the name sounds

- Don't let them read you a code or ask you to read one to them
- If you want to check, hang up, wait five minutes, then ring the company on a number you already had

If you let someone onto your computer

Act quickly and in this order.

- Disconnect from the internet — unplug the cable or switch Wi-Fi off
- Ring your bank from a different phone if any banking screen was open
- Change your email and banking passwords from another device, not that computer
- Have the machine properly checked before using it again — remote tools and hidden accounts are often left behind
- Report it to Action Fraud on 0300 123 2040, and to your bank if money moved

Protecting an older relative

The most useful thing you can give someone is permission to hang up. Agree in advance that nobody will ever be cross with them for ending a call, and that they can always ring you first.

Practically: register with the Telephone Preference Service, switch on call blocking if the phone or provider offers it, and make sure they know that a real company never asks for remote access. On a monitored machine we can also see if an unexpected remote tool has been installed, which is often the first proof that a call went further than they remember.

Calls from "your bank" asking you to move money

The phone rings and someone from your bank's fraud team says there's suspicious activity on your account. They sound calm, they know your name, and the number on your screen may even match your bank's.

It is a scam. Your bank will never ask you to move money to another account to keep it safe, and it will never ask you to read out a code sent to your phone.

How it usually goes

The details change, but the pattern is very consistent.

- A call, text or message says your account has been used fraudulently
- The caller already knows some details about you, which makes them seem genuine
- They say a member of staff is involved, so you mustn't tell anyone at the branch
- They ask you to move money to a "safe account", or read out a one-time code
- Some callers claim to be the police and ask you to help with an investigation

Why the number on your phone can't be trusted

Criminals can make a call display any number they like, including your bank's real one. This is called number spoofing. A familiar number proves nothing.

The same goes for text messages, which can appear in the same thread as genuine messages from your bank.

The rule that stops it

If anyone contacts you about your bank account, end the call and ring 159. It connects you safely to most major UK banks. Or call the number on the back of your card — from a different phone if you can, because some criminals keep the line open after you hang up.

- Never move money because someone has asked you to on a call you didn't make
- Never read out a code sent to your phone, whoever asks
- Never let a caller onto your computer to "check" your banking
- Being told to keep it secret is a warning sign on its own

If you've already moved money

Speed matters. Banks can sometimes stop or recover a payment if they hear quickly.

- Ring your bank straight away on 159 or the number on your card
- Report it to Action Fraud on 0300 123 2040
- If the caller was on your computer, switch it off and have it checked before you bank on it again

"Hi Mum, this is my new number" messages

It starts with a friendly message: "Hi Mum, I've broken my phone, this is my new number." A little later comes a request to pay a bill urgently because their banking app isn't working on the new phone.

It works because it relies on kindness, not on any lack of knowledge. Plenty of sharp, careful people have been caught by it.

Signs it's a scam

- A message from an unknown number saying they've lost or broken their phone
- They don't use your name, or the name they use for you is slightly off
- They can't talk on the phone right now — only message
- A request to pay someone else's account, often "a friend" or "the landlord"
- Pressure to do it quickly, before the end of the day

How to check in under a minute

Ring your child on the number you already have. If their phone really is broken, call them through someone they live or work with, or ask the new number for a voice note or quick video call. A scammer will make an excuse.

Some families agree a simple code word in advance. If the message can't give it, it isn't them.

If you've already paid

- Call your bank straight away on 159 or the number on your card
- Report it to Action Fraud on 0300 123 2040
- Report the number in WhatsApp and block it

A pop-up says your computer is infected

The screen suddenly goes full-size, an alarm sounds, and a message says your computer is infected and you must ring a number immediately. It is designed to frighten you.

In almost every case, nothing is wrong with the computer. It's a web page pretending to be a warning. The danger only starts if you ring the number.

How to tell it's fake

- It appears while you're browsing a website, not from your antivirus program
- It gives a phone number to call — real security software never does
- It uses sound, flashing or a countdown to rush you
- It claims to be from Microsoft, Apple or Windows Defender

How to close it

Don't click anything inside the warning, including buttons that say "close" or "cancel".

- Press and hold the Esc key — this often exits full screen
- On Windows, press Ctrl, Shift and Esc together to open Task Manager, then end the web browser
- On a Mac, press Cmd, Option and Esc together and choose Force Quit for the browser
- If all else fails, hold the power button until the computer switches off
- When you reopen the browser, don't restore the previous pages

If you rang the number

The person who answers will try to get onto your computer and then ask for payment. If that's already happened, follow the steps in our guide to fake tech support calls: disconnect from the internet, ring your bank if any card details were given, and have the computer checked.

Banking and shopping online safely

Online banking and shopping are safe for most people most of the time. The problems usually come from a fake link, a fake shop or a reused password, rather than from the bank itself.

A handful of habits removes most of the risk.

Getting to your bank safely

- Use your bank's official app, or type the address yourself and save it as a bookmark
- Never log in through a link in an email or text, however genuine it looks
- Use a password for your bank that you don't use anywhere else
- Switch on the extra security your bank offers, such as app approval or text codes
- Keep your phone and computer up to date

Spotting a fake shop

Fake shops often appear in social media adverts with prices that seem too good to be true.

- Prices far lower than every other shop
- No proper UK address or phone number
- A web address that doesn't quite match the brand name
- Asked to pay by bank transfer rather than by card
- Reviews that are all very recent, or all suspiciously glowing

Pay in the safest way

Paying by credit card for purchases over £100 gives extra legal protection under Section 75 of the Consumer Credit Act. Debit cards and PayPal also offer ways to dispute a payment. A bank transfer to a stranger is the hardest payment to get back.

On a shared or public computer

Avoid banking on a library or hotel computer. If you must, always log out fully and never let the browser save your password.

Passwords: the simple system that actually works

Most accounts aren't broken into by guessing. They're opened with a password that was already stolen from somewhere else entirely — a shop, a forum, an old service that leaked years ago.

So the advice that matters isn't "make it complicated". It's "never use the same one twice".

Why reuse is the whole problem

When a company is breached, the stolen email-and-password pairs are sold in bulk. Automated tools then try those pairs on hundreds of other sites — email, shopping, banking. If you reused the password, they're in, and no amount of capital letters or exclamation marks helps.

You can check whether your own address has appeared in a known breach at haveibeenpwned.com. Most people are on at least one list, which is normal — it only matters if the password is still in use somewhere.

What a good password looks like now

The old rules produced passwords that were hard for people to remember and easy for computers to guess. Length beats complexity.

- Three or four unrelated words strung together, for example purple-harbour-kettle-92
- At least 14 characters where the site allows it
- Nothing drawn from your life: no names, pets, birthdays, street or football team
- No pattern you repeat across sites, like the site name plus your usual password
- Change a password when there's a reason to — not on a routine every 90 days

The three passwords worth memorising

You only need to hold a few in your head. Make these three long, unique and unwritten:

- Your email password — it's the master key, because every other account resets through it
- Your password manager's master password
- Your computer or phone unlock code

How a password manager actually works

It's an encrypted vault. You remember one strong password; it remembers everything else, generates new ones and fills them in for you. Bitwarden and 1Password are both sound choices, and the ones built into Apple, Google and Microsoft accounts are fine too if you live inside one of those.

The common worry — "isn't it dangerous to keep them all in one place?" — is understandable but backwards. The realistic risk isn't the vault being cracked; it's you reusing one password across 40 sites because remembering 40 is impossible.

If you'd rather use paper

A notebook is far better than reusing one password everywhere. Burglars are not after your passwords; automated credential stuffing is. Keep the book somewhere sensible, don't write the website next to each one in obvious terms, and never keep it in a file called passwords on the computer itself.

Two-factor authentication, explained properly

Two-factor authentication — 2FA, MFA, two-step verification — all mean the same thing: proving who you are with something more than a password.

It is the single most effective thing you can do for your online safety, and on the accounts that matter it takes about two minutes to switch on.

Why it works

A stolen password becomes useless on its own. The attacker has half of what they need, and the other half is sitting in your pocket. That's why almost every serious attack now tries to get around 2FA rather than through it.

The types, best first

They are not all equal, though any of them beats nothing.

- Security key or passkey — a physical key or your phone's fingerprint/face unlock. Phishing-proof, because it will only work on the real website
- Authenticator app — a six-digit code that changes every 30 seconds. Free, and works without signal
- Push approval — a "was this you?" prompt. Convenient, but never approve one you didn't trigger
- Text message code — the weakest, because numbers can be hijacked, but still far better than a password alone

Where to turn it on first

Start with the accounts that unlock everything else, then work outwards.

- Email — first, always; it's how every other account is reset
- Online banking and payment accounts

- Your Microsoft or Apple account
- Anywhere a card is stored: Amazon, PayPal, the supermarket
- Social media, so nobody can impersonate you to your friends
- For a business: remote access, accounting software and the payroll system

Set up recovery before you need it

This is the step people skip, and it's the one that causes the lockouts.

- Save the backup or recovery codes each service gives you — print them or store them in your password manager
- Add a second method, such as a partner's phone number or a second authenticator
- If you use an authenticator app, pick one that backs up to your account, so a new phone restores everything
- Don't store the codes only on the same phone that holds the app

Never approve a prompt you didn't ask for

If a code arrives or your phone asks you to approve a sign-in and you weren't signing in, somebody has your password. Don't approve it, and don't read the code to anyone who rings about it — that phone call is part of the attack.

Change that password straight away, then check the account's list of signed-in devices and remove anything you don't recognise.

What to do if your email account is hacked

Your email is the master key to your digital life. Everything else — banking, shopping, social media — resets through it, which is why it's the account attackers want most.

If you think yours has been taken over, order matters. Do these in sequence.

Signs it's actually been compromised

Not every oddity means a break-in, but these do.

- Contacts receiving messages you didn't send, especially odd links or invoices
- Sign-in alerts from places you've never been
- Password reset emails you didn't request, for other services
- Messages disappearing from your inbox, or replies to conversations you've never seen
- Your password suddenly not working

Step one: get control back

Use a device you trust. If your own computer might be infected, use a phone or another machine.

- Change the password to something long and unique you've never used elsewhere
- Turn on two-factor authentication immediately, before anything else
- In the account's security settings, sign out all other devices and sessions
- Check and correct the recovery phone number and recovery email address

Step two: the hidden rules nearly everyone misses

Attackers routinely leave a quiet way back in, and changing the password doesn't remove it. Check all of these in your mail settings:

- Forwarding — is a copy of everything being sent to an address you don't recognise?
- Rules or filters — anything that deletes, archives or moves messages containing words like invoice, bank or password
- App passwords and connected apps — remove anything unfamiliar
- Aliases or send-as addresses that you didn't add
- The auto-reply, which is sometimes altered to redirect people

Step three: contain the damage

Assume anything sitting in the mailbox has been read.

- Change the password on any account that uses this email address, starting with banking and anywhere a card is saved
- Tell your contacts — briefly and without embarrassment — so they ignore anything odd they received
- Check your sent items and deleted items to see what was actually sent
- If you run a business and invoices go through this mailbox, warn customers to verify bank details by phone before paying
- If financial data was exposed, contact your bank and report it to Action Fraud

Stopping the repeat

Almost every compromised mailbox we see comes down to one of two things: a password reused from a site that was breached, or a convincing phishing page that harvested the login.

A unique password plus two-factor authentication removes both. If the break-in also involved software on the computer, get the machine checked — a password change means nothing if something on the device is still capturing what you type.

Staying safe on public Wi-Fi

Public Wi-Fi used to be genuinely dangerous: anyone on the network could read what you were doing. Almost every website is encrypted now, so the old horror stories are largely out of date.

Some real risks remain, though, and they're not the ones people worry about.

What's still worth worrying about

The threats that survive are about who you're connecting to, not what passes over the air.

- Fake hotspots named to look official — "Hotel Guest WiFi Free" sitting next to the real one
- Sign-in pages that ask for far more than they need, or ask you to install something
- Certificate or security warnings in the browser, which you should never click past on a public network
- File sharing left switched on, exposing folders to everyone else on the network
- Someone simply reading your screen over your shoulder

Simple habits that cover most of it

None of this requires extra software.

- Ask staff for the exact network name rather than guessing from the list
- Turn off automatic joining of open networks, so your phone doesn't reconnect to a fake one later
- Set the network as Public on Windows, which switches off sharing
- Use your phone's own mobile hotspot for anything sensitive — it's usually faster anyway
- Keep the device patched, and keep antivirus running

Does a VPN help?

It genuinely does two things: it stops the network operator and anyone else on it seeing which sites you visit, and it protects you on badly configured or hostile networks. On a hotel, airport or conference network that's worth having.

What it doesn't do is make you anonymous or protect you from phishing, malware or a weak password. Treat it as one sensible layer rather than a shield. If you use one, pay for a reputable service — free VPNs make their money by selling the very browsing data you installed them to protect.

For people working away from the office

If work data travels with you, a VPN stops being optional. So does full-disk encryption (BitLocker on Windows, FileVault on a Mac), because the realistic loss is a laptop left on a train rather than anything clever happening over Wi-Fi.

Make sure remote access to the office goes through a VPN or a properly secured gateway with two-factor authentication — exposed remote desktop is still one of the most common ways businesses are breached.

Helping an older parent stay safe online

Many of the people we help at the workshop are in their seventies and eighties and use their computers every day. Scammers target this group not because they're less able, but because they're more likely to be polite, trusting and at home to answer the phone.

The aim isn't to take the computer away or to lecture. It's to set things up sensibly and make it easy to ask for help.

Start with one conversation

The most valuable thing you can say is: "You'll never be in trouble with me for asking, and you can always hang up on anyone." Embarrassment stops people reporting scams, and that gives criminals a second chance.

Agree a simple rule together: before paying anyone, or letting anyone onto the computer, they ring you or someone they trust first.

Practical things to set up

- Automatic updates switched on for the computer, tablet and phone
- Reliable antivirus that someone is keeping an eye on
- A password manager, or a written password book kept safely at home
- Two-factor authentication on email and banking
- Registration with the Telephone Preference Service to cut cold calls
- Call blocking on the landline, if the provider offers it
- A backup of photos and documents, so a scam or failure doesn't mean losing them

The four phrases worth remembering

Almost every scam uses at least one of these. If they hear one, it's time to stop and check.

- "Act now" — urgency is the scammer's main tool

- "Don't tell anyone" — no real organisation asks for secrecy
- "Let me onto your computer" — never for a cold caller
- "Move your money" — banks never ask this

If something has already happened

Stay calm and reassuring. Ring the bank on 159, report it to Action Fraud on 0300 123 2040, change the email password from another device, and have the computer checked if anyone had access to it.

What to do if you think you've been scammed

Realising you've been scammed is horrible, and it happens to clever, careful people every day. The most important thing now is to act quickly, not to blame yourself.

Work through these steps in order. You don't need to do them all at once — the first two matter most.

1. If money or card details are involved

Ring your bank immediately on 159 or the number on the back of your card. Tell them exactly what happened. The sooner they know, the better the chance of stopping a payment.

2. If someone was on your computer

Disconnect it from the internet — unplug the cable or switch Wi-Fi off — and don't use it for banking until it has been checked. Scammers often leave remote access tools behind.

3. Change your passwords

Use a different device that you know is safe.

- Email first, because it can be used to reset everything else
- Then online banking and any shopping accounts
- Then any account where you used the same password

4. Report it

- Action Fraud: 0300 123 2040
- Scam texts: forward to 7726
- Scam emails: forward to report@phishing.gov.uk

5. Watch out for the follow-up

People who have been scammed are often contacted again by someone offering to "recover" the money for a fee. That is a second scam. Genuine help from your bank or the police never costs money.

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.

Want us to keep an eye on it for you?

ARK Care plans look after your computer in the background: antivirus we manage for you, updates checked, and a friendly team to ring when something looks wrong. It works wherever you live, and if your computer ever needs the workshop you can post it to us. No long-term commitment, and you can cancel any time.

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.