

Vision Tech

Scams & online safety Handbook

26 free step-by-step guides in plain English

Free to print and share.

guides.visiontech336.com - admin@visiontech336.com

Contents

Caught out? What to do next

I think my account has been hacked	3
A pop-up says my computer has a virus	4
What to do if you clicked a bad link	5
What to do if you gave away your card details	7
What to do if you gave away a password	9
Recovering a hacked social media account	11

Spotting scams

How to spot a scam email, text or call	13
Fake delivery texts: Royal Mail, DPD and Evri	14
The fake bank call and the 'safe account' scam	15
HMRC, TV licence, Amazon and PayPal scams	16
Romance and investment scams	17
Remote access scams and tech-support cold calls	19
Fake QR code scams	21
WhatsApp scams: 'Hi Mum' and account takeover	22
Buying and selling safely on Facebook Marketplace, Vinted and eBay	23

Passwords & account protection

How to create a strong password	24
How to turn on two-step sign-in	25
Has your email been in a data breach? Using Have I Been Pwned	26
Securing your Facebook and Instagram accounts	28

Safe browsing & protection

Staying safe online	30
How to check whether a website is real	31
Do you need antivirus beyond Windows Security?	33
Ransomware basics and why backups matter	35
Staying safe on public Wi-Fi	37
Shopping online safely	39
Keeping an older relative safe online: how to start the conversation	41

Scams & online safety | Medium | 2 min read

I think my account has been hacked

If you think an account has been hacked, act quickly but calmly. Signs include login alerts you did not expect, password reset emails you did not ask for, strange messages sent from your account, or being unable to sign in.

First steps

- Use a device you trust, ideally one that is not behaving oddly.
- Go to the official website or app, typed in yourself, not via a link in a message.
- If you cannot sign in, use the **Forgot password** option on the real site.

Step by step

1. Change your password to a new, strong, unique one. Do not reuse an old one.
2. Look for an option to **Sign out of all devices** in the account's security settings, and use it.
3. Turn on two-step sign-in so a stolen password is not enough.
4. Check your recovery email address and phone number are yours.
5. For email accounts, check settings for rules or forwarding you did not set up. Hackers sometimes forward your mail to themselves.
6. If you used the same password elsewhere, change it on those sites too, starting with your email and banking.
7. Tell friends and family not to open odd messages sent from your account.

If money or banking is involved

Phone your bank at once using the number on your card. Ask them to check recent activity.

Report it

- Report to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.
- Forward scam emails to report@phishing.gov.uk, and scam texts to 7726.

When to get more help

Stop and ask for help if you cannot get back into the account, the hacker has changed your recovery details, your computer may also be infected, or money has gone. Please do not pay anyone offering to recover your account. Tell us which account, what you noticed and when.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

A pop-up says my computer has a virus

A pop-up saying your computer has a virus, often with loud noises and a phone number, is almost always a scam. Real security warnings do not ask you to phone a number. It cannot be a real warning if it is on a website.

What not to do

- Do not call the number or click anything in the pop-up.
- Do not download or install anything it offers.
- Do not pay, or give out card details or passwords.
- Do not let anyone take remote control of your computer.

Step by step

1. If you can, close the page. Press Alt and F4 together on Windows, or Command and Q on a Mac, to close the browser.
2. If it will not close, press Ctrl, Shift and Esc to open **Task Manager** (Windows), select your browser and choose **End task**. On a Mac, press Option, Command and Esc, select the browser and choose **Force Quit**.
3. Open the browser again. If it offers to restore your previous pages, choose not to.
4. Run a scan with the security software already on your computer. On Windows, open **Settings**, then **Privacy & security**, then **Windows Security** (in Windows 10, **Update & Security**, then **Windows Security**), and choose **Virus & threat protection**.
5. Restart the computer. Do not switch off your security software.

If you already called or paid

- Stop all contact. Hang up if on the phone.
- If they have access to your computer, switch off Wi-Fi or unplug the network cable.
- Phone your bank at once using the number on your card if you gave card details or paid.
- Change passwords from a different, clean device.
- Report to Report Fraud at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.

When to get more help

Stop and ask for help if the pop-ups keep coming back, your browser has strange extensions, or anyone has had access to your computer. Tell us exactly what the pop-up said and what you did.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

What to do if you clicked a bad link

It happens to nearly everyone at some point. Clicking a bad link does not always cause harm, and there are clear steps to take that keep you safe.

First, stay calm

Often the link just opens a page that tries to trick you. Harm usually happens only if you then type in details or download something. So think about what happened after the click.

If you only clicked and nothing else happened

1. **Close the page or tab.**
2. Do not type anything into it.
3. Do not allow notifications if the page asks.
4. Run a scan with Windows Security (or your own antivirus) as a precaution.

If you typed in a password

1. Go to the real website, not through the link, and **change the password** straight away.
2. If you use the same password anywhere else, change those too.
3. Turn on two-step sign-in if you have not already.

If you typed in card or bank details

Ring your bank on **159** or the number on your card and tell them. They can block the card and watch for odd payments.

If something downloaded or installed

1. Do not open it.
2. Disconnect from the internet if the computer behaves strangely.
3. Run a full scan with Windows Security.
4. If you are worried, ask us for a check.

Tell people

Forward scam emails to **report@phishing.gov.uk** and scam texts to **7726**. If money was lost, report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or to Police Scotland on 101.

Next time

If a message makes you feel rushed or worried, stop and take five minutes. Go to the official website or app yourself instead of using the link.

When to get more help

Contact us if your computer is slow, shows pop-ups after the click, or you would like a calm second pair of eyes.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

What to do if you gave away your card details

If you have typed your card number into a fake site or read it out to a scammer, you can act quickly to limit the harm. Banks deal with this every day and will not judge you.

Step by step

1. **Ring your bank straight away.** Use **159**, which connects you to many UK banks, or the number on the back of your card. If you gave details of more than one card, ring each provider.
2. Tell them exactly what you shared: the number, expiry date, the three digits on the back, your PIN, or any codes.
3. Ask them to **cancel and replace the card** and to check recent payments.
4. Ask whether any payments can be reversed.
5. Write down the time, the name of the person you spoke to and what you were told.

Check your accounts

Look at your recent transactions on your banking app or statements. Tell the bank about anything you do not recognise. Keep checking for a few weeks.

Watch for follow-up

Scammers sometimes call again, pretending to be the bank "helping" you. Hang up and call your bank back on 159 or the number on your card.

If you also shared a password

Change it on the real website and anywhere else you used it.

Your rights

In many cases, if someone steals your card details and you have not been careless or dishonest, the bank will refund the money. Do not be embarrassed. Tell them quickly.

Report it

Report to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101. Forward scam texts to 7726 and scam emails to report@phishing.gov.uk.

Tips for the future

- Use a credit card for online shopping when possible, as it offers extra protection.
- Turn on payment alerts in your banking app.
- Never read out your PIN or full card details to anyone who rings you.

When to get more help

If you feel anxious or are not sure what to say to your bank, ask us or a trusted friend to sit with you while you ring.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

What to do if you gave away a password

If you have shared a password with a scammer or typed it into a fake page, the fix is simple: change it quickly. Here is what to do, in a sensible order.

Step by step

1. **Go to the real website or app** by typing the address yourself, not by using the link you were sent.
2. Sign in and change the password to a new one. Choose three random words joined together, such as "TeaCupBicycle", then add a number or symbol if the site asks.
3. **Turn on two-step sign-in** on that account. This means a stolen password alone is no longer enough.
4. Look at recent activity or sign-in history for anything you do not recognise.
5. Sign out of all other devices if the site offers this.

Change it elsewhere too

If you used the same password on other accounts, change those as well. Start with the important ones:

- Your main email account, because it can be used to reset other passwords.
- Online banking and shopping accounts.
- Social media.

If you cannot sign in

Scammers may have already changed the password. Use the site's **Forgotten password** option. If that does not work, use the site's help page to recover the account. Our guide on a hacked account may help.

If it was your email password

Check your email settings for forwarding rules or other addresses you did not add. These are sometimes set up by a scammer to watch your mail.

Tell the right people

If it was a bank password, ring your bank on **159** or the number on your card. Forward scam emails to report@phishing.gov.uk. If money or accounts were affected, report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or to Police Scotland on 101.

Make it easier next time

A password manager can remember a different strong password for each site, so you only need to remember one. We can help you set one up.

When to get more help

If you are locked out or unsure what to change first, get in touch and we will go through it with you step by step.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Recovering a hacked social media account

Finding your Facebook, Instagram or other social media account has been taken over is upsetting. There is a clear way back in most cases, so take it one step at a time.

Signs your account may be hacked

- Your password no longer works.
- Friends say they have had odd messages from you.
- You see posts or sign-in alerts you did not make.
- Your email or phone number on the account has changed.

Step by step

1. **Check your email** for messages from the platform about changes. These may include a link that says "**This wasn't me**" or "**Secure your account**". Use it if it is genuine, ideally by going to the real site yourself.
2. On the sign-in page, choose **Forgotten password**, and follow the steps.
3. Look for the official recovery pages. On Facebook, go to facebook.com/hacked. On Instagram, use **Get help signing in** on the login screen.
4. You may be asked to confirm your identity, perhaps by a video selfie. This is normal on genuine sites.
5. Once back in, **change your password** and turn on **two-step sign-in**.
6. Check your account settings for changed email addresses, phone numbers or connected apps, and remove anything unfamiliar.
7. Log out of all other devices.

Tell your friends

Post from another account or message friends to say your account was hacked and that they should ignore any requests for money.

Change other passwords

If you used the same password elsewhere, change those too, beginning with your email.

Beware of recovery scams

Be wary of anyone who offers to "get your account back" for a fee. Scammers target people in this situation. Only use the platform's official help pages.

Report it

If someone asked your friends for money, or you lost money, ring your bank on 159 or the number on your card. Report to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

If the official routes do not work or you are not sure what to click, contact us and we will go through it with you.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

How to spot a scam email, text or call

Scammers pretend to be banks, delivery firms, the tax office or people you know. Their messages are designed to rush you. The best defence is to slow down and check through a route you trust.

Common warning signs

- The message is unexpected, or says you must act now, or something bad will happen.
- It asks for personal details, passwords, PINs, codes or payment.
- It comes from a strange address or number, or the wording and spelling are odd.
- It offers a prize, refund or too-good-to-be-true deal.
- A caller says they are from your bank, the police or tech support and asks you to move money or let them onto your computer.

What to do

1. Stop. Do not click links, open attachments, reply or call back on a number in the message.
2. Check independently. Contact the organisation through its official app, website typed in yourself, or the number on your card or bill.
3. Hang up if a call feels wrong. Wait a few minutes, then call back on a number you know to be real, ideally from a different phone.
4. Never share one-time codes or passwords with anyone. Real firms will not ask for them.
5. Never let a stranger take remote control of your computer.

Report it

- Forward scam texts to 7726 (free).
- Forward scam emails to report@phishing.gov.uk.
- Report fraud and cyber crime to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.

When to get more help

If you have already clicked, paid or shared details, do not panic. Phone your bank straight away using the number on your card, and ask for help changing passwords. Stop and ask for help if you gave someone access to your computer or are being pressured right now. Tell us what happened and keep the message.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Fake delivery texts: Royal Mail, DPD and Evri

Many people get a text saying a parcel is waiting and a small fee is due. These messages are very common, and they are easy to deal with once you know the signs.

What the message usually looks like

- It says a delivery has failed or is being held.
- It asks you to tap a link to rearrange delivery or pay a small fee, often under £3.
- It uses real company names such as Royal Mail, DPD or Evri.
- It may say you must act today.

Why it is a trick

Real delivery firms do not ask for card details through a text link. The link leads to a copy of a real website, built to collect your card number and the security code on the back. The small fee is just a way of getting you to type those details in.

What to do

1. **Do not tap the link**, and do not reply, even to say stop.
2. Think: are you actually expecting a parcel? If so, go to the company's own app or type their website address in yourself.
3. Forward the text to **7726**. This is free and helps your phone network block the sender.
4. Delete the message.

If you are unsure, you can also check the tracking number in the email from the shop where you ordered.

If you already tapped or paid

Do not panic. Tapping a link alone usually does no harm if you close the page straight away. If you typed in card details, ring your bank on the number on the back of your card, or dial **159**, and tell them. They can stop the card and check for payments. Our guide on giving away card details has more.

You can report the scam to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.

When to get more help

Ask us if you are not sure whether a message is real, if you tapped a link and your phone is behaving oddly, or if you would like help setting up your phone to filter junk texts. There is no such thing as a silly question here.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

The fake bank call and the 'safe account' scam

Someone rings, says they are from your bank or the police, and tells you your money is in danger. They ask you to move it to a "safe account". This is a well-known scam, and knowing how it works is your best protection.

The key fact

Your bank will never ask you to move your money to a new or safe account. Neither will the police. Anyone who asks this is a fraudster.

How the call usually goes

- The caller sounds professional and may know your name or the last few digits of your card.
- They say there has been suspicious activity, or that a bank member of staff is under investigation.
- They create urgency and ask you to keep the call secret.
- They may say "hang up and call back", then keep the line open so you are still talking to them.

What to do

1. **Hang up.** You are never rude by ending a call.
2. Wait at least ten minutes, or use a different phone, because scammers can keep a landline connected.
3. Ring your bank on **159**, which connects you to many UK banks, or use the number on the back of your card. Do not use a number the caller gave you.
4. Tell the bank what happened.

Handy rules

- Never share your PIN, full password or one-time codes with anyone, ever.
- A caller number on your screen can be faked, so do not trust it.
- Take Five: stop, take a moment, and think before you act.

If you have already moved money

Ring your bank straight away on 159 or the number on your card. The sooner they know, the more they can often do. Then report it to Report Fraud (formerly Action Fraud) on 0300 123 2040, or Police Scotland on 101 if you live in Scotland. Being tricked is not your fault, as these criminals are skilled at what they do.

When to get more help

Talk to a family member or to us if a call has left you worried. We can help you set up call blocking and check your accounts.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

HMRC, TV licence, Amazon and PayPal scams

Scammers like to pretend to be big names that most of us deal with. The messages look different but follow the same pattern: something is wrong, and you must act quickly.

Common examples

- **HMRC:** a text or email says you are owed a tax refund, or a call says you face arrest over unpaid tax.
- **TV Licensing:** an email says your licence has expired or your payment failed, with a link to "update your details".
- **Amazon:** a call or message says there is a suspicious order or your Prime membership is about to renew, and asks you to press a number or click a link.
- **PayPal:** a message says your account is limited or someone has taken a payment.

Signs it is not genuine

- It creates panic, or promises free money.
- It asks for bank details, passwords or codes.
- It does not use your name, or the sender's address looks slightly odd.
- It pushes you to click a link or phone a number inside the message.

What to do

1. **Do not click, call back or reply.**
2. Go to the real website by typing the address yourself, or open the company's official app, and look at your account there.
3. Forward suspicious emails to **report@phishing.gov.uk** and suspicious texts to **7726**.
4. Delete the message.

Good to know

HMRC does not threaten arrest by phone or text, and does not ask for payment in gift cards. Amazon will not ask you to give control of your computer or buy vouchers. If an account really has a problem, it will show when you sign in the normal way.

If you shared details

If you gave out a password, change it at once on the real site. If you gave card details, ring your bank on 159 or the number on your card. You can report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

If you are unsure whether a message is real, pass it to us or someone you trust before doing anything.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Romance and investment scams

These scams are slow and patient. The criminal builds trust over weeks or months before asking for money, which is why they can catch out sensible, careful people. It is nothing to be ashamed of.

Romance scams

Someone you have met online, perhaps on a dating site or social media, becomes very close very quickly. They often say they work abroad, for example on an oil rig or in the military. Then something goes wrong, such as an illness, a travel problem or a customs fee, and they ask for help with money.

Warning signs:

- They refuse to video call, or always have an excuse.
- They want to move the chat to private messaging quickly.
- They ask for money, gift cards or bank details.
- Their story changes, or things feel too good to be true.

Investment scams

You may see an advert or message promising high returns, often with a famous face attached, or be added to a group where "members" share big profits. You are pushed to invest quickly, perhaps in crypto, and the website shows growing figures that are not real.

Warning signs:

- Guaranteed or very high returns with no risk.
- Pressure to act now.
- A company you cannot find on the Financial Conduct Authority register at register.fca.org.uk.

What to do

1. **Never send money to someone you have not met in person.**
2. Talk to a friend or family member about the situation.
3. Check any investment firm on the FCA register before you pay.
4. Stop contact and block them.

If you have lost money

Contact your bank on 159 or the number on your card straight away. Report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or 0300 123 2040, or Police Scotland on 101. Citizens Advice can also help you work out next steps.

When to get more help

If you feel worried or upset, please talk to someone. We can help you check profiles and block contacts, and your bank or Citizens Advice can help with money worries.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Remote access scams and tech-support cold calls

A caller says they are from Microsoft, your broadband provider or "tech support" and that your computer has a problem. They ask you to install a program so they can "fix" it. This is a scam, and it is one we see often.

The key rule

Never give a stranger control of your computer. Real companies do not ring people out of the blue to say your computer is faulty.

How it works

- The caller sounds friendly and technical.
- They may ask you to open a harmless-looking screen to "show" errors. These screens are normal and do not mean anything is wrong.
- They ask you to install a remote access tool such as AnyDesk or TeamViewer. Once you do, they can see and control everything.
- They then ask you to log in to online banking, "to receive a refund", and move money without you noticing.

What to do if someone rings

1. Say you are not interested and **hang up**. You do not have to be polite to a cold caller.
2. Do not follow any instructions, even small ones.
3. Do not install anything or type anything into the computer.

If you have already let them in

1. **Turn off Wi-Fi or unplug the network cable**, then shut down the computer.
2. Ring your bank on **159** or the number on your card, from a different phone if you can.
3. Do not use the computer for banking until it has been checked.
4. Change your passwords later, from a clean device.
5. Report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or 0300 123 2040, or Police Scotland on 101.

Staying safe

Remote access tools are useful when you ask a trusted person, like us, for help. The difference is that you start the contact, and you know who you are talking to.

When to get more help

If anything like this has happened, contact us. We will check the computer, remove anything unwanted and help you secure your accounts.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Fake QR code scams

QR codes are those square black and white patterns you scan with your phone camera. Most are perfectly safe, but criminals sometimes use them to send people to fake websites.

Where the risk is

- Stickers placed over the real QR code on a car park payment machine.
- Codes in unexpected emails, letters or text messages.
- Codes on posters or flyers in public places that promise prizes or discounts.
- Codes sent by a "bank" or "delivery company".

Why it works

You cannot read a QR code with your eyes, so you cannot tell where it leads until you scan it. A fake one can take you to a page that looks like a real payment page and collects your card details.

Staying safe

1. **Look at the web address that appears** after you scan, before you tap it. Does it match the company? Is it spelt correctly?
2. Check whether a sticker has been placed over the original code. If it looks peeled, bumpy or added on, do not use it.
3. In a car park, you can often pay with the official app downloaded from your phone's app store, or by phone or cash instead.
4. Do not scan codes from messages you were not expecting.
5. Never enter card details, passwords or codes after a QR scan unless you are sure of the website.

Tip for restaurants and events

A code on a restaurant table is usually fine. If it asks for a lot of personal details, just ask staff for a paper menu.

If you scanned a bad code

Close the page and do not type anything in. If you entered card details, ring your bank on 159 or the number on your card. If you entered a password, change it on the real website. You can report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

If you are not sure about a code, or you would like us to show you how to check a link on your phone, just ask.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

WhatsApp scams: 'Hi Mum' and account takeover

WhatsApp is a handy way to keep in touch, which is why scammers use it too. Two tricks are very common, and both are easy to defend against.

The 'Hi Mum' message

A message arrives from an unknown number saying "Hi Mum, I've lost my phone, this is my new number." After a little chat, they say they need money urgently, perhaps to pay a bill they cannot sort out on the new phone.

What to do:

1. **Do not send money.**
2. Ring your child, or the person they claim to be, on the number you already have saved.
3. Ask a question only they would know, or ask them to send a voice note.
4. Block and report the number in WhatsApp.

Account takeover

Here, a criminal tries to get into your WhatsApp. You receive a text with a six-digit code you did not request. Then a "friend" messages saying they sent the code to you by mistake and asks you to send it on. If you do, they take over your account and message your contacts asking for money.

Never share a WhatsApp code with anyone, even a friend.

Protect your account

1. Open WhatsApp, tap **Settings**, then **Account**, then **Two-step verification**.
2. Choose **Turn on** and set a six-digit PIN that you will remember. Add an email address in case you forget it.
3. Do not tell anyone the PIN.

If your account has been taken

Try to sign in again with your phone number. If you can, use **Settings** and **Linked devices** to remove anything you do not recognise. Tell your friends and family that messages from your number may not be from you. WhatsApp support can also help from their website.

You can report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

Contact us if you are locked out of WhatsApp, or would like help turning on two-step verification.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Buying and selling safely on Facebook Marketplace, Vinted and eBay

Online marketplaces are a great way to find a bargain or clear out your home. A few simple habits will keep you safe whether you are buying or selling.

When you are buying

- Be wary of prices that are far too good to be true.
- **Stay inside the site's own payment system** where there is one. On eBay and Vinted, buyer protection usually only works if you pay through the site.
- Be cautious if a seller asks you to pay by bank transfer, or to move the chat to WhatsApp or email.
- Check the seller's profile, age of account and reviews.
- For big items, such as a car or bicycle, see them in person first.

When you are selling

- Be careful of "buyers" who send you a link to "confirm payment" or "receive your money". Real sites do not do this.
- Beware overpayments. A buyer who sends too much and asks for a refund of the difference is probably using a stolen or fake payment.
- Do not post an item until the money is truly in your account. A message saying "payment sent" is not proof.
- Never share bank passwords, codes or card security numbers.

Meeting people

1. Meet in a busy public place, in daylight, or ask for collection by a friend.
2. Tell someone where you are going.
3. Do not let strangers into your home alone.

If something goes wrong

Report the problem inside the app or site first. If you paid by bank transfer, ring your bank on **159** or the number on your card straight away. Paying by credit card or PayPal offers extra protection in some cases. You can also report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or 0300 123 2040, or Police Scotland on 101.

When to get more help

If you are unsure about a sale, or a message has made you uneasy, ask us. We can look through it with you before you reply.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

How to create a strong password

A strong password is long, unique and hard to guess. It protects your accounts better than short passwords with clever symbols, and it is easier to remember than you might think.

What makes a password strong

- **Length:** aim for at least 12 characters. Longer is better.
- **Unique:** use a different password for every important account. If one site is breached, the others stay safe.
- **Not personal:** avoid names, birthdays, pets, football teams and anything on social media.
- **Not common:** avoid "password", "123456" and keyboard patterns like "qwerty".

An easy method

1. Pick three or four random words, such as "teapot river candle ladder".
2. Join them together, and add a number or symbol if the site asks for one.
3. Make sure it is not a phrase from a song or well-known saying.
4. Use this for your main email, and a different one elsewhere.

Keep passwords safe

- Use a password manager. Many phones and browsers have a built-in one, and they can make and remember passwords for you.
- If you write passwords down, keep the paper somewhere safe at home, not near the computer, and do not label it.
- Never share a password, including by email or text, even with someone who claims to be from your bank or from support.
- Turn on two-step sign-in so a stolen password is not enough.

Changing passwords

Only change a password through the official website or app, never via a link in an email or text. Change it at once if a site tells you it has been breached, if you used it on more than one site, or if you shared it.

When to get more help

Stop and ask for help if you are locked out, you cannot remember your main email password, you think someone has seen your password, or you are not sure how to set up a password manager. Do not reuse your old password. Tell us which accounts are affected.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

How to turn on two-step sign-in

Two-step sign-in (also called two-factor or 2-step verification) asks for a second proof that it is really you, usually a code, as well as your password. Even if someone steals your password, they cannot get in.

Before you start

- Have your phone to hand, and be signed in to the account on a trusted device.
- Start with your email, as it can reset your other accounts. Then do banking, Apple, Google, Microsoft and social media.
- Menu wording changes from time to time, so the names below may differ slightly.

Step by step

1. **Google:** go to your Google Account, choose **Security**, then **2-Step Verification**, and follow the steps.
2. **Microsoft:** sign in to your Microsoft account, open **Security**, then **Advanced security options**, and turn on **Two-step verification**.
3. **Apple:** on an iPhone, open **Settings**, tap your name, then **Sign-In & Security**. Two-factor authentication is on by default for most accounts, so you may find it already enabled.
4. **Other sites:** look in **Security** or **Account settings** for **Two-factor**, **2-step** or **Multi-factor**.
5. Choose how to receive codes. An authenticator app is safer than text messages, but text messages are much better than nothing.
6. Save any backup codes the site gives you and keep them somewhere safe, away from the phone.

Staying safe

- Never read a code out to anyone who contacts you. Scammers phone and say they need the code. Real firms will not ask.
- If you get a code you did not request, someone may know your password. Change it straight away.
- Keep your phone number up to date with your accounts.

When to get more help

Stop and ask for help if you have lost your phone, changed your number, cannot get codes, or are locked out. Do not trust anyone who contacts you offering to help. Tell us which account and which device you used.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Has your email been in a data breach? Using Have I Been Pwned

Sometimes a company is hacked and customer details are leaked. A free website called Have I Been Pwned lets you check whether your email address was caught up. It is run by a respected security researcher and is widely trusted.

What a breach means

A breach means information such as email addresses, and sometimes passwords, was copied from a company's systems. It does not mean your own computer was hacked. It does mean you should change the password for that company.

How to check safely

1. Open your web browser and type **haveibeenpwned.com** into the address bar yourself.
2. Enter your **email address** in the box and press the search button.
3. Read the result. Green means no breach was found. Red lists the companies that lost your details.

Never type your password into the email box. The site only needs your email address. It will never ask for your password to check an email.

If your email was found

- Change the password on each site listed.
- If you used the same password anywhere else, change it there too.
- Turn on two-step sign-in where it is offered.
- Be extra careful with emails and texts, because scammers may use leaked details to sound convincing.

Do not be alarmed

Most people find their email in at least one breach. It is very common and often involves old accounts. The important thing is that you act on it.

Staying alert

You can sign up on the site for a free alert if your email appears in a future breach. You will get an email from the site to confirm it first.

Be careful of copies

Only use the real address haveibeenpwned.com. Fake lookalike sites exist. Never trust a message that says "you were hacked, click here to check".

Report problems

Forward suspicious emails to report@phishing.gov.uk. If you lose money, ring your bank on 159 and report it to Report Fraud (formerly Action Fraud) on 0300 123 2040, or Police Scotland on 101.

When to get more help

If you find several breaches and are not sure where to start, we can help you sort your passwords out one at a time.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Securing your Facebook and Instagram accounts

Facebook and Instagram are the platforms where we see the most hacked accounts. A few settings take about ten minutes and make it much harder for someone to break in.

Why accounts get taken

Often someone is tricked into giving away a password or a code, or used the same password as on another site that was leaked. Once in, a criminal may message your friends asking for money.

Step 1: A strong, unique password

Choose a password you do not use anywhere else. Three random words is a good approach.

Step 2: Turn on two-step sign-in

On Facebook:

1. Tap your profile picture, then **Settings & privacy**, then **Settings**.
2. Choose **Accounts Centre**, then **Password and security**.
3. Tap **Two-factor authentication** and choose your account.
4. Pick an **authentication app** or **text message** and follow the steps.

On Instagram: go to your profile, tap the menu, then **Accounts Centre**, then **Password and security** and **Two-factor authentication**.

Step 3: Check your sign-ins

In **Password and security**, look at **Where you are logged in**. Log out of any device you do not recognise.

Step 4: Privacy settings

- Set your posts to **Friends** rather than Public if you prefer.
- Check who can see your friends list and phone number.
- Be careful what you share, such as holiday dates, your address or children's school.

Watch for tricks

- Friend requests from people you are already friends with, because that may be a copy account.
- Messages with a link saying "is this you in this video?"
- Emails claiming your page will be deleted unless you click.

Never share a code sent to your phone, even with a friend.

Report fake accounts

Use the three dots on a profile, choose **Report**, and follow the steps.

When to get more help

If you would like us to sit with you and check your settings, or your account has already been hacked, get in touch. Our guide on recovering a hacked social media account may help too.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Staying safe online

Staying safe online mostly comes down to a few good habits. You do not need to be technical, and you do not need to be afraid. Doing a handful of simple things protects you from most problems.

The basics

- Use a different strong password for each important account, such as email and banking. A password manager can remember them for you.
- Turn on two-step sign-in wherever it is offered, especially for email and banking.
- Install updates on your computer, phone and tablet when they appear.
- Keep your security software switched on and up to date. Windows includes Windows Security, which is good for most people.

Think before you click

1. Be cautious of unexpected emails, texts and calls, particularly ones that create urgency, offer prizes or ask for money or personal details.
2. Do not click links in messages you were not expecting. Open your bank or provider's website or app yourself instead.
3. Banks and the police will never ask you to move money to a "safe account", or ask for your PIN or full password.
4. Only download apps from the App Store or Play Store, and programs from the maker's own website.

If you think something is wrong

- If you have been scammed, contact your bank straight away using the number on your card.
- Report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.
- Forward scam texts to 7726, and scam emails to report@phishing.gov.uk.

It is never your fault, and scammers are good at what they do. Reporting helps protect others.

When to get more help

Stop and ask for help if you have clicked a link or opened an attachment and feel unsure, have given details to someone you do not trust, or your computer is behaving strangely afterwards. Do not feel embarrassed, as we have seen it all before. Tell us what happened and when.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

How to check whether a website is real

Fake websites can look just like the real thing, so it helps to have a few simple checks. None is perfect on its own, but together they catch most fakes.

Checks you can do

1. **Read the address carefully.** Look at the part just before ".co.uk" or ".com". A fake might add extra words or swap a letter, such as "royalmail-parcel-help.com".
2. **Do not rely on the padlock.** The padlock only means the connection is private. Scammers can have padlocks too.
3. **Be wary of how you got there.** A link in a text or email is riskier than typing the address yourself or using a bookmark.
4. **Look for contact details.** Real shops show a UK address, phone number and clear returns policy.
5. **Check the price.** A brand new item at a huge discount is a red flag.
6. **Search the name with the word "reviews".** Look for independent opinions, not only the ones on the site.
7. **Look at the spelling and design.** Poor grammar and blurry logos are clues, though good fakes look polished.

Handy tools

- Use the **Check a website** tool from Get Safe Online at [getsafeonline.org](https://www.getsafeonline.org).
- Check companies on Companies House at find-and-update.company-information.service.gov.uk.

Be cautious about

- Pop-ups asking you to "verify" your account.
- Pages asking for far more than you would normally give, such as your PIN.
- Sites that ask you to pay only by bank transfer or gift card.

Safer habits

Bookmark the sites you use, such as your bank. Use the official app instead of searching, because fake sites can appear in search adverts.

If you think you have used a fake site

Do not enter any more information. If you typed card details, ring your bank on 159 or the number on your card. If you typed a password, change it on the real site. You can report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or 0300 123 2040, or Police Scotland on 101.

When to get more help

If you are not sure about a website, send us the address and we will take a look for you.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Do you need antivirus beyond Windows Security?

Many people are told they must buy extra antivirus software. For most home users, the free protection already built into Windows is good enough, as long as it is switched on and you stay careful.

What Windows Security is

Windows 10 and 11 come with **Microsoft Defender**, part of an app called **Windows Security**. It scans for viruses, blocks harmful downloads and provides a firewall. It updates itself automatically.

Is it enough?

For most people, yes. Independent testing has found it works well. Similarly, Macs have built-in protections and Apple checks apps in its store. The biggest risk is not a missing program but being tricked into handing over details or installing something yourself.

When paid antivirus can help

- You like extras such as a password manager, a VPN or identity monitoring.
- You want one product covering several devices.
- You would like a helpline.

These are optional extras, not a must.

What to be careful of

- **Never trust pop-ups** that say your computer is infected and tell you to call a number or buy something.
- Do not run two antivirus programs at once, as they can slow things down and clash.
- Be wary of "free" antivirus from unknown sources, as some is itself unwanted software.
- When a paid subscription renews, check the price. Many renew at higher rates.

How to check Windows Security is on

1. Click **Start**, type **Windows Security** and open it.
2. Look for green ticks on the main screen.
3. If you see a yellow or red mark, click it and follow the suggestion.
4. Choose **Virus & threat protection** and then **Quick scan** for a manual check.

Keep it working

The best protection is keeping Windows and your apps updated, using strong passwords and two-step sign-in, and thinking before you click.

When to get more help

If you have two antivirus programs, a warning you do not understand, or a bill for security software you do not remember buying, contact us and we will sort it out.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Medium | 2 min read

Ransomware basics and why backups matter

Ransomware is a type of harmful software that locks your files and demands money to unlock them. It sounds frightening, but a simple habit makes it far less of a worry: keeping good backups.

How ransomware usually arrives

- Opening an attachment in an email you were not expecting.
- Clicking a link to a fake website.
- Installing software from an unreliable source.
- Not keeping the computer up to date.

Signs something is wrong

- Your files will not open, or their names have changed.
- A message appears demanding payment and giving a deadline.

What to do if it happens

1. **Disconnect the computer from the internet**, by turning off Wi-Fi or unplugging the cable.
2. Unplug any external drives, so they are not affected too.
3. **Do not pay.** Payment does not guarantee you get your files back and it encourages the criminals.
4. Do not restart repeatedly or try to delete things.
5. Get help from someone you trust. We can check what has happened.
6. Report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

Why backups are your safety net

If you have a recent copy of your files somewhere else, you can clean the computer and restore them. No ransom is needed.

A simple backup plan

The common advice is "3-2-1":

- Keep **3** copies of important files.
- Use **2** different places, such as an external drive and the cloud.
- Keep **1** copy away from the computer.

Disconnect an external drive when you are not backing up. A drive left plugged in can be locked too.

Reduce the risk

- Install updates when asked.
- Be careful with attachments, especially from people you do not know.
- Keep Windows Security turned on.

When to get more help

If you are not sure your files are backed up, ask us to set up a plan with you. It takes less time than most people expect.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Staying safe on public Wi-Fi

Free Wi-Fi in cafes, hotels, trains and libraries is handy. It is generally fine for casual use, but a few habits will keep your information safe.

Why care?

Public Wi-Fi is shared with strangers. On a poorly protected network, someone could snoop on what you do or set up a fake network with a convincing name, such as "Cafe_Free_WiFi". Modern websites are mostly encrypted, which helps a great deal, but it is sensible to take care.

Simple habits

1. **Confirm the network name** with staff before you connect.
2. Choose networks that need a password, where possible.
3. Be wary of a sign-in page asking for lots of personal information. A genuine one asks for little, such as an email address or a room number.
4. Look for the **padlock** in the address bar. It shows the connection to that website is private.
5. Turn off automatic connection to open networks in your settings.
6. **Forget the network** when you have finished.

What to avoid on public Wi-Fi

- Online banking and shopping, where you can.
- Entering passwords on sites you do not know well.
- Sharing files or leaving file sharing on.

A better choice

Your **mobile data** (4G or 5G) is usually more private than public Wi-Fi. For banking on the go, use your phone's data instead. Many phones can also share their data with a laptop, using **Hotspot** in settings.

About VPNs

A VPN adds an extra layer of privacy on public networks. It can help but is not essential if you follow the habits above. Choose a well-known provider, and avoid free ones you have not researched.

Keep your device updated

Updates fix security gaps, so install them regularly.

If you think you have been caught out

Change the passwords you used while on the network. If you entered card details, ring your bank on 159 or the number on your card.

When to get more help

If you travel a lot and want us to help set up your phone or laptop for safer use abroad or on trains, just ask.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Shopping online safely

Shopping online is convenient and, with a few habits, very safe. Millions of UK shoppers do it every day without problems.

Before you buy

- **Stick to shops you know** or those recommended by people you trust.
- If it is a new shop, search its name with the word "reviews" and look for independent opinions.
- Check that the web address looks right and the site has a UK address, phone number and returns policy.
- Be sceptical of prices far lower than anywhere else.

How to pay

1. **Use a credit card** if you can. Under Section 75 of the Consumer Credit Act, you may be able to claim from your card provider for purchases between £100 and £30,000 if something goes wrong.
2. A debit card has some protection through the chargeback scheme, though it is not a legal right in the same way.
3. **PayPal** is a good option, because the shop never sees your card number.
4. Avoid paying by bank transfer to people or shops you do not know. It is hard to get back.
5. Never pay by gift card or crypto for a purchase.

At the checkout

- Look for the padlock, but remember it is not a guarantee of honesty.
- Only give the details needed: name, address, card details. A shop never needs your PIN.
- Do not save your card on sites you rarely use.

Afterwards

- Keep your order confirmation.
- Check your bank statement for unfamiliar payments.
- Be wary of "delivery problem" texts. Check the order in the shop's own app or website.

Make it extra safe

Use a different password for each shop. Turn on payment alerts in your banking app. Check your statements regularly.

If something goes wrong

Contact the seller first, then your card provider on the number on the back of your card. Citizens Advice can help with consumer rights. To report a scam, contact Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

If you would like us to go through your accounts and saved cards with you, we are happy to.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Scams & online safety | Easy | 2 min read

Keeping an older relative safe online: how to start the conversation

If you are worried about a parent, grandparent or friend falling for scams, it is natural to want to help. How you raise it often matters more than what you say. The aim is to protect them while keeping their confidence and independence.

Choose your moment

Pick a calm time, not just after a scare. Start with a question rather than a warning, such as "Have you had any odd calls or messages lately?"

Be kind, not critical

Scammers are professionals who trick intelligent people every day. Say so. Avoid phrases like "you should know better". If they feel embarrassed, they may hide a problem rather than tell you.

Agree a few simple rules together

1. **If anyone asks for money or details, pause and check with someone first.** A family member, a neighbour or us.
2. **A real bank or the police will never ask you to move money.** Hang up and ring 159.
3. **Never let anyone take control of your computer.**
4. **Never share codes sent by text.**
5. **Real companies do not mind waiting.** Anyone pressing for a quick decision is suspicious.

Practical help you can offer

- Set up call blocking, or a call-screening phone, to cut down cold calls. Register with the free Telephone Preference Service at tpsonline.org.uk.
- Turn on two-step sign-in for email and bank apps.
- Help them use a password manager or a written list kept somewhere safe at home.
- Keep a short list of numbers by the phone, including their bank, Report Fraud and a family contact.

If they have been scammed

Stay calm and thank them for telling you. Ring the bank together on 159 or the number on the card. Report it to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101. Age UK and Citizens Advice can offer further support.

When to get more help

If you would like a hand setting up safer devices for someone you care about, we can visit or talk them through it.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.