How to protect yourself from fraud

Essential information for your own protection

The Cumberland

We take fraud very seriously and do a lot to help **protect you** from fraud

This leaflet explains how you can help **protect yourself** from being a victim of fraud

GENERAL FRAUD PROTECTION

1. Keep your cards safe and never leave them unattended.
2. Be cautious when using a cash machine, look out for anyone behaving suspiciously and any signs of tampering on the machine.
3. Never tell anyone else your PIN/password/access code/passcode/memorable word, and never write any of them down in a way which could easily be understood by someone else.
4. Be wary of unprompted phone calls, emails or text messages asking you for personal information. We'll never call, text or email you asking for account information.
5. Regularly check your account and let us know immediately if you notice anything unusual.

CUMBERLAND INTERNET BANKING

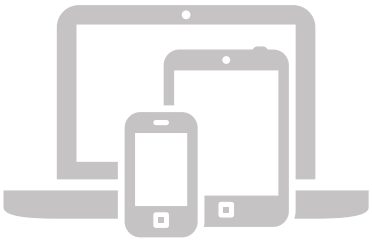
1. Only log on from our website www.cumberland.co.uk (or www.cumberland.co.uk/business for businesses).
2. Never open or respond to any emails you receive claiming to be from Cumberland Building Society, unless it's in response to an email you've sent to us or in relation to an application you've made with us.
3. Install firewall, anti-virus and anti-spyware on your computer. Keep them, your operating system and browser up to date and carry out regular scans.
4. If you have your own WiFi hub, make sure it's securely configured and password protected.
5. Don't use public computers to access Cumberland Internet Banking unless absolutely necessary, always ensuring your access details cannot be viewed by anybody else and you fully log out when finished.

CUMBERLAND MOBILE BANKING APP

1. Check your mobile devices are protected against the risk of downloading malware (malicious software) or viruses.
2. Set up a PIN or fingerprint on your mobile device, don't store your passcode/password or access code on it and don't share it with others.
3. Avoid using public Wi-Fi and disable Bluetooth when using our App.
4. Only ever download our App from the official app stores we've approved (iTunes or Google Play).
5. Don't install the Cumberland Mobile Banking App on a rooted or jailbroken device (i.e. a handset which has had its default operating system restrictions removed).

KEEP YOUR CONTACT DETAILS UP TO DATE

If we spot unusual transactions on your account, we'll contact you by phone or text to check these with you. It's therefore important that we have your up to date telephone numbers on our records. You can update your contact details in branch or by writing to us.



GENERAL FRAUD TIPS

Be wary of unsolicited calls/emails/text messages

- Treat unsolicited communications with caution and stay alert no matter what your caller display may show.
- To verify the identity of a person claiming to be calling from the Cumberland call us back on 01228 403141. When doing so you should use a different phone or wait for at least 10 minutes to ensure that a fraudster is not intercepting the telephone line.

Check your statements carefully

- Review your statements as soon as they arrive and tell us immediately about any suspicious transactions.
- If you're expecting a statement in the post and it doesn't arrive, please tell us.
- If you have Cumberland Internet Banking your statements are only available online and you should check these each month.

Destroy unwanted financial or personal paperwork securely

- Shred documents such as bills, statements and receipts before throwing them away.

The remainder of this leaflet gives more specific advice which should be followed in relation to debit card and online security, including the safe and secure use of Cumberland Internet Banking, and the Cumberland Mobile Banking App.

DEBIT CARD SECURITY

TAKE CARE OF YOUR CARDS

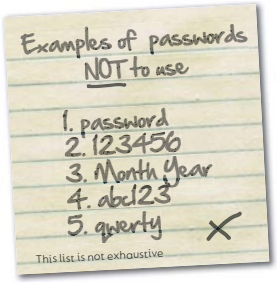
- Treat your cards in the same way you'd treat your cash.
- Don't let your card out of your sight when making a transaction.
- Never allow someone else to use your card.
- Never hand your card over to someone that comes to your door.
- Don't let anyone distract you when using your card and always put it away quickly afterwards.
- If you live in a property where other people have access to your mail, you can ask us to make your card unusable until you call us to say you've received it.
- If your card is lost or stolen, tell us immediately by calling us on 01228 403141. Ensure you leave a message on our automated service if calling out of hours, as by doing so your liability for any fraudulent transactions ceases at that point.

AT THE CASH MACHINE

- Be aware of others around you. If someone close by the machine is behaving suspiciously or makes you feel uncomfortable, use another one.
- If there's anything unusual about the cash machine or there are signs of tampering, don't use it and tell the building society, bank, Police or premises owner immediately.
- Avoid using cash machines in poorly lit or isolated areas.
- Don't accept help from 'well-meaning' strangers and never allow yourself to be distracted.
- Cover the key pad when using a cash machine to prevent anyone seeing your PIN when you enter it.
- If the cash machine doesn't return your card, tell us immediately.

PERSONAL CODES AND NUMBERS

- These include your PINs, passwords, access code, passcode and memorable word.
- Learn the PIN we send you and destroy the letter containing your PIN.
- Never choose personal codes and numbers which could be easy for others to guess (such as your date of birth).
- We'll never ask for your personal codes or numbers, either verbally or in writing.
- Never enter your PIN into a telephone keypad.



SHOPPING ONLINE

Register your card for Verified by Visa (VbV)

Verified by VISA

Whether or not you shop online, in the wrong hands your card details can be used without your authority. The VbV service provides password protection and helps prevent another person using your card online at participating online VbV retailers.

You can register your card for VbV:

- Through our website www.cumberland.co.uk
- Whilst shopping at a VbV registered retailer.

You'll never be asked to enter your full VbV password when shopping online; you'll only be required to enter certain characters.

One Time Passcode (OTP)

When you register for VbV for the first time, or when you reset your existing VbV password, you'll receive a unique 6 digit code referred to as One Time Passcode (OTP) via text message to your mobile phone. You'll need to enter the OTP online to complete your registration or password reset.

OTP helps prevent another person from being able to reset your VbV password and then carry out transactions using your debit card.

1. When shopping online at a participating VbV retailer, you will be required to enter your Visa debit card details to successfully complete your purchase as normal.

2. If you are not already registered for the VbV service you will be prompted to register for VbV and you will receive, via text, a unique 6 digit code (referred to as a OTP).

3. You will then need to enter your OTP to enable you to set your VbV password.

4. You will be prompted to set your VbV password and complete your VbV registration to enable you to continue shopping safely and securely online at participating VbV retailers.

Phishing

Phishing is where fraudsters contact you by email, text message or phone pretending to be a trustworthy company such as your bank or building society.

Phishing emails may ask you to click on a link which takes you to a website that asks you to enter sensitive information such as your card details, or trick you into downloading malicious software (malware) by opening an attachment. The website may look almost identical to the real one, but is actually fake.

If you receive a suspicious email which claims to be from us, forward it to emailalerts@cumberland.co.uk and then delete it.

Phishing text messages are sent by fraudsters who use software to change the sender ID so it looks like the message has been sent from a company, such as your bank or building society. The fraudulent text message can even appear in an existing conversation thread of genuine text messages that you've previously received from the company. We will never text you asking for personal or financial information.

Phishing can also be carried out by telephone and if you are suspicious you should always call your bank or building society back using the number which is publicised either on their website or on the back of your card in order to verify the identity of the caller. You should either wait for 10 minutes to ensure any potential fraudster is not still on the line, or use a different phone to return the call.

If you believe you've disclosed your personal or financial details to a fraudster, tell us immediately.

Only shop online using your own personal computer/mobile device

Although shopping 'on the go' in a public Wi-Fi area or using a public device may be convenient, the risks are greater and it is therefore best to avoid this. Stick to using your own computer or mobile device and only enter your card details using your own personal Wi-Fi.

Always use well known, reputable retailers

- Avoid buying from retailers you don't recognise.
- Check customer reviews if you've not used the retailer before.
- Ensure there's a physical address and telephone number for the retailer in case of queries.
- Carefully read the Terms and Conditions to make sure you don't unknowingly sign up to a regular recurring payment.
- Check the retailer's privacy and returns policies.

DEBIT CARD SECURITY

Only use secure websites

Only enter your card details into secure websites. Look out for the following reassuring signs:

- The website address should begin with https:// rather than http://. The 's' stands for secure.
- Look for a padlock or unbroken key symbol in the browser, next to the website address.
- Click on the padlock or key to check the certificate; this will tell you who has registered the website. If you get a warning about a certificate be very cautious before continuing.

SecureCard

Cumberland Visa debit cards can be used abroad[1], if you tell us the dates and destination of your travel.

SecureCard helps to protect your account as fraud can occur when a debit card is 'cloned' and then used to make purchases or withdraw cash in foreign countries. SecureCard gives you peace of mind knowing that your money will be protected from overseas fraud while you are in the UK.

You can set your card to be used in a foreign country for up to 31 days at a time. All you have to do is tell us the destination and dates of your travels in one of the following ways:

- Using Cumberland Internet Banking
- Using the Cumberland Mobile Banking App
- By calling us on 01228 403141 (+441228 403141 from abroad)
- By calling into any of our branches

We recommend that you have our telephone number with you when you go abroad

[1] The Channel Islands, Isle of Wight and Isle of Man are part of the UK and not classed as abroad.

CUMBERLAND INTERNET BANKING AND CUMBERLAND MOBILE BANKING APP SECURITY

The Cumberland website

Before logging on to Cumberland Internet Banking, look for our 'Secure Site' icon which will always be displayed. If the web page is valid, the icon will display a green tick. In this case, you can safely proceed to log on to Internet Banking. If the icon does not display a green tick, don't proceed.

When clicked, the icon will take you to a website, which will provide you with confirmation of the page's validity. If you have any doubts, do not log on and call us on 01228 403141.

How to protect you and your computer

- Install and maintain a firewall to protect your computer from unauthorised access by others.
- Set your browser security to the highest possible level which will allow you to continue using the internet as normal without blocking access. For guidance on how to do this, refer to the Help section of your internet browser.
- Don't allow someone you don't know have access to your computer, especially remotely (when you're not face-to-face with them).

How to protect you and your mobile device

- Follow your handset manufacturer and network service provider's security advice.
- Set up a password/PIN/fingerprint to access/unlock your mobile device.
- Don't choose a device password/PIN that can easily be guessed by anyone else.

INTERNET AND MOBILE SECURITY

- Don't share your password/PIN with anyone else.
- Don't store anyone else's fingerprint on your mobile device.
- Set your mobile device to lock after a period of inactivity.
- Don't let anyone else use the e-wallet on your mobile device. An e-wallet allows you to store debit cards on your mobile device and make payments using your device.
- Keep your mobile device software up to date and ensure it's protected against the risk of downloading malware (malicious software) and viruses. Make sure your mobile device's operating system and browser are updated to the latest version, including any security updates.
- Install and maintain security software (where available) that is specially designed for mobile devices and keep this up to date. Like computers, mobile devices are vulnerable to viruses.
- Don't modify your mobile device (known as 'jailbreaking' on an iPhone or 'rooting' on Android phones) to allow installation of unofficial apps. Doing this removes certain security features that protect your phone. Don't install the Cumberland Mobile Banking App on a jailbroken or modified device. If you do and as a result transactions take place on your account that you didn't authorise, we will not be liable for these transactions.
- Delete all data off any mobile device that you no longer need, before disposing of it.
- Treat your mobile device like your wallet - keep it safe at all times and don't share it with others.
- Make a note of your IMEI (International Mobile Equipment Identity) number. Should you lose your mobile, this will allow your phone operator to disable it. Type *#06# into your handset to get your IMEI number.

- Register your phone on the Immobilise National Property Register (www.immobilise.com) - there's a better chance of you being reunited with your mobile device if it is recovered.
- Tell us and your mobile network service provider immediately if you lose your mobile device.
- If you call out of hours, leave a message on the automated facility. By doing so your liability for any fraudulent transactions ceases at that point.

SIM Swapping

If you suddenly experience a flurry of nuisance calls or texts, or you experience an extended loss of mobile phone signal, tell your network provider and us immediately. This could indicate that a fraudster has taken control over your mobile phone account and has access to your calls and text messages, known as SIM swap fraud.

SIM swap fraud occurs when a fraudster contacts your mobile phone provider, pretends to be you, and asks to transfer your mobile telephone number onto a new SIM card. Once activated, the fraudster will receive all calls and text messages sent to your mobile number.

Once in control, fraudsters can bypass text message based One Time Passcodes which are used to reset passwords, access codes and to send online payments. They will also receive any text messages or calls made by your bank to check such transactions.

How to protect your Cumberland Internet Banking and Cumberland Mobile Banking App

- Don't use public computers to access Internet Banking and don't access the App through anyone else's mobile device.
- Don't use Internet Banking or the App in public WiFi 'hot spot' locations. Switch off the Bluetooth function on your mobile device when it's not in use and before logging into the App. This will stop any unmonitored wireless activity on your mobile device.

INTERNET AND MOBILE SECURITY

- If you believe that your access code, passcode, user name or memorable word is known by another person you should change it immediately.

If you must use a public computer to access Internet Banking, or you must access the App in a public place, take the following precautions:

- Be aware if anybody is near you who could watch you enter your personal information (known as 'shoulder surfing'). This includes ensuring that neither you nor your screen are being overlooked by CCTV cameras.
- Log out of Internet Banking when you've finished your session. Don't just close your browser, or simply get up and walk away.
- Quit the App once you've finished using it.
- Never leave your computer or mobile device unattended whilst you are logged on.

Third Party Providers

If you are registered for Internet Banking you may allow authorised third party providers to have access to your account information or to make payments from your account.

You must only allow a third party provider to access your account once you have checked that they are legitimate and that they are authorised under Financial Conduct Authority (FCA) regulations. You can check this on the FCA website (www.fca.org.uk).

HOW CUMBERLAND INTERNET BANKING AND THE CUMBERLAND MOBILE BANKING APP HELPS TO PROTECT YOU

Secure Messages

Internet Banking and the App contain a messaging service as a secure means of communication between you and us.

You should use the Secure Message service to contact us whenever possible. Alternatively, call us on 01228 403141.

SecureCall

SecureCall is a fraud prevention feature of Internet Banking which contacts you by telephone to confirm that it's you making certain payments from your accounts.

When a payment is being made from one of your accounts in internet banking to another person or company you haven't paid before, you'll receive an immediate automated telephone call to confirm that it is you trying to make the payment. The call will confirm the details of the payment and give you a code to enter into internet banking in order for the transaction to proceed.

That payee then becomes a trusted payee and you will not have to use SecureCall again for future payments you send to them*.

You can't make payments to another person or company you haven't paid before via the App. These payments should be initiated through Internet Banking. You are able to make payments to trusted payees via the App.

* You may receive a SecureCall for payments to trusted payees which are above certain monetary limits.

INTERNET AND MOBILE SECURITY

Secure Access

Internet Banking is a secure website that uses SSL (Secure Sockets Layer) protocol to ensure that all data transmitted via the internet is secured by encryption. When accessing Internet Banking you should see a padlock in your internet browser. When you select the padlock (by double clicking on it in most cases) you can view the certification details of the SSL being used. You should always ensure that the padlock is displayed and that the certification details are genuine by checking it has been issued to 'banking.cumberland.co.uk' and that the certificate remains within a valid date range.

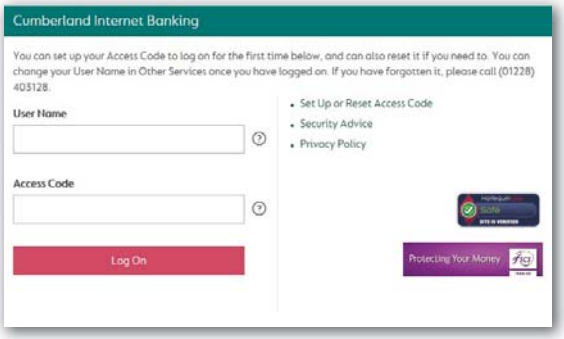
Internet Banking and the App contain features and functions designed to protect you and your money. Ensure you are aware of the importance and meaning of each one as detailed below:

Customer Number/User Name

You'll be provided with a unique Customer Number when you register for Internet Banking and this must be entered when you log on for the first time. You can choose an alternative User Name instead if you wish to do so and this will be used when you log on in future. Your Customer Number and User Name should be kept safe and should not be shared with others.

Access Code

This is a unique code given to you when you register for Internet Banking. You'll be required to change your Access Code to one of your choice when you log on to Internet Banking for the first time. You'll need to enter your chosen Access Code on each subsequent occasion you log on to Internet Banking. For your own security, if you incorrectly enter your Access Code too many times your logon will be suspended and you will not be able to gain access to Internet Banking. This is designed to prevent unauthorised access by potential fraudsters.



If you forget your Access Code, or if your logon has been suspended, you should call us to request a new Access Code. Alternatively, if your mobile number is registered with us you can reset your Access Code on the Internet Banking log on page.

Memorable Word

When you log on to Internet Banking for the first time you'll be required to set a Memorable Word which will be used every time that you log on. When choosing your Memorable Word you should not use any information that is also used for social media or other aspects of online life, and it should be kept secret at all times.

Alerts

When you log on to Internet Banking you will be informed of any failed attempts to use your logon where the Access Code or Memorable Word has been entered incorrectly.

You can set up text alerts to notify you when your Access Code has been changed, or when your Internet Banking access has been suspended due to too many failed log on attempts.

We recommend that you activate these text alerts and ensure that you are satisfied that any failed log on attempts were made by you.

INTERNET AND MOBILE SECURITY

Last Logon

When you log on to Internet Banking, you will be informed of the last time your logon was used successfully. We recommend that you take notice of this information and ensure that you are satisfied that it was you who logged on, and not anybody else who has gained unauthorised access.

Session Summary

Every time that you log on to Internet Banking or the App a unique 'Session ID' is allocated. You can access a record of each of your logon sessions which includes the date, time and duration of each session, as well as details of specific activities, including payments and transfers, which were carried out during each one.

Automatic idle log off

If you log on to Internet Banking and don't actively use the site on your device for 15 minutes or more, you'll be logged off automatically. Although we recommend that you log off Internet Banking as soon as you've finished your session, this facility acts as a 'safety net' and assists in reducing the risk of any unauthorised users from accessing your accounts.

BUSINESS USERS ONLY

My Users

Internet Banking requires your business to appoint a Primary User who is responsible for managing the permissions of other staff (Delegated Users) who are given access to Internet Banking. This allows your business to give staff varying levels of access to your business accounts including the ability to carry out transactions up to maximum values you set. The Primary User can give Delegated Users permission to use, or restrict them from using, many of the functions in Internet Banking. The Primary User can also monitor their internet banking activity within Internet Banking by using text message alerts (date, time and duration of each session, and details of specific activities, including payments and transfers carried out).

CHEQUE FRAUD

- Keep your cheque book in a safe place and separate from your debit card.
- Complete all sections of the cheque (date, payee, amount in both words and figures) and don't forget to sign it
- Cheques should only be signed by the individuals named on the account.
- Add additional details next to the name of the person or company you're paying when possible, for example an account number or bill reference (eg. HMRC, Reference XYZ).
- You should draw a line through unused spaces and include the word 'only' after writing the amount in words.
- If you make a mistake, cross it out and sign your name next to the correction.
- Never sign blank cheques.

IDENTITY THEFT

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud.

Fraudsters can use stolen identity details to:

- Open bank accounts in your name.
- Obtain credit cards, loans and state benefits in your name.
- Order goods in your name.
- Take over your existing accounts.
- Take out mobile phone contracts.
- Obtain genuine documents such as passports and driving licences in your name.

How can you protect your identity?

- Shred documents with personal details on – such as name, address, financial details.
- Don't make personal data, such as your address and date of birth, publicly available on social media. Make sure the privacy settings on your profiles are set to private.
- Do not give personal details out over the phone or in response to an email or text message.
- Check statements carefully, and report any suspicious transactions to us.
- If a statement doesn't arrive, tell us immediately.

You can check your identity hasn't been stolen by getting a copy of your credit report from a credit reference agency such as:

- Experian www.experian.co.uk or
- Equifax www.equifax.co.uk or
- Call Credit www.callcredit.co.uk

This list is not exhaustive and there may be charges for these services.

Our promise to you

When you use our online banking services you are protected by our safe and secure promise, shown opposite. This means that if a fraudster takes money from your account, we'll refund the transactions to your account so it's like it never happened. This includes refunding any charges and interest you've incurred, and paying any interest you have missed out on.

You may however be liable for the full amount of any losses if you have acted fraudulently or with gross negligence (for example, allowing someone else to use your card, telling someone else your personal information, keeping your card and PIN together, not contacting us immediately to report a loss or theft, or leaving bags, wallets or purses unattended).

You must tell us immediately if you notice any unauthorised transactions on your account, or if your debit card is lost or stolen.

THINGS WE'LL **NEVER** DO...

1. Ask for your PIN number or any online banking passwords over the phone or via email or text message
2. Send someone to your home to collect cash, bank cards or anything else
3. Ask you to email or text personal or banking information
4. Ask you to authorise the transfer of funds to a new account or hand over cash
5. Call to advise you to buy diamonds, land or other commodities
6. Ask you to carry out a test transaction online

OUR PROMISE TO YOU

Safe and secure
our promise to **you**

Our banking services have been designed to protect you and your money, but you must also take all the precautions we recommend in our terms and conditions and fraud guidance to ensure that your devices are secure and that your personal details are kept safe. Unless you have been careless in your use of these services, we will fully reimburse the money taken from your account.

Simple as that.

The following websites contain important information on protecting yourself against fraud and identity theft.

www.getsafeonline.org - a site which gives valuable advice and information about internet safety.

www.actionfraud.police.uk - a site provided by the National Fraud Authority, the government agency that helps to co-ordinate the fight against fraud in the UK.

www.financialfraudaction.org.uk - simple advice from Financial Fraud Action UK on how to stay safe when shopping online.

www.fca.org.uk/consumers/scams - The Financial Conduct Authority (FCA) site that provides guidance on how to avoid scams.

Cumberland Building Society is not responsible for the content of these external internet sites.

Cumberland Building Society
Cumberland House, Cooper Way,
Parkhouse, Carlisle, CA3 0JF

Phone: 01228 403141

customerservice@cumberland.co.uk

cumberland.co.uk

The Cumberland

recycle
INV407 12/17 V8