QIIB الدولي الإسلامي

eBanking Security Tips

How we protect you:

- Online and mobile banking guarantee
- Free Security Software
- Other Ways we protect your money.

How you can protect yourself:

- Protect yourself from fraud.
- Financial scams and how to avoid them.
- On line and mobile banking security.
- Card fraud.

Need help with fraud or security?

- Report Fraud.
- Lost and stolen cards.
- Check and fraud team phone number.

How we protect you:

Online and Mobile Banking Guarantee:

When you use our Online Banking or Mobile Banking services, you're automatically protected by our Online and Mobile Banking Guarantee. This means that, if any money is taken from your account by a fraudster via these services we'll put your account back as if it hadn't happened – including paying back the money, refunding any charges and interest you have paid, and paying any interest you've missed out on.

Our promise to you

In the unlikely event that a fraudster takes money from your account using our Online or Mobile Banking services, we'll put your account back as if it hadn't happened – that means we'll pay back the money, refund any charges and interest you have paid, and pay any interest you've missed out on.

When we won't refund you

If we have reasonable grounds to think you're not entitled to a refund, we may look into your claim first.

We won't give you a refund if we reasonably think you have acted fraudulently, and we may involve the police in these cases.

If you have either deliberately, or with gross negligence

- Failed to keep your card, PIN, password, PINs entry or mobile PINs entry generated codes, device or equivalent secure.
- failed to tell us as soon as possible that you have lost your card or mobile (especially if you think someone else might be able to find or use it)

We won't refund any payment made before you told us your card or security details have been lost or compromised.

Protecting your account

We give you tools, which are personal to you, so you can log into your online or mobile banking and carry out transactions. These include your Online Banking passcodes and memorable word, PINs entry generated codes, and your 5–digit passcodes for Qiib Mobile Banking or Qiib Ping it. It's important you keep these safe:

- Make sure that other people can't read your security information (for example, by not using a shared email or mobile)
- Memorise your PIN, password or passcodes and destroy any letter that includes a PIN
- Choose a PIN, password or passcode that's difficult to guess (for example, you shouldn't use something like '1234' or your date of birth)
- Never give your PIN, full password, or passcode to anyone, or write them

down in a way they might be recognised
- Never share PINs entry generated codes with anyone who contacts you
- Don’t give someone access to a device where your details are stored
- Contact us as soon as possible if you think someone else has used, or may be able to use, your card, PIN or password
- Take reasonable care when using Online Banking and Mobile Banking (log out at the end of each session and don’t leave your computer or mobile unattended while you’re logged in)
- Carry out regular internet security checks and software updates
- Comply with security requirements for your device and any other requirements we tell you about

Other ways we protect you when you're using online and mobile banking

- One secure log-in protects your accounts on Qiib Mobile Banking and Qiib Ping it
- We'll automatically log you out when you navigate away from the apps, or if you haven’t used the apps for 3 minutes or online banking for 10 minutes
- If you’re an Online Banking user, your PINs entry device or the Mobile PINs entry tool in Qiib Mobile Banking app provides an extra level of protection for your more security-sensitive transactions, keeping your money safe from fraudsters
- Your security is our priority but you can take some steps yourself to make using our service even more secure

- **Important information:** Lines are open 24 hours a day, 7 days a week. To maintain a quality service, we may monitor or record phone calls. Call 000000

How we protect you:

What we're doing to protect your account

Protecting your account

We’re always keeping an eye out for threats from hackers and fraudsters. Here are some of the measures we take to make sure your money is safe.

On this page:

Security standards and accreditation.

Shopping online

Fraud monitoring

Free security software

Protecting your devices with security software helps protect your accounts from malicious software used by fraudsters.

Our Online and Mobile Banking Guarantee

If a fraudster manages to steal money from your account, you’re automatically protected by our Online and Mobile Banking guarantee. This means we’ll refund any money that may be fraudulently taken from your account, as long as you've used the services correctly.

PINs entry

PINs entry provides a strong layer of protection in addition to your login details, and helps keep your accounts even safer. It works by asking you to insert your Qiib debit card and PIN into a card reader that we send you. The reader generates a unique security code that you'll need to type into Online Banking. And if you register for our mobile banking app, you can get the code on your smart phone using Mobile PINs entry. That way, you get the additional security when logging in without needing to carry your card reader around.

Our online security system

- **Data encryption** - Our Online Banking service is hosted on a secure, 256-bit encrypted server. This means that any information you send us is scrambled for your protection
- **Timed log out** - We’ll log you out if you don't use the service for 10 minutes. This gives you added protection if you forget to log yourself out
- **Deactivation of your login details** - We'll automatically disable your access to Online Banking if 3 incorrect log in attempts are made. This is to stop fraudsters making repeated

attempts to get into your accounts

Security standards and accreditation

Managing your money online or on your smart phone is easy and convenient. And it's so safe that we have received the following security certifications and awards:

- Kite mark for Secure Digital Transactions – awarded to our Mobile Banking and Barclays Ping it apps by the British Standards Institute (BSI). Both apps have been independently tested to ensure they protect your financial and personal data
- Cyber Essentials Scheme – a government-backed programme that recognises

  Good security practices in business

We offer free security software and our Online and Mobile Banking Guarantee protects you from losses (as long as you've used the services correctly).

Shopping online

Qiib Secure (in association with Verified by Visa (Link opens in a new window) protects your cards against unauthorised use when you shop online at participating retailers. Qiib Secure assesses whether additional security information is needed to verify your purchase. In most cases, no further verification is required but, in certain circumstances, we'll ask for some additional security information.

Fraud monitoring

We're always checking for any suspicious activity on your account, so you may get a text message or call from our automated system to confirm a recent transaction or a change of address. We may sometimes delay or decline transactions that are out of character for you, or even block your account until we can confirm that you're making the transaction. Keep your contact details up to date so we can contact you quickly to minimise any inconvenience.

If we do call, we'll never ask for your passcodes, passwords, PIN, card details, PINs entry codes or sensitive account information.

If you get a call from someone claiming to be from our Fraud Team and you think it's suspicious, call us back using the number from our website.

How you can protect yourself:

Fraud is a serious problem

Check out our fraud smart tips to help protect yourself against it, and remember that we'll never call you and ask for your passcode, password, PIN or PINs entry code

Always Check:

- Stay alert when someone you don't know calls you – no matter who they claim to be. Often fraudsters will claim they're from a bank or the police and then trick you into transferring money to a fake account
- If someone calls asking for your personal details, end the call. Then call the company back at a telephone number found on their official website (or from one of your statements or bills). Always check the initial call has been properly disconnected by calling someone you know first and then call the company back. Or, better yet, use a different phone
- If you get an automated call from our fraud-detection service, we'll only ask you to confirm your date of birth by selecting from several choices; we won't ask you for any other security details. Use our telephone number to always check the number is a genuine QIIB Fraud Department number
- Always check a website is secure before you enter any account or card details. Look for the `https' at the start of the web address and the gold padlock or unbroken key icon at the top of the page next to the address bar
- Always check other people can't see or hear your details when making payments in store, online or by phone. Afterwards, check your statement and contact us straight away if you spot anything unusual. Read more about different types of Financial Scams to help protect yourself from them

Never Share:

- Never share your personal or security information on a website you've reached via a link in an email. We will never email you a link that takes you straight to the Online Banking page
- Never share your PIN, PINs entry codes and passwords with anyone who contacts you. If a caller does ask for this information, end the call
- Never enter your card PIN into a telephone – it doesn't keep it secret from the caller
- Never share confidential information via email

ACT With Care:

- Act with care when clicking on links or downloading attachments from unsolicited emails or texts. Forward suspect emails claiming to be from QIIB to "contactus@qiib.com.qa" and then delete them
- Only download apps, files or programmes from trusted sources, such as official sites or app stores
- When logging on to online banking, always type the web address into the browser or use QIIB' official mobile banking app
- Treat all unsolicited calls with caution. Remember, banks and Police will never contact you to ask you to transfer funds, buy high value goods, or hand over cards or money
- Don't enter reference or amount details into the PINs entry card reader unless you wish to make that payment
- Never write down your security details or passwords in a way someone else would recognise
- Call us straight away if your card, PIN or other security details have been compromised

Financial scams and how to avoid them

Phone calls, letters, emails and texts from scammers can seem legitimate and convincing so

it’s important to be vigilant and keep an eye out for anything suspicious.

Become familiar with some of the more common scams listed below. If you think you may have been a victim of a Fraud, report it immediately to Action Fraud, either by calling 44840005 straightaway if someone has taken money from your account or you think you have accidentally given your details to a fraudster.

Email scams:

Phishing’ is where fraudsters send you emails with links to bogus sites or they may ask you to fill in an online form to capture your security information. Other emails trick you into downloading malicious software (malware) that helps fraudsters get hold of your details and your money. The emails look like they are from legitimate organisations and give a plausible story to try to trick you into clicking a link, downloading something or opening an attachment.

Some emails try to trick you into opening attachments which install something known as ‘ransomware’ on your computer. It encrypts all of your files, including music and photos, and the scammer then asks for a ‘ransom’ to release them. Protect your computer and devices with the most up-to-date security software and be wary of opening attachments or links in emails you’re not expecting or are unsure about. Keep your important files backed up off your network and never pay ransom money to criminals.

Emails from QIIB
we may contact you by email from time to time with useful advice and information about products and services, but we will…

- Never email you a link that takes you straight to the Online Banking log-in page
- Never email you asking you to verify your account details
- Never email (or call) to ask you for card details, PINs, PINs entry codes or passwords
- Never email you asking you to confirm a recent transaction

If you have received a suspicious email that claims to be from us, please forward it to “contactus@qiib.com.qa” and then delete the email immediately.

Scam phone calls:

Vishing’ is similar to phishing but involves a phone call from a fraudster, who will come up with a plausible story to try to get you to divulge your information. For example, the fraudster may say they’re from a satellite TV provider, phone or utility company and offer you a refund. To process the refund, they'll ask you to input your debit card into your PINs entry card reader and give your authorisation codes.

They'll then use the codes to make fraudulent Online Banking payments from your account. Never share your PIN, PINs entry codes or passwords with anyone who contacts you.

Fraudsters also call pretending they're the bank or the Police and tell you there's a problem with your debit or credit card. They may ask you to key your card PIN into the phone and tell you they are sending a courier to collect your card. Alternatively, they may ask you to withdraw funds or buy high value items and hand them to a courier to help in an investigation, or even try to convince you to transfer funds to a new 'safe' account. Banks and the Police will never ask you to hand over your PIN, cards or cash, or buy high value items or transfer funds to a new account. If someone calls asking you to do this, end the call. Always check the call is properly disconnected before calling the bank or Police to report it – wait 5 minutes or use a different phone.

Investment scams:

This is when scammers pose as salespeople and contact you offering investment opportunities like shares, plots of land, gold, carbon credits or wine. The caller will often tell you that the opportunity will be missed if not acted upon quickly. Despite the promise of a high return, the investment turns out to be worthless. If anyone offers you an investment opportunity out of the blue, does some research before you take the plunge. Get independent advice – call the call centre on 44840000 for guidance. Remember, if it sounds too good to be true, it probably is.

Advance fee scams:

This type of scam involves the promise of a large sum of money or other opportunities, like a lottery win, inheritance claim or prize draw. You'll be asked to pay an upfront fee which the scammer will take, but you'll see nothing in return. Treat any such offers with suspicion. Genuine organisations dealing with the lottery winnings, prize draws or inheritance payments never ask for a fee before paying out your money.

Software scam:

A caller will claim to be from a computer company or the technical department of a bank and tell you your computer has a virus. They'll convince you to install some special software which will allow them to access your passwords and account details. Sometimes they try to charge you for the software or for their 'help'. Legitimate computer companies and banks will never call you out of the blue to say that your computer needs repairing. If you do get such a call, don't follow their instructions to go to a website and don't type

anything into your computer or install software.

Pension scams:

Pension scams typically involve promises of pension investment opportunities or unsolicited offers to help you release cash from your pension early.

With over 55s getting greater access to their retirement savings from April 2015, there are more opportunities for investment scammers to convince people to invest their pension pots in unregulated or bogus schemes.

Anything claiming you can cash in your pension before the age of 55 is also likely to be a scam, and early pension release may cost you most of the money in your pension fund. Ignore offers of a 'free pension review' and calls out of the blue to discuss your pension. Never be rushed into agreeing to a pension transfer or investment decision.

Online shopping scams:

Scammers will advertise goods/services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive. Before buying online do some research into the seller to check that they're genuine and avoid those with poor ratings. Insist on seeing high-value items, like cars on online auction sites, before paying and always use secure payment methods, such as PayPal or credit card.

Money mules:

Unfortunately, in the majority of cases, Barclays will not be able to recover the funds for you if you have paid money away to a scam. However, we do take all cases seriously and our staff will be happy to take the details of your case. The information will be used to support our continued efforts to combat fraud and help protect you and others from falling victim to such scams.

Online and mobile banking security

Our security awards

Managing your money online or on your smartphone is easy and convenient. And it's so safe that we have received the following security certifications and awards:

- payments safe and secure
- Cyber Essentials Scheme – a government-backed

programme that recognises good security practices in business

Our top 10 security tips for banking online and on your mobile:

- Protect your computer and mobile devices with up-to-date security software and install regular security and software updates.
- Only use official mobile banking apps provided by your bank, eg QIIB Mobile Banking and QIIB, only download apps from an official app store.
- Never log in to Online Banking through a link in an email. Either type the address into your browser or use your bookmarks.
- Use PINs or passwords that are hard for someone to guess. For example, use a mix of letters, numbers and symbols for passwords. Change your PIN or password immediately if you think someone may have discovered it.
- Don't give anyone your security details and never write them down or store them on your mobile in a way that might be recognised by someone else.
- Never give your PIN, password, PINs entry codes or full security details to anyone who calls you or in an email or text message.
- Be wary of opening attachments or clicking on links in emails or texts that you weren't expecting or are unsure about.
- Banks will never call you and ask you to transfer money to a new account, so ignore such calls. Ensure we have your up-to-date mobile number so we can contact you if we spot unusual or suspicious activity on your account.
- If your phone is lost or stolen, call us straight away so we can disable your mobile banking apps as a precaution. For QIIB Mobile Banking call 00974 44840000
-

Card fraud

Protect yourself from credit and debit card fraud by taking a few easy steps to help keep your cards safe from fraudsters. If you think, you have fallen victim to card fraud.

Take care with your cards:

- Sign new bank cards as soon as you get them and keep them in a safe place
- Never let someone take your card away to process a transaction
- Never hand your card over to anyone that comes to your door

- Check your card expiry dates and call us if a new card hasn't arrived when it should
- If you live in a property where other people have access to your mail, it may be better to collect new cards from your local branch
- Report any lost or stolen cards immediately

Protect your PIN:

- Don't use personal details or combinations that are easy to guess when choosing your PIN
- Never reveal your PIN to anyone, not even the bank or the Police
- Never enter your card PIN into the telephone
- Always cover your PIN to prevent anyone from seeing it
- Change your PIN immediately if you suspect someone else may know it

At the cash machine:

- If anything about the cash machine looks suspicious don't use it. Tell a member of staff or the police
- Never put yourself at risk by attempting to remove any suspect devices from a cash machine
- Avoid using a cash machine if suspicious looking individuals are hanging around
- Don't let anyone distract you during your transaction, even if they seem to be 'helpful'
- Contact us straight away if your card is unexpectedly retained by a cash machine

Shopping online:

- Use a computer, laptop or mobile device that's protected with up-to-date security software
- Know who you're buying from before giving your card details online or over the phone
- Register for Verified by Visa and/or MasterCard Secure Code
- Only enter your card details on secure sites - check the web address begins with 'https' and that there's an unbroken padlock symbol in the browser address bar
- Avoid entering your card details on shared or public computers
- Always log out after shopping and save the confirmation email as a record of your purchase

Travelling abroad:

- Take a note of our 24-hour emergency number if you're calling from outside 00974 44840000
- If your cards are registered with a card protection agency, remember to take their number too
- Take another card or alternative payment method with you so that you are not reliant on one card
- Check the information on the sales voucher before you sign or enter your PIN
- Keep a copy of your sales receipts and check your statement carefully when you get back

Reporting fraud to us and the next steps...

Once you've reported any fraud to us, we'll refund your account straightaway in most cases, provided you've not acted fraudulently or without reasonable care (for example, you haven't kept your PIN written down with your card or disclosed it to someone else).

We'll send you a form to confirm the transactions that you say were fraudulent. You'll need to sign the form and return it to us so we can investigate. If we don't receive the form within 28 days, we'll assume you're not proceeding with your claim and any refund we've already given will be taken back out of your account.

We'll also send you a new card, which you should receive within 2 working days. If you need your card straightaway, we also offer a debit card replacement in selected branches. Opening hours and address details can be found using our branch finder (Link opens in a new window). It may take up to 5 working days if both your card and PIN need replacing and unfortunately we can't issue replacement PINs in branch.

Need help with fraud or security?

Contact us about fraud

00974 –44840000 (Call Centre)

00974 - 44840005 (Hot Line)

Police

If your debit card, credit card or cheque-book has been stolen, report it to your local police station. However, the police will only accept reports of fraud from banks

Lost or stolen debit or credit card

We understand that sinking feeling you get when your card's lost or stolen, so we try to make reporting, cancelling and replacing your card as stress-free as possible.

The quickest way to report your card lost or stolen, from wherever you are, is through the QIIB call

Fraud team and telephone number checker

QIIB numbers

00974 –44840000 (Call Centre)

00974 - 44840005 (Hot Line)

The Fraud team
if we ever see any unusual activity on your account, we will contact you. We, call you using one of our Fraud Team will be in touch.

Check a telephone number
Use our telephone number checker to ensure the number you've been given is a genuine QIIB Fraud Department number.