



Protecting you, your wealth and your data

At Rothschild & Co, protecting your data and wealth is our highest priority. With the rise in sophisticated cybercrime and fraud, here are some simple ways to help you stay protected.

One thing to remember

Fraudsters win by surprise and speed. They often call pretending to be your bank, the police or a company you trust, and create panic so that you act before you think.

So every time:

STOP — it's fine to pause.

CHALLENGE — could this be fake? Hang up and check.

PROTECT — contact us on a number you trust.

Rothschild & Co will never ask you to move money to a “safe” account, share a passcode, or grant remote access to your devices. If anyone does — **it's a scam.**



Essential Tips

Beware of Fraudulent Requests

Rothschild & Co will never send you a code to reverse or stop a transaction. We will also never ask you to move your money to a 'safe' account.

Monitor Your Transactions

Regularly review transactions on your bank accounts. You can do this at any time, anywhere with Mobile and Internet Banking.

Protect Your Personal Information

Be cautious of requests from unfamiliar parties asking for copies of your identity documents, proof of address, or any other personal information.

Limit Sharing on Social Media

Don't post personal or sensitive information — criminals use it to profile you and steal your identity.

Stay Alert to Urgent Requests

Fraudsters often claim urgent action is required, such as your account being closed or your money lost if you don't act immediately.



Online Tips

Use strong passwords and keep logins confidential

Choose a unique passphrase or a string of unrelated words. Keep your email password completely different from others, as email can be used to reset your other accounts. Never write down or share your banking login details.

Criminals increasingly impersonate banks, fraud departments and other trusted organisations in an attempt to obtain your online banking credentials.

Remember:

- Rothschild & Co will never ask for your online banking password or full security credentials.
- We will never ask you to disclose a One Time Passcode (OTP) by telephone, email or text message.
- We will never ask you to approve a Mobile Banking authentication request that you did not initiate yourself.
- If anyone contacts you unexpectedly and asks for banking login details, passcodes or authentication approvals, end the conversation and contact us using trusted contact details.
- Treat your banking credentials in the same way you would treat the keys to your home - never share them with anyone.

Enable Two-Factor Authentication (2FA)

Where possible, secure your online accounts — including email — with 2FA.

Avoid Remote Access Software

Never download software that gives a third party remote access to your computer or devices.

Use Secure Networks

Avoid unsecured Wi-Fi and never log in to Internet Banking on public computers.

Be Cautious with Emails

Don't respond to unsolicited emails and avoid clicking unknown links or opening attachments.

Keep Software Updated

Keep your devices on the latest operating system and update your anti-virus/malware protection as recommended by your provider.



Payment Card Tips

Safeguard Your Bank Cards

Keep cards in a secure place and never share your card number or PIN. Never let anyone take your card away to process a transaction.

Protect Your Online Transactions

Rothschild & Co uses Verified by Visa. **Never share your One Time Passcode (OTP) with anyone**, even if they claim to be from “your bank” or “the fraud team” — **we will never ask for it**. When paying with your card online, we recommend using the temporary ‘security code’ (CVV) that is available in the ‘card details’ > ‘show more card details’ section of our CardAssist app.

We also recommend selecting the option to authenticate online purchases using the CardAssist app instead of receiving a One Time Passcode (OTP) via text.

Block a lost or compromised card.

Debit and charge cards can be blocked via the CardAssist mobile app or by calling +44 1481 705000 (available 24/7).



Beware of SIM Swap Fraud

SIM-swap fraud occurs when a criminal convinces a mobile phone provider to transfer your mobile number to a replacement SIM card under their control.

Warning signs may include:

- Your mobile phone suddenly loses signal or stops receiving calls and text messages.
- Your handset displays messages indicating that the SIM card is invalid or inactive.
- You receive notifications about changes to your mobile account that you did not request.

If this happens:

1. Contact your mobile network provider immediately.
2. Contact Rothschild & Co as soon as possible.
3. Monitor your accounts and cards for any unusual activity.

Fraudsters who take control of a mobile number may attempt to intercept authentication codes or telephone calls intended for you.

If something feels off

If you're unsure about any contact, online or by phone:

1. Remain **calm**.
2. **Take your time** over any question or request you're unsure of.
3. If a message asks you to contact us, use our **published** phone number or email address, or speak to your designated Account Executive directly.
4. **Call us back on a number you already know.** If a call leaves you in any doubt, hang up and call us back using the number on the back of your card, on your statement or on our website www.rothschildandco.com/privatebanking — never a number the caller gives you.
5. **Ask us to confirm correspondence securely.** You can ask us to send you a secure message through Mobile or Internet Banking to validate that a request or communication from us is genuine. If you do not have Mobile or Internet Banking which can help you monitor transactions 24/7 as well as allow you to send and receive secure messages to us during business hours, please contact your Account Executive to learn more.

Recognise these common scams

These are common everyday “scripts” criminals use. If a call, text or email sounds like the left-hand column, treat it as fraud.

What the fraudster says	Why it's a scam
<i>“We’ve spotted fraud — move your money to a safe account now.”</i>	<i>We will never ask you to move your money to a “safe” account.</i>
<i>“Read me the one-time passcode (OTP) we’ve just sent you.”</i>	<i>These codes are the key to your money. Never share them with anyone — we will never ask you to provide any passcodes.</i>
<i>“Your card is compromised. What’s your card number, secure 3 digit number (CW) or PIN?”</i>	<i>We will never ask you for any of the details printed on your card.,</i>
<i>“Click this link to unblock your payment.”</i>	<i>We will never ask you to click a link to release a payment you have made.</i>
<i>“Install this application/software so we can remove a virus or secure your banking.”</i>	<i>We will never ask you to install remote-access software.</i>
<i>“Here are the updated account details for your transfer.” (before you make a large payment)</i>	<i>Payees will not advise you that banking details have changed at the last minute, or by telephone. Always confirm payment details with your payees via a communication channel you trust.</i>
<i>“To verify your account, please provide your online banking password, passcode or authentication code”</i>	<i>We will never ask for your online banking password, full credentials, or authentication codes.</i>

If you have any questions, please contact:

Rothschild & Co Bank International Limited
St Julian's Court, St Peter Port, Guernsey GY1 3BP
Tel +44 1481 713713
banking.services@rothschildandco.com
rothschildandco.com

Registered number 1088 Guernsey. Registered office as shown.
*Licensed and regulated by the Guernsey Financial Services Commission for the provision of
Banking, Investment and Credit services.*