Rothschild & Co

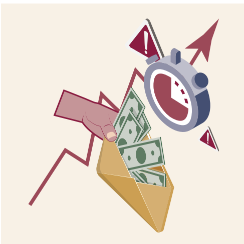
Protecting your wealth in the digital age

Your cybersecurity guide

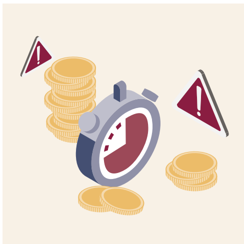
Detecting fraud

In today's digital world, the convenience of online banking and financial management comes with new and evolving risks. As a valued client, your trust and security are of utmost importance. While we invest heavily in a safe cybersecurity infrastructure, true protection is a shared responsibility.

Modern scams range from cleverly disguised online attacks to traditional fraud tactics powered by new technologies. To stay safe, it is essential to understand how these schemes operate. Most follow a familiar pattern:



A tempting opportunity



A request for urgent payment or action

A costly loss or betrayal

Whether it's a fake investment, a deceptive phone call, or a case of identity theft, recognising these red flags early can make all the difference.

This brochure is designed to empower you with essential knowledge and practical tips to help safeguard your digital identity and financial assets. From recognising common fraud tactics to adopting simple yet powerful cybersecurity habits, our goal is to help you stay one step ahead of cyber threats.

Best practices for personal digital security

Use strong, unique passwords for each service

Creating different passwords for each online account such as eBanking, email, and social media helps protect your data in case one service is compromised. A password manager can simplify this by securely generating and storing complex passwords for you.

Enable two factor authentication (2FA)

Adding two factor authentication to your accounts provides an extra layer of security. It requires a second form of verification like a code sent to your phone, making it much harder for unauthorised users to gain access, especially for banking and email.

Keep your devices and apps up to date

Installing updates regularly ensures your devices and applications have the latest security patches. These updates fix vulnerabilities that hackers could exploit, making them a crucial part of your digital defence.

Monitor your account activity and report anomalies

Regularly checking your account activity helps you spot suspicious behaviour early. If you notice anything unusual, report it immediately to prevent further issues and secure your data.

Verify the source of messages before acting

Phishing attempts often look like legitimate emails, texts, or calls. Always confirm the sender's identity before clicking links or sharing personal details, especially if the message seems urgent or unexpected.

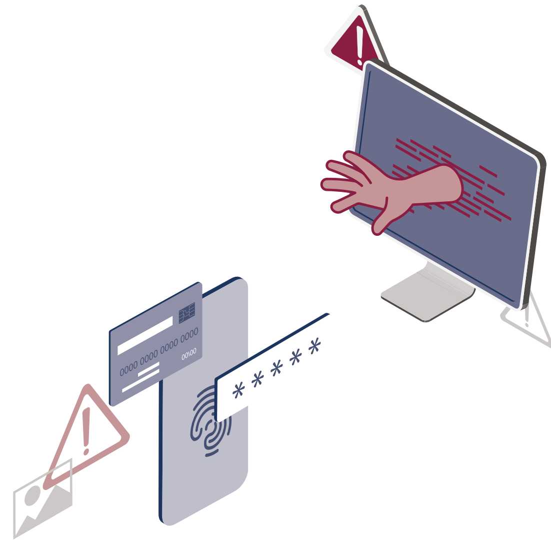
Contact your bank through official channels

If something feels suspicious or urgent, reach out to us directly via our official website or your Client Adviser. Avoid using contact details provided in unsolicited messages as they may be part of a scam.

Common cyber fraud scenarios

Realistic examples show how fraudsters operate and how you can stop them in time.

Phishing attacks



Scenario:

You receive an email that, at first glance, appears to be from us or another trusted institution, asking you to click a link or open an attachment.

What attackers are after:

- Gaining access to your personal data and systems
- Selling your information or demanding a ransom

How to stay safe:

DON'T click on suspicious links. Always log in to eBanking by typing the website address manually.

DO verify the sender and contact us through official channels if unsure.

Tip: We will never ask for sensitive information or your password via phone or email.

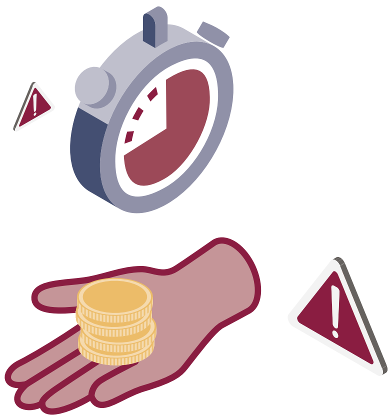
“Easy money” investment scams

Scenario:

You’re contacted via email or phone about a “guaranteed” investment opportunity with high returns. These offers often misuse the names or images of celebrities.

What attackers are after:

- Your ID documents and personal data
- Repeated payments under false pretences
- Using your identity for further fraudulent activities



How to stay safe:

DON’T share your personal documents or invest in unknown companies or individuals.

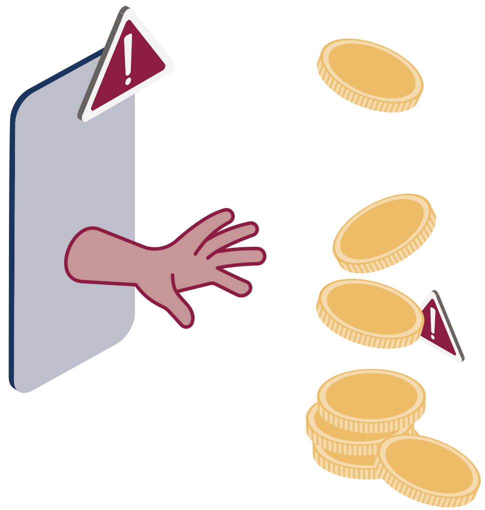
DO consult us before making any financial commitment.

Impersonating a family member

Scenario:

You receive a WhatsApp message from an unknown number pretending to be someone you know, for example:

“Hi Mom, this is my new number”



After a brief, friendly exchange, the conversation shifts to a request for urgent financial help.

In other cases, you might receive a phone call claiming a loved one has been in an accident or is in legal trouble. The caller may impersonate a police officer, lawyer, or hospital staff, urging you to act immediately.

What attackers are after:

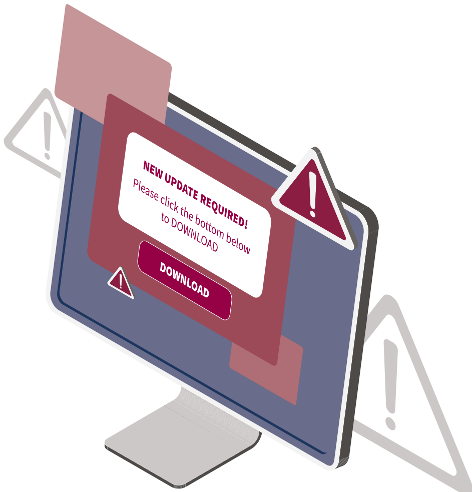
- Creating emotional distress to cloud your judgement
- Pressuring you into sending money quickly
- Gaining access to your banking details

How to stay safe:

DON’T send money or share banking data under pressure.

DO call your family member using a known number before taking action.

IT support scam



Scenario:

A pop-up appears on your screen warning of a technical error that has occurred, urging you to call a displayed support number. The fraudsters pretend to be support staff and ask you to install software to fix the issue.

What attackers are after:

- Installing malware to steal your data or control your device
- Selling fake support services

How to stay safe:

DON'T give remote access to your device.

DO close the window and contact your IT provider or us directly to obtain trustworthy advice.

Staying safe also means knowing what not to do.

Avoid these common traps:

Never share your eBanking credentials, passwords, or PINs with anyone. We will never request your banking credentials.

Don't click on links from unknown or unexpected senders – especially those claiming urgency or offering rewards.

Never install software or grant remote access to your device unless you are certain of the source.

Avoid public Wi-Fi for sensitive transactions like online banking or payments.

Don't act under pressure. Scammers often create a false sense of urgency – pause and verify before responding.

Don't make payments to unknown recipients or based solely on digital communication.

How we safeguard your digital experience

We understand that digital security is a key concern in today's connected world and protecting your personal and financial data is a top priority.

While no system can guarantee absolute protection, we apply a range of measures and processes aimed at identifying and addressing potential risks. These include continuous monitoring, promoting safe usage practices and adhering to industry best practices.

Security is a shared responsibility, and your vigilance plays a key role in protecting your financial well-being. We remain committed to helping you navigate this evolving landscape with confidence and care.

Something doesn't feel right?

Immediate action

If you suspect fraud or something doesn't feel right, contact your Client Adviser without delay. In urgent situations, you can also call the police directly.

Ongoing protection

Whenever you encounter a suspicious situation, keep any relevant evidence such as emails, screenshots, or messages, and avoid engaging further with the suspected fraudster.

Refrain from clicking additional links, replying to messages, or providing any personal details.

Rothschild & Co Bank AG