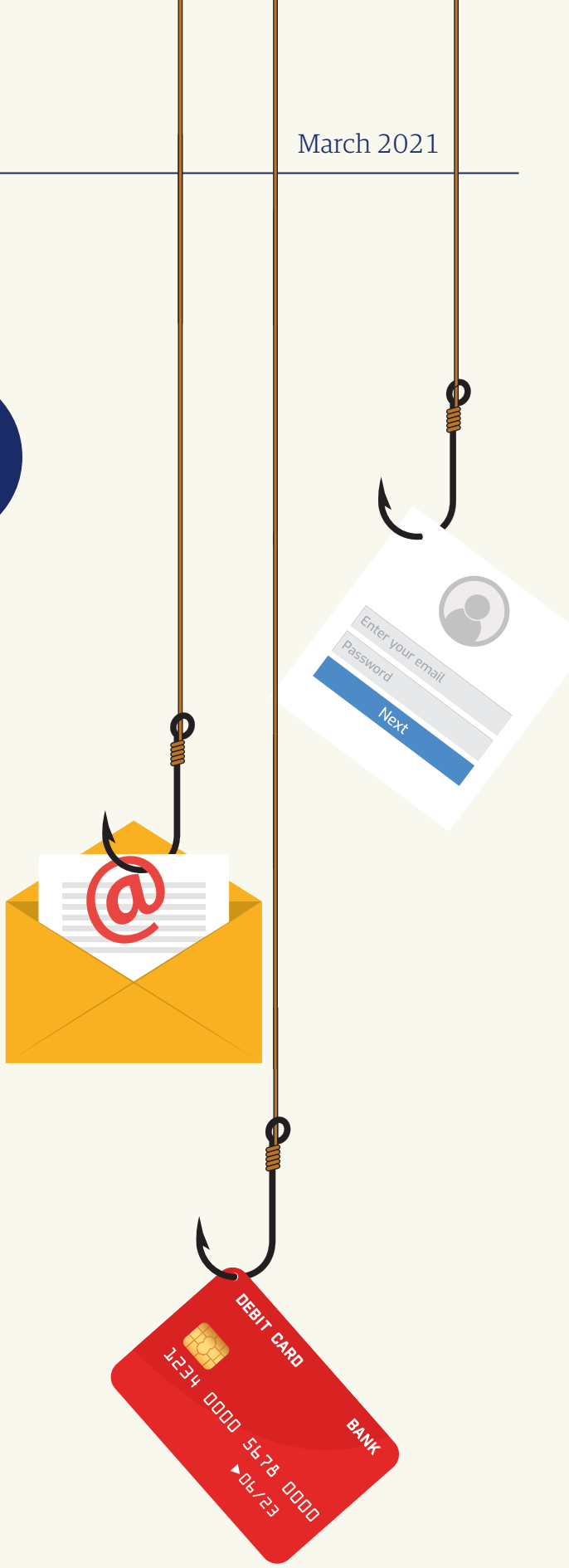
Talking*Points*

March 2021

Keeping you safe

Scammers stole £479 million from almost 150,000 victims in 2020. The problem of financial fraud is worsening, and in particular the issue of fraudsters impersonating organisations like banks, investment managers and HMRC. How can you protect yourself?



The ongoing financial impact of coronavirus has made people more susceptible than ever to impersonation scams, according to Action Fraud, the UK's national reporting centre for fraud and cybercrime.

Last year savers lost £78 million – on average £45,242 for each victim – from 'clone' attacks alone, after transferring their savings to criminals they thought were genuine investment professionals.

Don't be hooked in

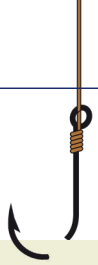
The fraudsters create 'clone firms', using the names, addresses and 'firm reference numbers' of real companies authorised by the industry regulator, the Financial Conduct Authority (FCA). They then take out adverts on social media and search engines. Victims who click on the adverts are taken to exact replicas of genuine websites.

In some cases the fraudsters are so sophisticated that they can clone a website domain name; more often it is very similar. Once victims register interest, the fraudsters contact them – by phone, email and even sometimes face-to-face – often using the names of genuine employees. They create seemingly legitimate company email addresses but with subtle changes. For instance, a fraudster using *rathlbones.com* has recently been impersonating our business, recommending a fixed income product that requires an initial deposit. **Be alert to emails that do not come from rathbones.com.**

Rising threat

Impersonation crimes extend far beyond cloning and the number of impersonation scams nearly doubled last year, according to figures from UK Finance, with losses of over £150 million. In particular, the fraudsters have been exploiting people's concern about fraud to steal money. They call pretending to be from a person's bank, wealth manager or the police, and say they have identified fraudulent activity on the person's account. The fraudsters can copy a bank's telephone number and will claim that the person needs to move the money

Rathbones
Look forward



"The number of impersonation scams nearly doubled last year according to figures from UK Finance, with losses of over £150 million."

to a safe account – one that happens to be in their control. Sometimes, victims can be persuaded to transfer to other 'investments' offering better returns.

The money is moved in seconds. The damage, which is financial, psychological and emotional, can last for years.

Remember, organisations like your bank or the police will never ask you to transfer money to a safe account, even if they say it is in your name. Do not send personal information by email. Your bank will never ask you to share your PIN or account details, like user ID or passwords.

Other scams

Here are some of the other most common scams to watch out for.

– Emails from public bodies

Criminals send fake emails designed to look like they are from government departments. They offer council tax reductions, relief funds or grants and contain links and forms to steal or solicit personal and financial information from victims. Other organisations targeted with similar schemes include the NHS, the Royal Mail and HMRC.

Scams that target bereaved families are particularly cruel. The fraudsters, posing as debt collectors or inheritance distributors, demand repayment of alleged debt incurred by the deceased or ask for payment to release inheritance.

– Pension scams

Fraudsters offer victims fake services such as free pension reviews, pension loans or cash up front. If scammers do not steal money outright, they may hide high fees within a complicated structure.

– Fake anti-virus software

Online users can be confronted by pop-up windows that allege viruses are infecting their machines. Directions to click a button or a link to remove a virus simply downloads malware that steals personal data, or ransomware, which can lock up a computer until payment is made to regain access.

Look out for cold calls and emails from individuals purporting to work for software companies and claiming to have identified a fault with your computer. If you receive an email containing links, hover your mouse over them (without clicking). Does the address match what you would expect for the company supposedly sending the email? **Never give anyone remote access to your computer as a result of a cold call or unsolicited message.**

– Romance scams

Another particularly cruel scam is the luring of lonely individuals into thinking they have developed a relationship with someone online. Once their confidence has been gained, the fraudsters ask for money, or bank details, and ultimately disappear with the victim's cash.

How to report scams

If you suspect a scam, report it to Action Fraud by calling 0300 123 2040. Alternatively, visit its website to use the online reporting tool.

You should contact your investment manager directly or email our fraud specialists at riskfunction@rathbones.com if you are approached by someone purporting to be from Rathbones and have any concerns.

Remember, you will only ever be contacted by your dedicated investment team from Rathbones. You will not be cold called, and if you are contacted by another member of the business you should not give out any personal details. Stay safe!

If you are at all suspicious, hang up. Contact your bank or the organisation you think may be being imitated on a number you know to be correct, such as the one on the back of your bank card. You can contact your local police force via the 101 service. Contact your bank straight away if you think you may have fallen victim to an impersonation scam.

Ways to stay safe

– Check the 'Keeping you safe' page on the Rathbones website and the FCA's ScamSmart website, which both provide more guidance on how to spot scams and stay safe online. Follow the advice on the Take Five to Stop Fraud website, a national anti-fraud campaign.

– **Stop, Challenge, Protect!** Before parting with your money or information, take a moment to **Stop** and think; **Challenge** whether it could be a fraudulent, scammers will try to rush or panic you. **Protect** yourself by contacting your bank immediately if you think you have fallen for a scam, and report it to Action Fraud.

– Check the FCA register for a list of authorised firms and only use the telephone and email address on the register – register.fca.org.uk.

– Double-check the URL and contact details of any firm that contacts you.

– Do not rush or make decisions based on time pressure. If an email conveys a tone of urgency, this is often a warning sign.

– Reject unexpected pension or investment offers, consult your financial adviser or look to the Pensions Advisory Service for guidance.

– Keep verified antivirus software up to date on your computer and never let a cold caller or someone sending an unsolicited message have remote access to your computer.

Image: iStock

Rathbones
Look forward

Rathbones
Look forward

For thought-provoking articles and helpful ideas, follow us on social media or visit rathbones.com/knowledge-and-insight

Connect with Rathbones

@Rathbones1742

Rathbone Brothers Plc

Rathbone Brothers Plc

Important information

Rathbones, Rathbone Unitised Portfolio Service and Rathbone Greenbank Investments are trading names of Rathbone Investment Management Limited, which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registered office: Port of Liverpool Building, Pier Head, Liverpool L3 1NW. Registered in England No. 01448919. Financial planning advice is provided by Rathbone Financial Planning (RFP) which is a part of Rathbone Investment Management Ltd.

Rathbone Unit Trust Management Limited is authorised and regulated by the Financial Conduct Authority and is a member of the Investment Association. Registered office: 8 Finsbury Circus, London EC2M 7AZ. Registered in England No. 02376568.

Provision of trust, tax and company administration services are provided by Rathbone Trust Company Limited (RTC). Provision of legal services is provided by Rathbone Trust Legal Services Limited (RTLS), a wholly owned subsidiary of RTC. RTLS is authorised and regulated by the Solicitors Regulation Authority.

RTC and RTLS are registered in England under company numbers 01688454 and 10514352 respectively. It should be noted that any services provided by Rathbone Trust Company are not regulated by either the Financial Conduct Authority nor the Prudential Regulation Authority.

The above companies are wholly owned subsidiaries of Rathbone Brothers Plc. Head office: 8 Finsbury Circus, London EC2M 7AZ.

Rathbone Brothers Plc is independently owned, is the sole shareholder in each of its subsidiary businesses and is listed on the London Stock Exchange. 'Independent' and 'independence' refer to the basis of Rathbones' ownership as a corporate entity, and not to our use of non-life packaged products for clients of our advisory or non-discretionary investment management.

Rathbone Investment Management International is the Registered Business Name of Rathbone Investment Management International Limited which is regulated by the Jersey Financial Services Commission. Registered office: 26 Esplanade, St. Helier, Jersey JE1 2RB. Company Registration No. 50503. Rathbone Investment Management International Limited is not authorised or regulated by the Prudential Regulation Authority or the Financial Conduct Authority in the UK. Rathbone Investment Management International Limited is not subject to the provisions of the UK Financial Services and Markets Act 2000 and the Financial Services Act 2012; and, investors entering into investment agreements with Rathbone Investment Management International Limited will not have the protections afforded by those Acts or the rules and regulations made under them, including the UK Financial Services Compensation Scheme.