Email hacking: the risk to advice firms

Two case studies

As managing our business and personal lives moves ever more online, criminals are also increasingly using the internet to commit fraud. Email is a favoured channel for fraudsters. Email hacking – the taking over of someone's email account without their knowledge – is becoming much more prevalent and is now a common feature of financial fraud. The trend towards home working – and the resulting use of insecure email – increases the risk of fraud even further.

To highlight how criminals can operate, we have detailed two case studies. These are fictitious accounts but closely resemble actual fraud cases seen across the industry. All the firms and product providers quoted are also fictional.

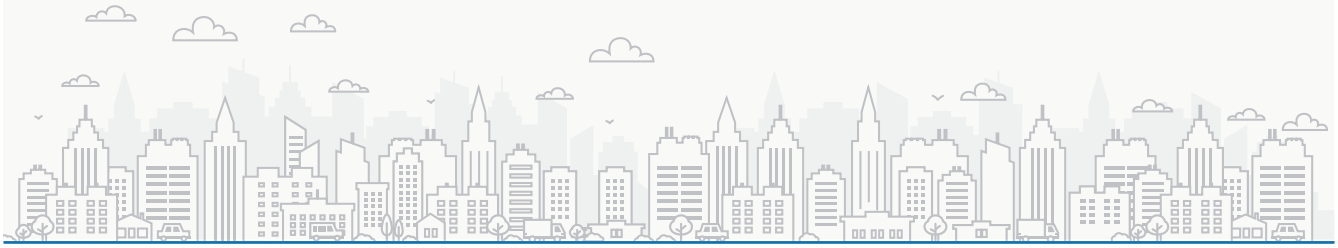
Did you know...

Criminals successfully stole £1.2 billion through fraud and scams in the UK in 2022.

UK Finance Annual Fraud Report 2023.

There were 277,000 cases of identity fraud reported in 2022 – with the over 60s an increasingly targeted age group.

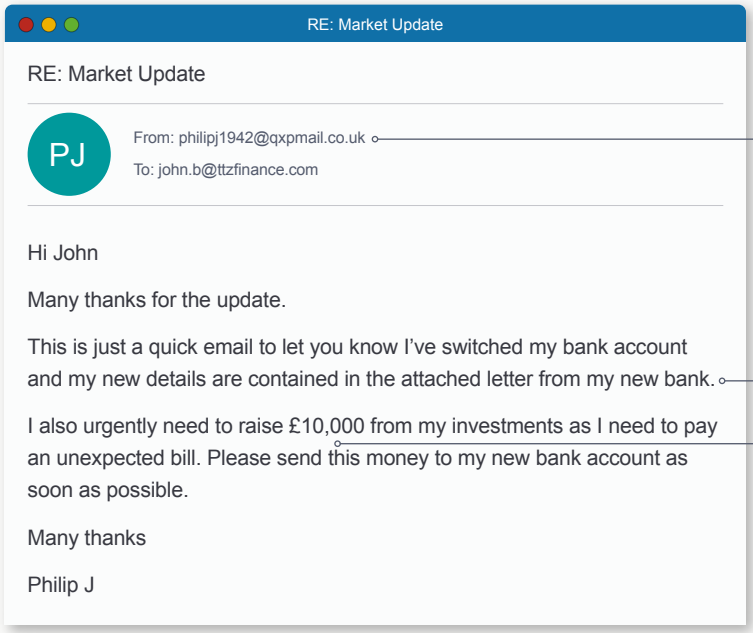
Cifas Fraudscape 2023 report.



Multiple fraud totalling £35,000

Mr Phillip J is a client of TTZ Finance Ltd. and has a substantial portfolio of mutual funds within ISAs and non-tax wrapped accounts. He normally meets his adviser (John B) once a year for an annual review and they generally talk once or twice a year by phone. Occasionally they communicate through unsecured email.

1. Unbeknown by Mr J, a fraudster has taken control of his email account. The criminal spots that Mr J recently received an email from his adviser.
2. The fraudster replies to this email, posing as Mr J.



Points to watch out for

The email address matches the one TTZ Finance Ltd. has on record for Mr J. It appears to be a genuine email, especially as it is a reply to a service email from the firm themselves. They are unaware that a fraudster is controlling the email account.

The attachment is a fake letter purportedly from the bank. The forgery is of a high standard.

The amount of the fraud is relatively modest – fraudsters often keep the initial sum relatively low to avoid arousing suspicion. The request is normally urgent.

3. The fraudster deletes the email from Mr J's sent box so that there is no record of the communication should Mr J review his sent mail. The fraudster continues to monitor Mr J's email account and may even set up mailbox rules so that any emails from the adviser automatically go into a hidden folder that Mr J himself will not see.
4. The adviser believes that the email is genuine and does not have a callback process for high risk instructions. They update the client's bank account with the product provider and place the sale instruction online.
5. The adviser sends a reply to Mr J stating that he has updated his bank account details and put through the withdrawal request. The fraudster intercepts the email and deletes it so that it is not seen by Mr J.
6. The product provider releases the £10,000 sale proceeds, paying the money into the bank account controlled by the fraudster.
7. The fraudster quickly moves the £10,000 from the false bank account to another account he controls.
8. After a successful fraud, it is common for a criminal to make a second fraud attempt on the same account. The amount of the second withdrawal will typically be higher than the first. In this case a further £25,000 was taken, resulting in a total of £35,000 stolen from the account.

While this is a fictitious scenario, advice firms in similar situations have been held responsible for this type of fraud and have been required to refund the sums involved to the client or product provider. They have been deemed at fault because, among other factors, all communications between the advice firm and the client were through unsecured email. No attempt was made to double check the instructions with the client through another established form of communication such as a telephone call made to a trusted number.

There were over 37,000 instances of facility takeover fraud in 2022. Criminals focused their efforts on gaining access to existing accounts.

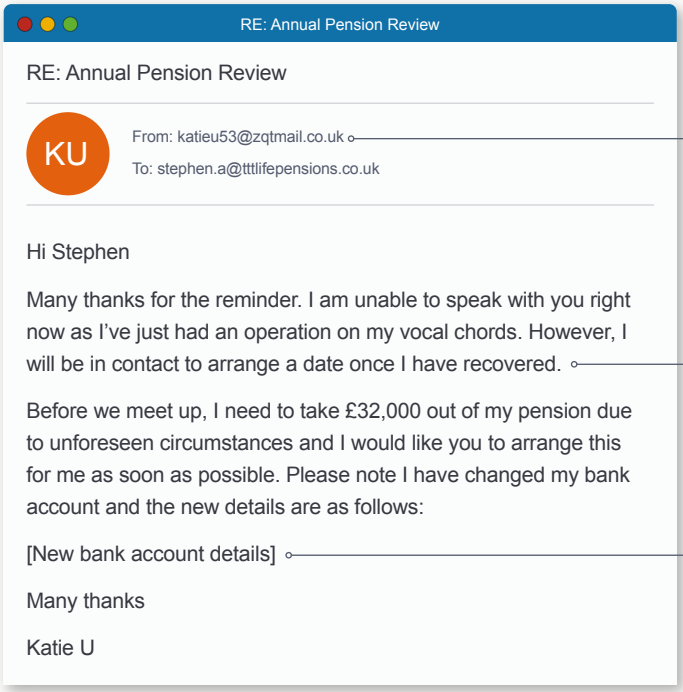
Cifas Fraudscape 2023 Report

Attempted fraud from a pension account...

...and how taking some simple steps prevented it

Mrs Katie U is a client of TTT Life & Pensions and has a drawdown portfolio from which she takes an income. She normally meets her adviser (Stephen A) once a year to review the portfolio and her withdrawals. They communicate through unsecured email from time to time.

1. Unbeknown by Mrs U, a fraudster has taken control of her email account. The criminal spots that she recently received an email from her adviser concerning her annual review.
2. The fraudster replies to this email, posing as Mrs U.



Points to watch out for

The email address matches the one TTT Life & Pensions has on record for Mrs U. It appears to be a genuine email, especially as it is in reply to an email concerning her annual review. The firm are unaware that a fraudster is controlling the email account.

The fraudster mentions that she ('Mrs U') cannot speak at the moment. This is a common tactic used by fraudsters. They want to:

- Give a reason why the client is emailing rather than calling the firm
- Discourage any follow up call from the adviser

A bank account controlled by the fraudster.

3. The fraudster deletes the email from Mrs U's sent box (so that there is no record of the communication). The fraudster continues to monitor Mrs U's email account.
4. Even though the client mentioned that she is unable to speak, the adviser regards the change of bank account details and surrounding circumstances as suspicious and therefore decides to call Mrs U (using a longstanding, trusted telephone number) to confirm the request.
5. Mrs U categorically denies the request. Realising that someone has gained access to her inbox, she immediately changes her email account login details including using an alternative, robust password.
6. The adviser ensures that all the staff at his firm are aware of the incident and that everyone is fully briefed on the risks of email account compromise and how it can enable fraud.

For more information on how to protect your business, visit our Technical matters hub

How we protect you and your clients

We understand the importance of keeping your firm's and your clients' information safe and secure. We use proven, industry-recognised security tools and processes to protect against fraud and security breaches and we regularly upgrade this protection in response to advances in security threats.

Fidelity is a member of Cifas, the UK's fraud prevention agency, which works closely with law enforcement partners. Cifas Protective Registration is a fraud protection scheme that helps us protect your clients should they be at risk of fraud.

If you have any concerns about security, please call us as soon as possible on 0800 358 7717.

More advice from the National Cyber Security Centre can be found on ncsc.gov.uk

Adviser Solutions

Fidelity INTERNATIONAL

UKM0823/LM 1471084/QC/0824