Capita Cyber incident Q&A

What happened?

Capita Pension Solutions Ltd, part of Capita plc, ("Capita") recently reported a cyber incident confirming that they had been targeted by professional hackers potentially impacting a number of their servers. The incident occurred because of a targeted phishing email, which is an email intended to trick individuals into clicking a link or opening an attachment, and is designed to steal money, credentials, or other sensitive information.

Capita provides outsourcing services for many different sectors of industry and public bodies.

Their technology platforms provide many pension schemes with administration services such as payroll services for pensions in payment.

The Trustee has worked closely with Capita to understand how the incident occurred, what actions they have taken to secure the personal data they hold, and how they will mitigate any increased risks of financial fraud and or identity theft that could occur because of this cyber incident.

Capita has regrettably told us that details of the William Hill Pension Scheme were accessed by the hackers. The information for those members impacted may contain some or all of the following:

- Title;
- Initial(s);
- Name;
- Date of Birth,
- National Insurance Number,
- Member ID Number,
- Tax Code,
- Tax Paid (along with any other deductions),
- Date the pension ceased, or
- Date of Retirement.

Capita are writing to those members whose data may have been compromised.

Capita has confirmed that impacted members will be given access to an online monitoring tool provided by Experian, a leading identity protection service, free of charge for a period of 12 months from activation. Those members directly impacted will receive a further letter which will include details of the service being provided by Experian, along with telephone support providing access to experts who can answer any concerns about identity theft and fraud.

We strongly encourage you to wait for these contact details if you are impacted as the service is designed to provide you with any assistance you may need.

When did it happen?

Capita detected the cyber incident on 31 March 2023 and took immediate steps to isolate and contain the issue. Since then, it has undertaken a complex forensic investigation with support from technical experts and specialist advisers. This has involved reviewing files across Capita's entire business.

What member data has been taken?

The full extent of the data breach is still to be confirmed; however, we understand that copies of data generated by Capita's administration platforms were taken from files held on a local server. A list of the data items that Capita has confirmed as exposed is provided above.

When was the Trustee first made aware that pension scheme member data had been impacted?

We received notifications from Capita on Wednesday 18th May that some of our members' data may have been compromised although it has taken longer for Capita to confirm which members.

Does my Pension remain safe?

Yes, only personal data was accessed in this incident, assets of the scheme have not been compromised.

Will I still receive my pension?

All pension payments have and will continue to be paid on time.

Does this impact all members?

No. The majority of members affected were those who were receiving their pension as at 31 March 2023 or whose pension had ceased in the three years prior to this date.

A pension may have ceased because the member died, the member took all their pension benefits as cash or the pension was being paid to a dependant.

Have you contacted all affected members?

All members who have been affected have been written to. This letter highlights the potential risks and the steps they can take to protect their personal data including access to a service that will help members monitor use of their personal data.

Is Capita certain that the personal data found on the files has been accessed?

Capita cannot be certain that the personal data has been accessed. Capita has publicly stated that it "has taken extensive steps to recover and secure the customer, supplier and colleague data contained within the impacted server estate, and to remediate any issues arising from the incident." You can read the full statement here - https://www.capita.com/news/update-actions-taken-resolve-cyber-incident

What advice can you give to members who are concerned?

Whether you've been impacted by this incident or not, in a data-driven world, we always recommend that members take steps to protect their personal data and avoid scams.

The National Cyber Security Centre website provides guidance that may be useful www.cyberaware.gov.uk.. We've also shared some information on the Pension Scams page and below are some simple steps on how to protect yourself.

Has the Trustee informed the Information Commissioner's Office (ICO) and The Pensions Regulator (TPR)?

Yes, we have reported this to ICO and TPR. We will work them on any investigation they may choose to conduct and any recommendations they might subsequently make.

How is the Trustee managing the incident?

We continue to engage with Capita in respect of their ongoing investigations and the details of the ongoing support they will be providing to those impacted.

As detailed earlier, members will be given access to a leading identity protection service, Experian, free of charge. We are coordinating with Capita regarding this and a letter will have been issued to those impacted.

What advice and guidance can you give me to help protect myself from potentially identify theft or fraud?

We encourage all members to be particularly vigilant if you receive any unexpected emails, telephone calls, texts, or letters.

Please be careful you do not share any personal or financial information when responding to emails or telephone calls and check your bank, building society and credit card accounts regularly for any unusual payments that you do not recognise.

Cyber criminals commonly use a scam technique called *phishing*, which is mostly email-based, to lure victims under false pretences to websites which look legitimate to get them to provide personal information including bank account and credit card details. These emails appear to be from recognisable sources such as banks but actually link to fraudulent websites.

So:

- Protect your email with a strong password (tip: use three random words to create a single password that is difficult to crack).
- Do not share your password with anyone.
- Turn on 2-step verification (2SV) on your email account.
- Install the latest security updates to your browser software and personal computing devices.
- If in doubt, do not open emails.
- Check that any links look correct before you click on them.
- Be suspicious of anyone who asks for your bank account or credit card details.
- If the email contains spelling mistakes, this can be a sign that this is a phishing scam. Do not open the email or attachments.

If you think you have been a victim of fraud you should report it to Action Fraud, the UK's national fraud and internet crime reporting centre, on 0300 123 2040.

If you receive a suspicious email, you should forward it to report@phishing.gov.uk. For text messages and telephone calls, forward the information to 7726 (free of charge). For items via post, contact the business concerned.

If there are any changes to your National Insurance information, HM Revenue & Customs would contact you – but you can also phone them on 0300 200 3500.

For more advice on how to stay secure online, please visit www.cyberaware.go.uk.

How can I check if one of my online accounts may have been compromised?

Services such as www.haveibeenpwned.com can tell you if your personal information or any of your account passwords have been made public in a major data breach. Help is also available from Experian, once you have access.