

# Capita Cyber Incident

## Questions and answers

You'll be aware that Capita provide the administration services for EAPF members pensions. On 31 March 2023, Capita detected malicious activity on their networks and we have set out below some questions you might have about what this means for our members.

### **1) How did the cyber incident occur?**

The cyber incident occurred at Capita plc and it impacted a small number of its computer servers. This included some used by Capita Pension Solutions, which is a business that provides pension administration services to members of the EAPF, along with several other major pension schemes.

The source of the cyber incident has been linked to a 'phishing' email which contained a malicious link that allowed attackers access to a small number of Capita's servers.

### **2) When did it happen?**

Capita detected malicious activity on 31 March 2023 and took immediate steps to isolate and contain the issue in order to keep member data safe from compromise.

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.

### **3) When were you first made aware that member data had been affected?**

We've been working closely with Capita since it first announced the cyber incident and have sought regular updates on the progress of its investigation. Once Capita had confirmed there was evidence that some personal data may have been accessed, we updated members on the EAPF public website. At this point, Capita were not able to confirm whether members' personal data had been affected.

We were formally informed of a personal data breach for a large group of members in the Scheme late in the afternoon on Friday 19 May and have been working swiftly to understand which members files were impacted. We're working as quickly as we can to review the data in order to write to all affected members.

#### **4) What personal data has been accessed in the incident?**

Regrettably, details of EAPF pensioner members (those in receipt of their pension) were held on the Capita servers accessed by the hackers. The information potentially accessed includes:

- Title, initial(s) and name
- National Insurance number
- Tax code
- Pension amount
- EAPF reference number
- Date of retirement
- In some cases, date of birth
- In some cases (approximately 13%) addresses

For a small amount of other members (approximately 2%), there was also some data containing;

- Title, initial(s) and name
- National Insurance number

Whilst Capita cannot currently confirm if this data was definitively “exfiltrated” (i.e. accessed and/or copied) by the hackers, they recommend we work on the assumption it was.

#### **5) Is my pension safe?**

We'd like to reassure all members that your pension remains secure. Hartlink, the database that holds all member pension records, was not impacted by this incident. The main advice we can provide is not to be alarmed, but to be vigilant given the circumstances.

We have set out some recommendations in question 10 below.

#### **6) Has this affected pension payments made to members?**

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

#### **7) Does this impact all members?**

No. The majority of members affected were those who were receiving their pension as at 31 March 2023. A smaller group of members who are not receiving their pension were also affected.

#### **8) Have you contacted all affected members?**

We will be writing to all members who have been affected by the incident once we've been able to confirm the details of the members whose information was on the affected server. We have also updated members internally and via the Fund's website confirming details of the incident.

The letter will highlight the potential risks and the steps the affected members can take to protect their personal data. We've also offered a service that will help members monitor the use of their personal data.

## 9) 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 at [www.capita.com/news/update-actions-taken-resolve-cyber-incident](http://www.capita.com/news/update-actions-taken-resolve-cyber-incident)

## 10) 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. We'd encourage all members to only ever give out personal information if you're absolutely sure you know who you're communicating with.

- **If you receive an email from the EAPF administration team**, please make sure the email is from a Capita email address (either @capita.com or @capita.co.uk).
- **If you receive an email from our Communications team**, please make sure the email is from [noreply@mail.eapf.org.uk](mailto:noreply@mail.eapf.org.uk)
- **If you receive an email directly from our EAPF Management team**, please make sure the email is from [@environment-agency.gov.uk](mailto:@environment-agency.gov.uk)
- **Do not click on any links included in emails** unless you know it is from a reliable source.
- **Do not provide any personal information** unless it is a request from the administration team that is in direct response to an enquiry from you.
- If you receive a suspicious email, you should forward it to [report@phishing.gov.uk](mailto: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.

If you're concerned someone might be impersonating EAPF, please let us know by emailing [info@eapf.org.uk](mailto:info@eapf.org.uk).

## 11) Is my pension account on the EAPF Portal safe?

Yes, the portal was not accessed and your login information remains safe.

## 12) What are your legal and regulatory obligations?

We are required to inform the Information Commissioners Office (ICO) and the Pensions Regulator (TPR). We have reported the impact to the Fund to both ICO and TPR and will work with them on any investigation they choose to conduct and any recommendations they may make.

### 13) Is there any guidance available from a regulatory perspective?

The National Cyber Security Centre and the Information Commissioner's Office (ICO) both provide guidance that may also be useful.

You can visit their websites using the below web addresses:

- [www.ncsc.gov.uk/guidance/data-breaches](http://www.ncsc.gov.uk/guidance/data-breaches)
- [ico.org.uk/for-the-public](http://ico.org.uk/for-the-public)

### 14) How will you make sure that this doesn't happen again?

In our discussions with Capita, we have sought information about what it has done to improve the security of personal data and avoid a future incident. Once the investigation has been finalised, we will receive a full report about the incident, how it was managed and what steps Capita has taken and will be taking to avoid this happening again.

### 15) What if I have other questions not covered here?

We have done our best to cover as many questions as possible. If you're an EAPF member and you're wondering if your personal data has been compromised, you will be contacted in writing to confirm if this is the case.

**Letters will be sent during the week commencing 29 May 23.**

**Please do not contact Capita to ask if you're affected.** If you do need to contact Capita, please do be patient with the team. The incident has had an impact on their 'business as usual' processing, and they're recovering from lost time as a result of the cyber incident.