Commonwealth War Graves Commission

Superannuation Scheme

20 mai 2024

Incident cybernétique – Données personnelles

Capita, les administrateurs du régime de pension, ont récemment annoncé avoir subi un «incident cybernétique» survenu à la suite d'un premier accès non autorisé aux données détenues par Capita.

À la suite des enquêtes de Capita, ceux-ci ont informé les fiduciaires du régime le 19 mai que les données personnelles que Capita traite en notre nom faisaient partie des données extraites à la suite de l'«incident cybernétique». Malheureusement, les données comprennent des données personnelles relatives aux membres du régime. Capita nous a informés que cette violation de données concernait les domaines suivants, tels que mis à jour:

- Nom
- Identification unique du membre
- Numéro d'assurance nationale
- Pension en cours de paiement
- Code des impôts
- Impôt payé et toute autre déduction, le cas échéant
- Date de naissance
- Date de la retraite
- Date de cessation de la pension
- Coordonnées bancaires
- Adresse

Cela signifie que pour certains membres, une partie ou la totalité de ces données peut avoir été extraite par les pirates. D'après ce que nous avons appris de Capita, l'examen indépendant a permis d'identifier qu'environ 10 autres membres ont été touchés et que des catégories de données supplémentaires ont été identifiées pour environ 370 des membres précédemment contactés. Pour être clair, cela ne signifie pas nécessairement que les données ont été identifiées comme exfiltrées, mais nous croyons qu'il est approprié d'agir comme s'il y avait une probabilité que ce soit le cas. Nous voulons être transparents avec vous sur les risques potentiels afin que vous puissiez déterminer si vous devez prendre des précautions.

Nous travaillons avec Capita pour identifier les membres touchés et les contacter afin qu'ils puissent prendre des mesures pour se protéger et minimiser l'impact potentiel de cet incident. Des lettres ont été envoyées aux membres concernés par Capita le lundi 5 juin.

Capita a informé le Bureau du commissaire à l'information (*Information Commissioner's Office* au Royaume-Uni ou «**ICO**») de l'incident cybernétique, et nous avons également fait un rapport séparé à l'ICO. Nous avons également informé la Commission du *Commonwealth War Graves* (la «**Commission**») et l'organisme de réglementation des pensions au Royaume-Uni.

À la suite des données qui ont été prises, nous considérons que cet incident présente un risque que les renseignements des membres puissent être utilisés pour des activités suspectes ou potentiellement criminelles. Il est possible que si l'information est consultée, elle puisse être utilisée pour la fraude, le vol d'identité ou pour envoyer des courriels malveillants, bien que Capita n'ait aucune preuve que les informations résultant de cet incident soient disponibles à la vente sur l'internet clandestin ou autrement. En effet, Capita a nommé un conseiller spécialisé tiers qui continue de surveiller l'internet clandestin pour confirmer que les données compromises à la suite de cet incident ne soient pas disponibles à la vente en ligne.

Nous sommes conscients que cela vous préoccupera. Nous nous en excusons et nous tenons à vous rassurer que nous prenons des mesures aux côtés de Capita pour essayer de minimiser l'effet de cet incident et de réduire la probabilité de préjudice. Dans ce cadre, les membres concernés ont eu accès gratuitement à un service de protection de l'identité de premier plan pendant 12 mois s'ils le souhaitent. Nous avons contacté les membres concernés pour leur expliquer comment cela fonctionnera et ce qu'ils doivent faire pour avoir accès au service.

Nous vous encourageons également à vous protéger autant que possible en consultant les conseils fournis sur les sites internet suivants et en apprenant les signes possibles de fraude d'identité, d'hameçonnage et d'autres cybercriminalités:

Le Centre national de cybersécurité - The National Cyber Security Centre - https://www.ncsc.gov.uk/

Commissariat à l'information - The Information Commissioner's Office - https://ico.org.uk/for-the-public/

Pour en savoir plus sur les escroqueries liées aux pensions et sur la façon de repérer une escroquerie, consultez https://www.fca.org.uk/consumers/protect-yourself-scams.

Les cybercriminels utilisent généralement une technique d'escroquerie appelée « hameçonnage », qui est principalement basée sur les e-mails, mais qui peut également se faire par téléphone, pour attirer les victimes sous de faux prétextes vers des sites Web qui semblent légitimes afin de les amener à fournir des informations, notamment sur leur compte bancaire et leur carte de crédit. Ces e-mails/appels téléphoniques semblent provenir de sources reconnaissables telles que des banques mais renvoient en fait à des sites Web frauduleux.

Nous encourageons les membres à ne donner des renseignements personnels que s'ils sont absolument sûrs de savoir avec qui ils communiquent. De plus:

- Protégez votre e-mail avec un mot de passe fort (astuce: utilisez 3 mots au hasard pour créer un mot de passe unique difficile à déchiffrer).
- Votre mot de passe ne doit être partagé avec quiconque.
- Installez les dernières mises à jour de sécurité sur votre logiciel de navigation et vos appareils informatiques personnels.
- En cas de doute, n'ouvrez pas les e-mails provenant d'expéditeurs que vous ne reconnaissez pas.
- Vérifiez que les liens semblent corrects avant de cliquer dessus.
- Si vous recevez des messages ou des appels suspects, veuillez ne pas transmettre d'informations telles que vos coordonnées bancaires.
- Si vous recevez un courriel suspect, vous devez le transférer à report@phishing.gov.uk.
- Pour les messages texte et les appels téléphoniques, raccrochez et transmettez l'information au 7726 (sans frais).
- Pour les envois par courrier, contactez l'entreprise concernée.
- En cas de modification de vos informations d'assurance nationale, HM Revenue & Customs vous contactera - mais vous pouvez également les appeler au 0300 200 3500.
- Si vous craignez qu'une personne se fasse passer pour un fiduciaire ou une personne de la Commission en ce qui concerne votre régime de retraite, veuillez agir avec prudence et demander à la personne de fournir une pièce d'identité et des renseignements complets avant de lui fournir des renseignements ou de prendre toute autre mesure à la suite de ce contact.

Les membres concernés recevront désormais des lettres, afin que nous puissions les soutenir et minimiser les risques associés à cet incident. Si vous n'avez pas reçu de lettre, nous comprenons de Capita que vos données n'ont pas été exfiltrées. Toutefois, nous croyons toujours que, pour des raisons de sécurité, vous devriez toujours agir comme s'il y avait une probabilité que vous ayez été affecté.

Encore une fois, nous sommes désolés pour la détresse et les inconvénients que cet incident vous a causé ou vous causera, et nous tenons à vous rassurer qu'une fois que nous en aurons pris connaissance, nous agirons rapidement pour essayer de réduire la probabilité d'effets négatifs.

Les fiduciaires du régime de pension du *Commonwealth War Graves Commission Superannuation*