Information about the cyber-attack | Electoral Commission Search Information about the cyber-attack You are in the Public notification of cyber-attack on Electoral Commission systems section Home Public notification of cyber-attack on Electoral Commission systems On this page About the cyber-attack About your data About voting and elections About our actions Contacting us First published: 8 August 2023 Last updated: 14 August 2023 What happened? The Electoral Commission has been the subject of a complex cyber-attack. The incident was identified in October 2022 after suspicious activity was detected on our systems. It became clear that hostile actors had first accessed the systems in August 2021. We worked with external security experts and the National Cyber Security Centre to investigate and secure our systems. About the cyber-attack What kind of information was accessible and how do I know if my data was accessed? How might the data be used? During the cyber-attack, our file sharing and email systems were accessible, which contain a broad range of information and data. The personal data most likely to have been accessible includes any names, addresses, email addresses, and any other personal data sent to us by email or held on the electoral registers. The following information is held by us and was accessible during the cyber-attack: The names and addresses of anyone in Great Britain who was registered to vote between 2014 and 2022, the names of those registered as overseas voters in the same period, and the names and addresses of anyone registered in Northern Ireland in 2018. The details of anonymous voters were not accessible, as we do not hold these. Any details provided to us via email or through forms on our website, such as the 'contact us online' form. The registers held by the Commission do not contain dates of birth, national insurance numbers, email addresses, information on your chosen voting method (post, proxy, or in person) or any other personal information. However, when people under 18 register to vote, the day and month they turn 18 is included on the register. This information could be used to calculate the date of birth for someone who is under 18. Information on people under 16 who are registered to vote in Scotland and Wales is not included in the registers held by the Commission. We know that data held by the Commission was accessible during the cyber-attack, but we have been unable to ascertain whether the attackers read or copied personal data held on our systems. We don’t know how this data might be used, but according to our risk assessment (which was conducted in line with an ICO-recommended framework) the personal data held on electoral registers, typically name and address, does not in itself present a high risk to individuals. Further information is available in our Privacy Policy , and you can submit a form to access the information that we hold on you. How serious is this breach? We know it can be troubling to hear that your data may have been accessed. We regret that sufficient protections were not in place to prevent this cyber-attack and apologise to those affected. The data contained in the electoral registers is limited, and much of it is already in the public domain. According to the risk assessment used by the Information Commissioner’s Office to assess the harm of data breaches, the personal data held on electoral registers, typically name and address, does not in itself present a high risk to individuals. It is possible however that this data could be combined with other data in the public domain, such as that which individuals choose to share themselves, to infer patterns of behaviour or to identify and profile individuals. Who was behind it? We do not know who is responsible for the attack. We reported the incident to the National Cyber Security Centre (NCSC). No groups or individuals have claimed responsibility for the attack. When and how did you find out? We were alerted to the attack by a suspicious pattern of log-in requests to our systems in October 2022. This led to an initial investigation and to the identification of a possible breach. Following a thorough investigation, we were informed by our security partners that hostile actors had accessed our servers in August 2021. Who did you alert? We contacted the National Cyber Security Centre (NCSC) (which is a part of the Government Communication Headquarters (GCHQ)) and advised them that we suspected we were the victim of a successful cyber-attack. We worked with the NCSC and a security partner to secure our systems and investigate further. We reported the incident to the Information Commissioner's Office (ICO) within 72 hours of identifying the breach. Why are you informing the public now? There were several steps that we needed to take before we could make the incident public. We needed to remove the actors and their access to our system. We had to assess the extent of the incident to understand who might be impacted and liaise with the National Cyber Security Centre and the Information Commissioner's Office. We also needed to put additional security measures in place to prevent any similar attacks from taking place in the future. About your data Is there anything I need to do? Can I check if my details have been shared on the internet? There is no indication that information accessed during this cyber-attack has been published online, but there remains the possibility that some information has found its way into the public domain. There are a number of steps that can be taken to check whether your personal information is publicly available. If you have not opted out of the open electoral register, the information we hold will already be publicly accessible via websites like 192.com. If you want to check if your email address has been compromised, you can search https://haveibeenpwned.com/ to see if your email address has been released through reported data breaches. If you think that you have supplied any financial data to us via email, there are free online credit check tools by reputable companies like Experian, which include online identity theft protection and monitoring. The National Cyber Security Centre has a suite of advice to help you and your family understand more about securing your data. For more detail, our Privacy Policy sets out the types of personal information that we collect, our legal basis for processing personal data and how to contact us if you have a question or concern. How can I check what information the Electoral Commission holds about me? To see what information we hold on you, you can submit a subject access request. The easiest way to do this is by submitting a form , but you can also make a subject access request by email or phone. When submitting a request, please let us know if you are asking for a search of the electoral register data, or all Commission systems, and what personal data you may have submitted to the Commission. In your request, please provide your name as it appears on the electoral register or your polling card, and a preferred contact email address for us to contact you about the request. We may follow up to ask you to provide proportionate information to confirm your identity, identify your data and process the request. Please note, if you are seeking the information of another adult or a child over the age of 13, you will need to demonstrate that you have the person's consent to collect their personal data and/or have legal authority to act on their behalf. Will someone be able to trace me to my home address? If you were registered to vote in Great Britain between 2014 and 2022, or in Northern Ireland in 2018, your address may have been accessed during this cyber-attack. The addresses of those registered as overseas voters were not accessible, nor were details of people registered anonymously which are not held by us. There is no indication that information accessed during this cyber-attack has been published online, but it is possible that individuals could be located if this information finds its way into the public domain. Please note, the addresses of those on the open register are already publicly available. The addresses of those who opt out of the open register, are not made publicly available, but were accessible during this cyber-attack. If you want to check your registration status or opt-out of the open electoral register, please contact the electoral services team at your local authority. Their contact details can be found through the postcode search on our website. We know it can be troubling to hear that your data may have been accessed. We regret that sufficient protections were not in place to prevent this cyber-attack and apologise to those affected. Will this impact my credit score? No, this will not have an impact on your credit score. If you have any concerns about identity theft, you can contact Action Fraud , which is the national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland, or Police Scotland , if you are based in Scotland. About voting and elections Will this have an impact on my ability to register to vote or take part in elections? No, this has no impact on your ability to take part in the democratic process and will not affect your current registration status or eligibility. The registers that we hold are copies that we use for research purposes and to check the permissibility of donors. Individual electoral registration officers for each local authority area hold the live versions of the electoral registers which are used to send out polling cards and at polling stations to check voters are registered and eligible to vote. The registers held by electoral registration officers are unaffected by this cyber-attack. Can someone impersonate me and vote? No, the data in this breach would not be enough for someone to impersonate you under current voting rules. What impact has the cyber-attack had on the security of UK elections? There has been no impact on the security of UK elections. The data accessed does not impact how people register, vote, or participate in democratic processes. It has no impact on the management of the electoral registers or on the running of elections. The UK’s democratic process is significantly dispersed and key aspects of it remain based on paper documentation and counting. This means it would be very hard to use a cyber-attack to influence the process. Can you be sure the electoral registers were not edited or changed in anyway? We do not amend the copies of the electoral register that we hold in the performance of our work, and we are confident that the information within the files was not altered during the incident. The registers that we hold are copies that we use to check the permissibility of donations and for research purposes. Individual electoral registration officers for each local authority area manage the registration processes and hold the live versions of the electoral registers which are used to send out polling cards, and at polling stations to check voters are registered and eligible to vote. How can I opt out of the open register? There are two versions of the electoral register. The full version includes the name and address of everyone who is registered to vote, except those who register to vote anonymously. The open register is an extract of the full electoral register. This version is available to anyone who wants to buy it, such as businesses or charities. You can opt out of the open register when you register to vote. If you are already registered to vote and want to opt out, you can do so at any time, by contacting your local electoral registration officer . The request must contain your full name, and address, and you will need confirm that you want to be removed from the open/edited register. You can find contact details for your local electoral registration officer by entering your postcode into our search . About our actions What steps has the Commission taken to ensure its system are now secure? We have taken steps to secure our systems against future attacks and improved our protections around personal data. We have strengthened our network login requirements, improved the monitoring and alert system for active threats and reviewed and updated our firewall policies. We have worked with external security experts and the National Cyber Security Centre to investigate and secure our systems. Contacting us How do I contact the Commission to complain, ask a question about this incident or to request the information the Commission holds on me? In the first instance, please read the information available in our Public Notification . You can submit a form if you still have questions, or if you want to: make a Subject Access Request request erasure make a Freedom of Information request submit a complaint Submit a form Who else can I raise concerns with about this incident? We would encourage you to contact us in the first instance with any concerns or questions. If you are not happy with our handling of your questions or subject access requests, you can contact the Information Commissioner’s Office, as the UK supervisory authority for data protection, via their online form.