Suffolk Housing

Cyberattack

Some frequently asked questions

What happened?

Online criminals gained access to our onsite data centre, via a suspected phishing attack. The hackers released a ransomware virus, encrypting our databases and compromising some personal staff and resident data.

When did the company learn of the incident?

On Sunday 1 November 2020, we became aware of a major IT incident, that took most of our systems offline, and limited some of our services. On discovering the incident, as a precautionary measure, we immediately took all our systems offline to prevent the issue spreading further. We found out the severity of the incident on 4 November 2020 and issued an official statement via our website, social media, and the press.

What steps should I immediately take?

We recommend that residents be vigilant in reviewing their account statements and credit reports, and that they immediately report any unauthorised activity to their bank. We also recommend that they monitor their personal information and visit **https://ico.org.uk/your-data-matters/identity-theft** to obtain information about steps they can take to better protect against identity theft.

Do I need to change my passwords?

We recommend that residents be extra vigilant, report any suspected phishing attempts to the authorities and amend passwords to prevent login attempts from third parties.

Why are Flagship only just notifying me? I already know about this from a third party.

To prevent the issue spreading further, we immediately took our systems offline. However, this limited the number of secure communication channels available to notify residents. We issued our statement through social media, a website holding page and via the press, to help notify more residents.

Who has been affected and what information may have been impacted?

We can confirm that despite our quick action, some personal resident and staff data has been compromised, however, we are yet to have a complete picture of all the data that has been encrypted. Therefore, please be cautious when dealing with telephone calls and emails. We will continue to provide updates, via our website and social media.

How do I get in touch whilst your systems are down?

Our teams are working tirelessly around the clock to bring our systems back online, and we apologise for any inconvenience this may have caused. You can still contact us on Twitter **@SuffolkHousing**, by telephone **01284 767 224** or by email **enquiries@suffolkhousing.org**

Can I still pay my rent?

Yes, our phone lines are back up - please call **01284 767 224** to pay your rent.

I need a repair - what should I do?

To book a repair, please call **01284 767 224**.

Why are my details incorrect?

We have contacted all residents based on the most recent secure data we have. We apologise if we've made a mistake. We kindly ask that you get in touch with us to update your contact details.

Is this a new cybersecurity incident?

There has NOT been an additional incident. These FAQs are based on our findings from the cybersecurity incident announced November 4, 2020.

Is the issue contained?

We have taken steps to stop the spread of the attack, which have been successful. We have already implemented extra security measures and controls.

How did this happen?

We have been intensely investigating the scope of the intrusion, with the assistance of a leading, independent cybersecurity firm, to determine what information was accessed and who has been impacted. We continue to work with the Police and other third parties as part of our criminal investigation.

What are you doing to prevent this happening again?

We engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

We continue to work tirelessly to support residents and make the necessary changes to minimise the risk that something like this happens again. We have taken numerous steps to review and enhance our cybersecurity practices, and we continue to work closely with our internal team and outside advisors to implement and accelerate long-term security improvements.

Has Gasway's data been compromised?

To date, there is no evidence that Gasway's data has been compromised. However, we are yet to have a complete picture of all the data that has been encrypted. We will update you if this changes.