Information and FAQs on the 23rd August 2021 data security incident

Last Modified on 01/09/2021 10:34 am BST

Last updated: 31st August 2021

On 23rd August 2021, BookingsPlus was informed of a data vulnerability on one of our testing servers. This involves the risk of unauthorised access to customers' documents through bypassing our server security. In this instance no financial information or user login details, such as usernames or passwords, were made accessible as this information is not stored on the server.

We understand that this is a cause of concern and we have put together some FAQs to answer some of the questions you might have. You can also reach us on our dedicated phone number 01604 677764, or by emailing support@bookingsplus.co.uk.

What happened?

On Monday 23rd August 2021, we were informed that one of our testing servers had a vulnerability which allowed for potentially unauthorised access to customers' documents.

A unique URL (web address) is generated when a user uploads a document while making a booking through BookingsPlus. This means someone with knowledge of the exact, unique URL would be able to bypass the server security measures and assess the documents. However, these URLs have never been made public and consequently the chances of someone being able to discover them are very low.

As soon as we were made aware of this vulnerability, we acted immediately to increase the security on this server and to stop potential unauthorised access to any information.

We have reported the incident to the Information Commissioner's Office, the UK's data protection regulatory authority. Our data protection officer and technical team will work closely with the authority to provide updates and to implement further actions if required.

Is the incident ongoing?

No. We have identified the cause of the vulnerability and addressed it to make the data secure.

What data was accessible?

The documents uploaded by some of the hirers required for making bookings on BookingsPlus were accessible. Depending on the nature of the specific booking, these could include documents such as copies of DBS/CRB certificates, Insurance Documents, Risk Assessments, First Aid Certificates, Booking Request Forms, Music Licences, Invoices, Purchase Receipts, passports, driving licenses and similar documents. No financial or account related data was stored on this server.

Although these documents were made accessible via the unique URL, they are not accessible online in general or via search engines such as Google. In addition, no usernames, passwords or payment details were compromised.

We have contacted the hirers whose documents were subject to the risk of unauthorised access.

Are my financial details secure?

Yes, all your financial details are secure as there was no financial information stored on the server where the vulnerability was detected.

Our detailed investigation of the extent of the incident has now been completed and all vulnerabilities have been addressed.

Who has been affected?

The documents outlined above were accessible for some of our hirers who have used BookingsPlus in the past. We are doing everything we can to contact everyone affected to explain what has happened as soon as possible.

What should I do now?

Whilst the risk of the uploaded documents being widely circulated is very low, we would advise our users to be vigilant. It is possible that while the vulnerability existed on our server your documents may have been accessed by an unauthorised party who could use the information for malicious activities. Some of the ways you can help to keep your information safe are:

- Watch out for suspicious calls, texts or emails or messages on social media accounts. Do not click links within emails you do not recognise.
- Delete texts from numbers or names you do not know.
- Let us know if you receive any suspicious or unsolicited emails, in particular any that appear to come from BookingsPlus.

If you are suspicious about an email, call or letter that appears to come from BookingsPlus, please contact us straight away. You can reach us on our dedicated helpdesk phone number 01604 677764 or by emailing support@bookingsplus.co.uk. We are experiencing higher call volumes than normal, so if you can, please email rather than calling. We will get back to you as fast as we can.

What measures are you putting in place to stop something like this happening in the future?

We have reviewed the security of all our servers and implemented enhanced security policies as required. We have also reviewed our technical processes to ensure there are robust controls in place to prevent such incidents from happening in the future. In addition, our data protection officer and technical team will be committing a thorough review of the incident and have committed to conduct more regular data protection risk assessments and security inspections moving forward as well as a refresher training session for staff.

Who can I talk to about this?

We have set up a dedicated team to deal with any questions or concerns you may have. You can reach us by phone on 01604 677764 or by emailing support@bookingsplus.co.uk. We are here Monday to Friday 9am – 5.30pm (UK time) and we will do our best to deal with all your queries as quickly as possible.