| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-2443Responded to: 21 October 2024 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## Under the Freedom of Information Act 2000, I kindly request the following information regarding cybersecurity breaches or hacks experienced by your police force over the past three years (from ****1st January 2020 to the present****):

## ****A chronological list of all cybersecurity breaches or hacks**** that have occurred within the specified time frame. For each incident, please provide:

## ****Date of the breach/hack********A brief description**** of the nature of the breach/hack****Impact on operations****, including any data compromised****Measures taken**** to address the breach/hack and prevent future incidents

I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland in terms of section 18 of the Act.

Section 18 applies where the following two conditions are met:

* It would be contrary to the public interest to reveal whether the information is held

Confirmation or otherwise would provide criminals and those of criminal intent with valuable information which could then be used to identify vulnerabilities in police systems and thus increase the risk of cyber-attack.
This could result in a loss of sensitive police data or deny the police service access to critical infrastructure systems.
Therefore, at this moment in time, it is our opinion that for these issues the balance test favours non-disclosure.

* If the information was held, it would be exempt from disclosure in terms of one or more of the exemptions set out in sections 28 to 35, 38, 39(1) or 41 of the Act.
The following exemptions are considered relevant:

**Section 31(1) - National Security and Defence**

The security of the United Kingdom is of paramount importance and we will not disclose information if it would impact on National Security.
Disclosure would highlight perceived vulnerabilities within force systems which could be exploited by terrorists.

**Section 35(1)(a) - Law Enforcement**

Disclosure would substantially prejudice the ability of Police Scotland with regards the prevention of crime, enabling criminals to build a picture of perceived vulnerabilities, informing their criminal activities.

This explanation should not be taken as indicative or conclusive evidence that the information you have requested does or does not exist.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.