Officers FAQs

What has happened?
On Saturday 9 and Thursday 21 March HQ systems were subject to cyber-attacks which impacted a number of our databases and servers. The first attack only affected PFEW's HQ at Federation House, Leatherhead and did not impact on branches. On Thursday 21 March a second attack occurred which has affected the majority of our Branches.

How was the second incident allowed to happen?
Following the first malware attack on 9 March we immediately took precautions to secure and stabilise our systems. We are still investigating the second incident. We will provide more detail as it emerges.

How did you discover the incident?
We were alerted to the first incident at around 1900 hours on Saturday 9 March through our own security systems. We were alerted to the second attack at approximately 1445 hours on Thursday 21 March.

What happened then?
On both occasions we immediately disconnected our network in order to minimise spread. Following the first attack we instructed BAE systems, a leading forensics firm, to assist with the response. They are continuing to work with us and were on site during the second attack.

Have you reported it?
Yes. Both incidents have been reported to the National Cyber Security Centre (NCSC), the National Crime Agency (NCA) and the Information Commissioner's Office (ICO).

The first incident was reported the incident to the Information Commissioner's Office (ICO) on Monday 11 March. The second attack was reported to the ICO on Friday 22 March.

What is the malware?
The malware is a type of malicious software which seizes and encrypts data. As the matter is subject to an ongoing police investigation we are unable to comment further at this stage.

Who is affected?
There is no evidence that any personal data has been extracted from PFEW at either the HQ or any of its branches. However, we cannot rule this out and investigations continue. We have been contacting various categories of individuals who may be affected and providing them with details as to where they can get help and further information.

Has my safety been compromised?
At present, we are not aware of any evidence that data has been extracted. However, this cannot be discounted at this stage. We are therefore proceeding with caution on the basis that this is at least a possibility.

As a precaution, we suggest that officers in the following categories, if they have not been contacted already, contact their force so a risk assessment can be carried out: Counter Terrorism, Undercover Police Officers, officers who have been involved in police shootings and CHIS handlers past and present.

What systems did it affect? How much data was affected?
Most of our systems have been affected but it's too early to tell how much of the data that has been encrypted can be recovered.

Was PFEW targeted directly?
Indications are that the first attack was not targeted specifically at PFEW and was likely part of a wider campaign. We cannot speculate as to the second attack at this stage. Both incidents are still being investigated and we will provide more detail when the facts emerge.

Are you informing those who have been affected?
There is no evidence at this stage that any data was extracted from our systems, although this cannot be discounted at this stage and we are proceeding to notify individuals who may be affected as a pre-caution.

Why have you not informed us until now?
The matter is complex and has been the subject of a criminal investigation. We have had to liaise carefully with relevant authorities as to the information that can be made public.

What is happening now?
We are continuing to work with various experts to restore systems and minimise disruption for those potentially affected and to provide as much information as we can.

Have you alerted people to the fact their data may be compromised?
Yes. Whilst there is no evidence that personal information was been extracted, we wanted to alert individuals as to the risk at the earliest opportunity.

What is the advice to officers?
The NCSC recommends PFEW members be vigilant to suspicious emails, texts and phone calls. Advice and guidance for individuals and organisations is available on the NCSC website.

Where can I go for further advice?
Advice on how organisations and home users can reduce the likelihood of malware infection is available on the NCSC website.

I am worried about my data, what can I do?
There is no evidence at this stage that any data was extracted from our systems, although this cannot be discounted. Whilst we consider at this stage the risk of your data being extracted or misused is low, we wanted to alert members as to the potential risk at the earliest opportunity.

We take data security very seriously and have a number of technical and organisational measures in place to protect the data of our members and others whose data we hold. On becoming aware of the attacks we immediately reacted and put in place a number of measures in order to stop further spread.

A dedicated helpline has been set up to answer any concerns you may have – 0800 358 0714 – this is open Saturday-Sunday, 9am-3pm and Monday-Friday, 8am-6pm. It is manned by specialist call handlers with experience in cyber-attacks.

Those concerned about fraud or lost data can also contact Action Fraud. Action Fraud's online fraud reporting tool any time of the day or night, or call 0300 123 2040. For further information visit www.actionfraud.police.uk Advice can also be obtained from the National Cyber Security Centre.