How to react to a cybersecurity incident

Step 1 - Isolate machine

1

Isolate the computer by removing the network cable (if present) AND put the machine in aeroplane mode by clicking on the network icon in the taskbar on the bottom of your screen, or by turning off Wifi and Bluetooth.

Step 2 - Don't switch off

2

Don't turn off the computer leave it turned on to ensure that any evidence is preserved.

Step 3 - Who is affected?

3

Who else has been affected? Is it just you, or are other people around you reporting the same or similar problems?

Step 4 - Call for help

4

Call for help. Telephone IT support on 01483 963 291. Support is available 24 hours a day, 7 days a week. Arrange for someone else to email your leadership team from an unaffected computer or mobile device with details of the incident.

Step 5 - Log off

5

Log off the computer, put a sign on it to stop others using it, and do not log onto any other machine.

Step 6 - Secure media

6

Secure and isolate any additional media, such as memory sticks that are connected to (or used in) the device.

Step 7 - Stay off email

7

Do not access or send any emails until IT/Cyber support have advised it is safe for you to do so.

Step 8 - Begin planning

8

Can you continue your role without your machine? Assist with the incident report.