Freedom of Information request: phishing attacks

To the extent that the request is a valid request for recorded information under the Freedom of Information Act 2000, the University responds as follows (responses highlighted in blue):

1. What is your policy for using personally owned devices accessing IT applications?
- We allow access to both student and staff with personal and corporate devices
- **We allow access to staff with personal and corporate devices**
- We only allow access to corporate devices

2. Do you have visibility into devices that are used to access University applications?
- **Yes**
- No

3. Do you use multi-factor authentication (such as a hardware token, software code generated by a mobile phone app, or an SMS code) to access IT applications? Please select one answer only.

- Yes, we use multi-factor authentication for all access by students, faculty and staff onto the devices, apps, intranet or IT network
- Yes, we only use it for access to all sensitive data such as financial payments, grades and personally identifiable data (PII) data held on the network
- **No, we just use single factor authentication today**
- We just use single factor authentication today but we are planning on implementing multi-factor authentication in the next 12 months.

5. What is your policy regarding patching and updating digital devices, operating systems and apps which access your corporate network? Please select one answer only.

- We implement all patches/upgrades within 48 hours from notification
- **We implement all patches/upgrades within 7 days of notification**
- We implement all patches/upgrades within 30 days of notification
- It is impossible for us to maintain all devices, operating systems and apps at the latest version and patches/upgrades typically take longer than 30 days to implement.
- We outsource the patching and upgrade of all our devices and systems to a third party

6. Has your university ever been the victim of a phishing attack (where an individual is duped into disclosing their login, password or credit card details via an email purporting to be from a trusted source)? Please select one answer

- **Yes**
- No
- Don't know

6a. If yes, how often have you experienced a phishing attack in the last 12 months? Please select one answer.

- 0-5 times
- 6-10 times
- **11-50 times**
- 51+ times
- Don't know

6b. If yes, which is the most common target of the phishing campaigns? (please select one)

- **Students**
- Lecturers/faculty staff
- Employees
- Other (please specify)

6c. What type of data was being targeted? (select all that apply)

- **Student personally identifiable information (PII) e.g. date of birth. National Insurance Nos.**
- Employee PII
- Financial/payroll data
- Research/patents
- **Other (please specify) Students' passwords**

6d. Did you identify the attackers and, if so, are they? (select all that apply). **Information not held**

- Organised cyber-criminals
- Opportunistic hackers (non-organised)
- Political hacktivists
- Disgruntled employees/former employees
- Disgruntled students/former students
- State sponsored hackers
- Other (please specify)