University of East Anglia

Information Services Directorate

The L brary
University of East Anglia
Norwich Research Park
Norwich NR4 7TJ
United Kingdom

Email: foi@uea.ac.uk
Tel: +44 (0) 1603 593 523
Fax: +44 (0) 1603 591 010
Web: http://www.uea.ac.uk

[redacted]

20 December 2016

Dear [redacted]

Freedom of Information Act 2000 – Information request (ref: FOI_16-229)

We have now considered your request of 22 November 2016 for information relating to connectivity with our network and the instances of phishing attacks.

Our response is on pages 3-5 of this letter, together with a copy of your request. As per your request, our response is made using the pre-determined range of answers you provided with your request. However, it should be noted that the Act is a device for providing recorded information and not a means of obtaining answers to questions. Where we have no recorded information that aligns with any of the provided responses, we have indicated that the information is not held.

Additionally, in line with your rights under section 1(1)(a) of the Act to be informed whether information is held, we confirm that the University does not hold information that would identify the perpetrators of phishing attacks on UEA.

Finally, the Act contains a number of exemptions that allow public authorities to withhold certain information from release. We have applied the following exemption to part of your request.

Exemption	Reason
s.31(1)(a), Law enforcement	Some of the requested information would, or would be likely to, prejudice the prevention or detection of crime

As with other large organisations, universities are reliant on the smooth running of their IT networks. Maintaining the security of these networks is a significant challenge for all universities, who are increasingly subject to both general cyber security threats and also targeted attempts to obtain information from students and staff.

Release of any information under the Act represents a disclosure to the world at large. We are aware of publicly available websites which list known vulnerabilities of specific vendors and systems, including the vendors of our networks and security systems. If we were to disclose the authentication methodology of applications and systems, or our policy regarding the patching and updating digital devices, operating systems and apps which access our corporate network, it would enable a motivated individual or group to identify both what security is in place and potentially any known vulnerabilities for that particular software or system. This would simplify and mask any chosen method of attack, would enhance intelligence on how to circumvent UEA security, and would reduce any pre-warning of impending attack. The result would be the exposure of the University's IT systems to various types of unlawful attack, consequently prejudicing the prevention of criminal activity.

Application of the s.31(1) exemption requires us to consider the public interest in withholding or disclosing this information. We acknowledge there is a public interest in increasing transparency in how the University manages its business, and this may include general information about how we manage the IT network underpinning much of the work of the organisation.

However, there is a very strong public interest in preventing criminal activity that could damage the running of the University and the security of information held by and about individual staff and students. On balance, we believe this interest outweighs any lawful public interest in the information that has been exempted from release.

We hope this response will meet your requirements, however if you are not satisfied you have the right of appeal. If you wish to appeal, please set out in writing your reasons for appealing and send to the above address. You must appeal within 60 calendar days of the date of this letter. Any appeal received after that date will not be considered nor acknowledged. This policy has been reviewed and approved by the Information Commissioner's Office.

You also have a subsequent right of appeal to the Information Commissioner's Office. Further information is available on their website: https://ico.org.uk/Global/contact_us, or by telephone on 0303 123 1113.

Please note that any material over which UEA has copyright is released on the understanding that you will comply with all relevant copyright rules regarding reproduction and/or transmission of the information provided.

Please quote our reference given at the head of this letter in all correspondence.

Yours sincerely

Dave Palmer
Information Policy and Compliance Manager
University of East Anglia

Response to Freedom of Information Act 2000 request (FOI_16-229)

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

We allow access to both student and staff with personal and corporate devices.

2. Do you have visibility into devices that are used to access University applications?

• Yes

• No

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.

[Information exempted pursuant to s.31(1)(a), Freedom of Information Act]

This information is exempted from release for the reasons stated in the above letter.

4. What security risks in personal devices are you most worried about when accessing University applications?

• Out of date software. Ex: Operating systems, browsers

• Physical security of devices. Ex: passcode lock

• Jailbroken / Rooted devices

• Others (Please specify)

All of the above. Our Conditions of Computer Use (CoCU)[1] document details all the actions the University expects users to take to protect their systems and data. CoCU references patching software and operating systems, PIN codes on mobile devices, and the risks of rooting devices. CoCU can also be referenced to understand what other security risks are addressed by its rules.

[1] https://portal.uea.ac.uk/documents/6207125/7465906/Section+3+Conditions+of+Computer+Use.pdf

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*

[Information exempted pursuant to s.31(1)(a), Freedom of Information Act]

This information is exempted from release for the reasons stated in the above letter.

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*

Yes

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*

51+ times. Our response is based upon the number of attacks to the University as a whole regardless of whether they were successful in duping an individual into disclosing data. Thousands of individual email addresses are targeted individually via a limited number of phishing campaigns targeting the University.

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

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

All of the noted categories are common targets. Phishing campaigns are quite generic and rarely aimed at a specific user base.

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)*

All the above. Whilst most attacks are designed to capture usernames and passwords to UEA systems, all the listed information has been targeted.

6d. Did you identify the attackers and, if so, are they? (select all that apply).

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

[Information not held – s.1(1), Freedom of Information Act]

The University does not hold this information.