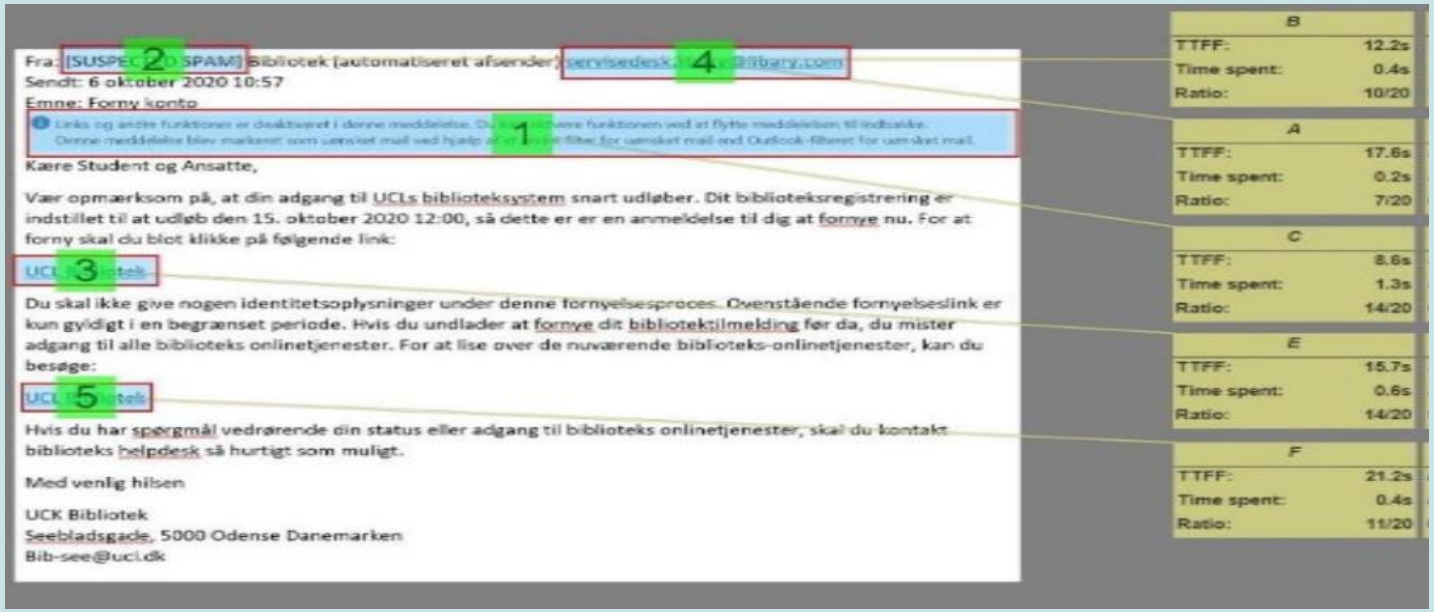
Mapping of a spear-phishing attack on HEI and IT security literacy among students



Kurt Gammelgaard Nielsen, CIO, University College Lillebaelt

University College

Lesson learned

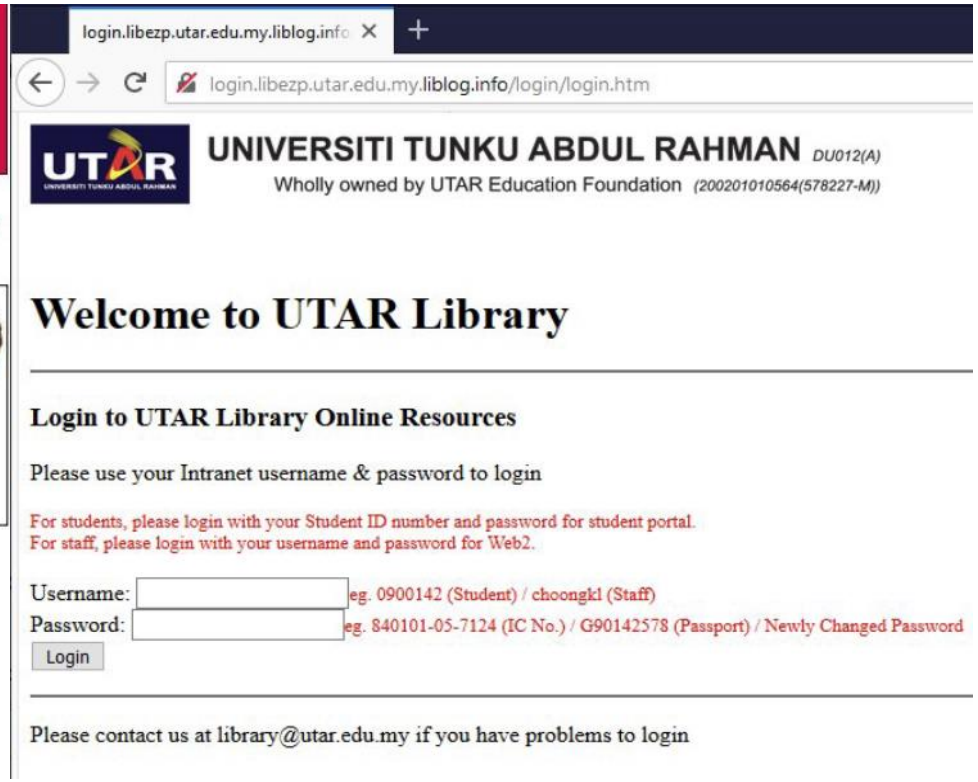
1.We can use open source intelligence tools to uncover attack vectors/infrastructure

2.Mapping a specific attacker revealed that 8 % of HEI in a region has been attacked.

3. Large scale user vulnerability assessment can be used to evaluate how successful an attack will be. This study consisting of 36,851 respondents from two educational institutions showed that a concrete spear-phishing attack will lure 20 to 49% of users.

4. Eye-tracking study can reveal security litteracy among students. This study shows that respondents generally spend more time viewing phishing indicator than one expect by chance, but there seems to be no correlation between viewing indicators and lured to action.

Spear-phishing attack from Silent Librarian



IP: 185.51.201.112. Timestamp: 2021-06-07

University College

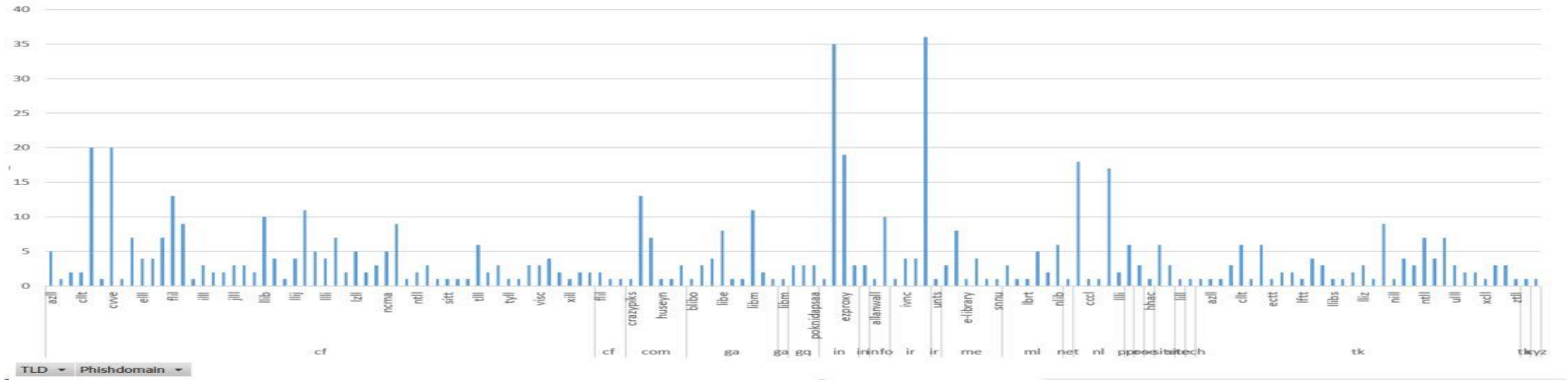
1. Open Source Intelligens Tools

We used passive DNS SIE Europe: https: //www.sie europe.net/

By using information from multiple phishing emails, it was possible to get a Fully Qualified Domain Name (FQDN) and identify the IP address and IP addresses over time.

With passive DNS as the focal point, 604 records or Indicators of Compromise (IOC) were identified across 24 Top Level Domain targeting HEI across EU, US and Australia activated since 2015.

Distribution of phishingsite over Top Level Domain



70 HEI in the Nordic region: 6 IOC in 2020 = 8% risk of attack

8	login.ezproxy.bib.hh.se.ezpro.xyz	19-02-2020	libguides.hh.se/	Halmstad University
13	login.ki.se.iftl.tk	27-10-2020	login.ki.se	Karolinska Institute
18	login.e.bibl.liu.se.ctit.tk	29-10-2020	liu.se	Linköping University
28	innsida.ntnu.snnu.me	31-10-2020	ntnu.no/ub	NTNU Norwegian University of Science and Technology
66	login.proxy3-bib.sdu.dk.ezlogin.info	02-03-2020	alvis-bib.sdu.dk	University of Southern Denmark

University College

2 Large scale user vulnerability assessment

- User vulnerability assessment on the specific spear-phishing attacks used in two comparable studies consisting of 36,851 respondents from two educational institutions: SDU in 2019 and UCL in 2020.
- This study used the DKCERT's phishing service: https://www.cert.dk/da/tjenester/awareness.
- Both groups were given the same information before campaigns.

Leasson learned

Large variation within usergroups: SDU's administrative staff had the lowest risk of 20%. The highest overall risk was found in employees and students at the Faculty of Health Sciences. They received a total of 2,247 emails, of which 1,307 were opened. 831 of these were clicked on, which corresponds to 37%.

The respondent group at UCL consisted of students in commercial and technological degree programs. They received a total of 1,137 emails, of which 185 were opened. 91 of these were clicked on, which corresponds to 49%.

The user vulnerability to this type of attack is thus very large - 20–49%.

The students' ability to transfer skills from the rule-based IT security information received before and during the awareness training until after the training has been very limited.

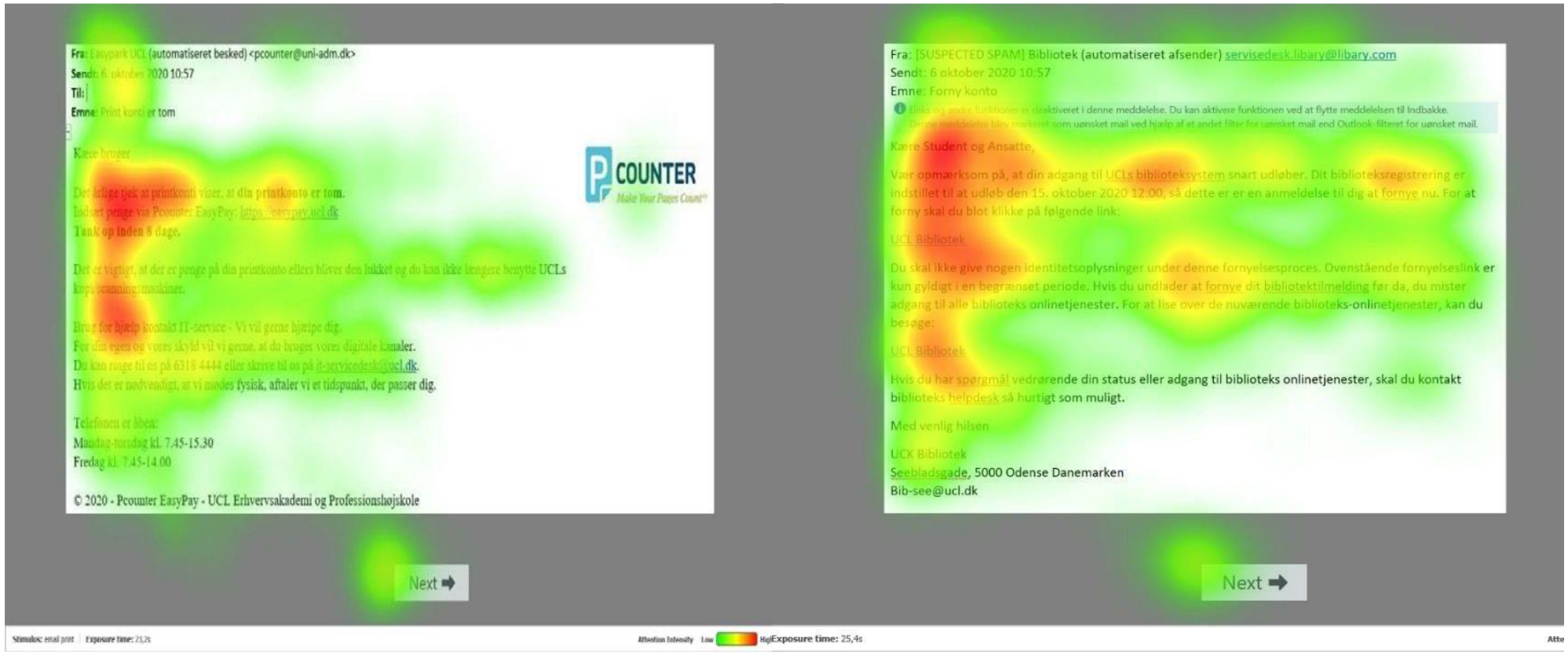
The staffs' ability to transfer skills seems better for administrative compared to academic staff.

University College

3. Eye-tracking study

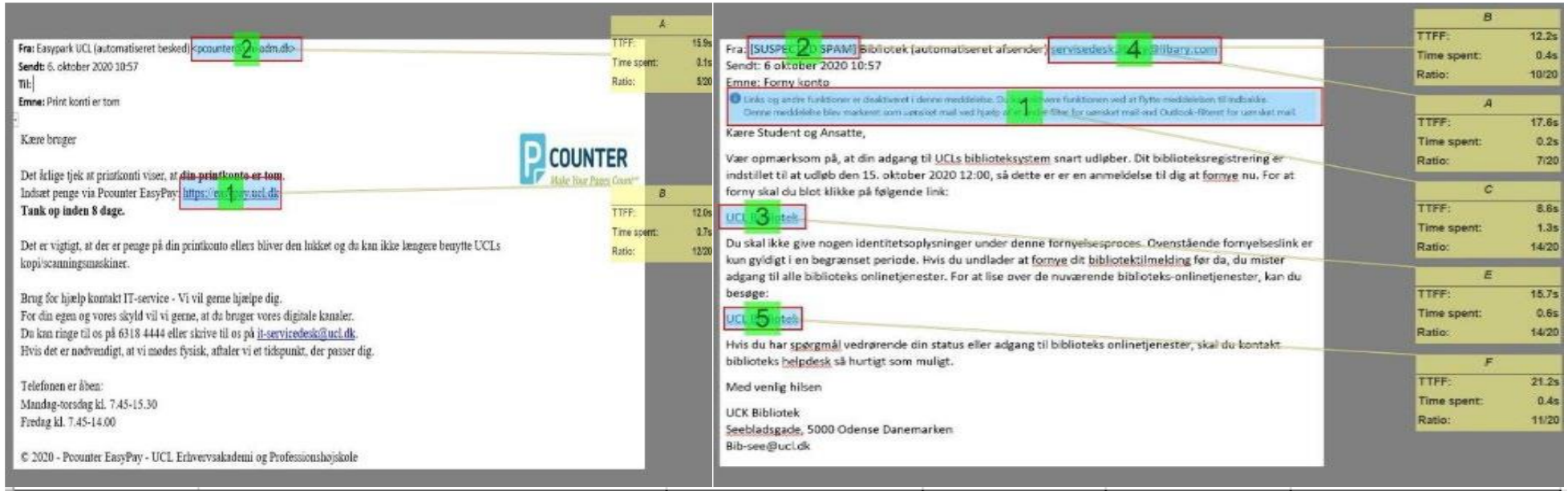
- Conducted on UCL's campus in Odense, Denmark, the 9th October 2020.
- In this study 21 random chosen students were placed in front of a computer connected to eye-tracking equipment (iMotion) and asked to answer a series of questions as well as read 3 emails, with the objective of measuring the respondents visual focus when reading emails and whether these focus areas related to aspects concerning IT security.

Heat maps



University College

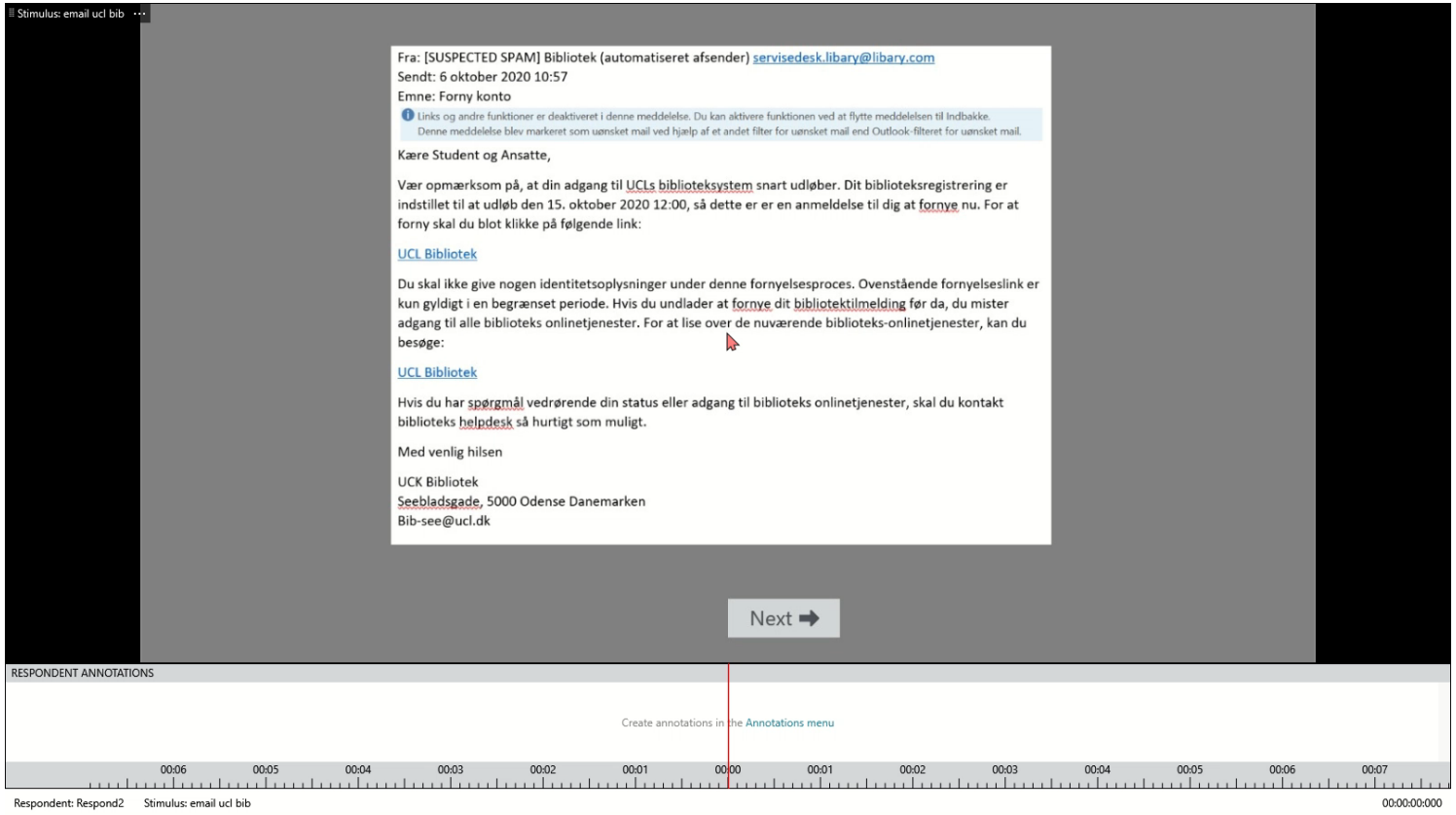
Areas Of Interest (AOI)



Area Of Interest		TimeSpentMs	Visitors	Revisitors	Call to action
Library	Library -real mailadress	241	7	2	
Library	Library -link	641	14	7	4
Print	Print - real mailadress	148	5	0	
Print	Print -link	676	12	8	0
Corona	Corona real sender	366	9	6	
Corona	Corona - link	370	10	5	2

University College

Reading of a spear-phishing mail/Security litteracy



University College

Conclusion

- Silent Librarian – have gone phishing again!
- We can detect Silent Libarian using passive DNS and predict new attack becuase of they reuse infrastructur, cerfificate and methode (phishkit).
- The user vulnerability assessment show that endusers are lured by this spear-phishing. Attack can therefore have high impact on institutions.
- The study shows that respondents generally spend more time viewing phishing indicator than one expect by chance, but are still lured.
- Endusers seems to rate the trustworthiness of mails by an overall reading. As a consequence endusers are easily lured by the attacker because of the trustworthiness of the library spear-phishing mail.
- The lack of security litteracy among students, suggest that more security information in mailheader will not protect HEI

University College