Appendix – responses to proposals and queries

Proposals

	Proposal	Response
1	Temporarily reverse the activation of Safe Links for the University until due diligence is done on the change including wider consultation to determine the business impact on all users, so that the best approach reaching a compromise between usability and security can be deployed.	Rather than reverse the activation of Safe Links for the whole University, ISG would like to work with Schools to fix forward the issues being faced by Schools (see also response to proposal 5). This means that we will be working to mitigate the impact of Safe Links, primarily by exempting domains that will no longer be rewritten and by looking for other actions that can reduce the impact. There is a tension created when trying to protect the whole estate, and ISG feel that each security measure and technology introduced adds to the overall protection. Safe Links is the first step in a rollout of security features in a package known as Defender for Office 365 that the University has access to and we want to ensure that the College Information Security Sub-group (CISSG) is involved in the rollout of further technologies. This should help prevent recurrence of unanticipated and poorly communicated changes to the College.
2	Change the Safe Links configuration to not rewrite (ignore and trust) links in email to domains hosted within the University network and approved external providers, as per the University of Cambridge policy1	ISG accept this on a proactive "allowlisting" basis rather than all ed.ac.uk domains due to risks around unmanaged web estate. Work is already underway to identify and exempt UoE domains and the domains requested have been exempted. The University has a very large web estate and a blanket exemption would open up an unmanaged attack surface. Instead, a positive process of

		identifying domains, running basic security scans and periodic recertification gives us a much more secure approach.
3	Change the Safe Links configuration to NOT rewrite the displayed URL but still redirect the user through Safe Links protection when they click on it. This would result in Safe Links only applying for users running supported Outlook clients to read email, predominantly professional services staff (at least in the School of Informatics).	This suggested change would limit protection to Outlook clients, meaning that many users and devices, particularly mobile devices, would be unprotected. The University has many users that connect to their email account using clients other than Outlook, e.g. Apple Mail. For mobile users alone, there are c8k connections per week made by non-Outlook clients.
4	Update the configuration of Safe Links to whitelist the domains requested in Unidesk ticket I231214-1123 (initially, further domains as necessary) used for sending mail by services within the School of Informatics (and similarly for other schools that request this) so mail sent out by them is not obfuscated by Safe Links (same effect as Proposal 2 above but more constrained). This follows the University of Cambridge policy. Note that this (and Proposal 2) potentially increases the risk associated with specifically targeted phishing attacks so should be considered carefully in balance.	ISG accept that allow-listing should have been considered in advance of release. If we had identified the full impact, we would have ensured an exemptions process was shared ahead of the release. We've started the process of allowing central services and have included all the domains that have been requested. School computing support can contact the service team to request in a bulk addition to the “allow-list” and existing exemptions will be shared Individual users who experience an issue, such as an accidental unsubscribe from a non-standard compliant mailing list, can request exemptions. ISG will then contact the site owner to attempt to address the issue. This is covered on the support page which has a link for requests for exemptions by individuals.
5	Allow any user within the School of Informatics (and similarly for other schools that request this) to opt out of using Safe	'Personal preference' is not a valid reason to exempt individuals from security controls. Following use of the

	Links purely as a personal preference. Given users will already opt out in many cases by individually applying their own third-party filter plugins in email clients that automatically remove Safe Links redirection, it doesn't seem necessary for senior school management approval to be needed. Note that this would be against the University of Cambridge policy.	site exemption process and third-party plugins, where a substantial negative business impact remains, ISG will help to exempt these affected staff from Safe Links and review the exemption on a regular basis.

Questions

	Question	Response
1	As far as we are aware no consultation and prototyping was carried out in schools, why was this not carried out in advance of this change being approved to go ahead?	This has highlighted to us a critical gap in our understanding of an important section of the user base for email which meant that the change impact was wrongly classified and processes for lower impact changes were followed. Consultation and prototyping takes place for all changes introduced by ISG (or justification where this is not possible). The introduction of Safe Links was categorised as delivering significant benefit across a user base of more than 60,000 email accounts by testing URLs for malicious payloads. It was incorrectly classified as having low user impact due to a lack of understanding of the userbase in CSCE and the prevalence of formatted (HTML) email more generally.
2	Why was it felt appropriate that no communication be made to all University users in advance of this change?	This wasn't identified as a change with wide scale impact. ISG acknowledge a more sophisticated awareness of differing user communities is needed, so that wider consultation and communication can be used. ISG use cascaded communication and where required this is supplemented by targeted communication. This approach is in line with University Communications and Marketing guidelines and has been successfully used in many projects such as the MFA rollout.
3	Given that our users can no longer realistically carry out due diligence in checking a link in email before they click on it, what are your recommendations now for protecting themselves from phishing emails?	De-obfuscation plugins and online tools such as: https://www.o365atp.com/ can be used, so due diligence can still be relevant. In evidence highlighted to ISG by TULiPs it is clear that *in general* users are poor at identifying malformed URLs and due diligence, although important, is less effective than automated checks.
4	Can you please provide references to any research papers or documentation (other than from Microsoft itself) that evidence a reduction in successful phishing attacks in an organisation following the introduction of Safe Links and that help support the University	ISG did not seek specific research about the operational effectiveness of this individual control. Safe Links is one of the options available to us with our existing MS365 licence and has been widely used by many Universities and other organisations across the MS user base for many years.

	adopting Safe Links and its chosen configuration?	We had no reason to doubt that it would be effective in adding to the breadth of controls and increase our defence in depth. There are many different types of cyber attacks and email is the primary attack method for targeting individuals. Safe Links is one element of how ISG is trying to reduce the likelihood of compromise of staff and student accounts and computers.
5	Discussion of URLs within email is a common operational requirement within technical teams and user support requests. Can you please provide us with your recommendation for the best way to do this now that the URLs are obfuscated by Safe Links?	There are different ways to mitigate the impact of Safe Links on URLs. Omitting the protocol or www. will enable discussion of addresses, although they won't technically be URLs this will suit some circumstances. Use of formatted email where possible and including URLs in attachments are also available workarounds. There are also decoder plugins for plain-text mail clients and online tools such as: https://www.o365atp.com/
6	Given the significant effect of many central changes on the operational business of schools we wonder if the membership of GoCAB (to make go/no-go decisions on live service changes) may not be sufficiently representative. What are your thoughts on this?	Director of User Services is undertaking a review of the processes around GoCAB, which will include the representation on this group. The results of the review will be communicated to all our stakeholders by the end of March 2024. We expect this to include clarity on the function of the GoCAB as well as updated guidance for those submitting changes to the GoCAB. For info, there is a GoCAB SharePoint site GoCAB is not intended as a vehicle for consultation but for change release. ISG will make full use of established groups in CSE (CPAG and CISS) for collaboration on service changes including planning and testing. Where possible roadmap discussions around the impact and best planning will be shared ahead of actual planning and testing.
7	Given the DPIA is not yet written can you directly provide the processing justification for the use of personal information being passed to (and presumably tracked by) Microsoft when a Safe Link protected URL is followed, including the retention period?	The Data Protection Impact Assessment (DPIA) was in the process for approval and signed off by the Data Protection Officer (DPO) on 16/1/24. In response to this query, we did further investigation as to the encoding of the email address of the recipient and have been able to prevent this happening as of 2/2/2024.

8	Do you believe this rollout followed the recommendations for improving change management, staff trust, and engagement as made by the external auditors of People and Money and fully accepted and endorsed by the Principal. If not, why not and what specific changes will you be making to address this?	The recommendations for improving change management, staff trust, and engagement made by the external auditors was focused on strategic change programmes. Although the change to introduce Safe Links adds to our overall security posture, it is not a strategic change in its own right. However, all changes require appropriate communication and engagement, and we accept this did not take place in this case.