University Activation of Safe Links

Tuesday 16th January 2024

To:

- Gavin McLachlan (CIO)

Cc:

- Alex Carter (Head of Service Management)
- Seye Kuti (Email and Diary Service Manager)
- Alistair Fenemore (Chief Information Security Officer)
- Garry Scobie (Deputy CISO)
- Iain Pryde (Head of Cyber Security Operations)
- Fiona Vine (Head of IT for the College of Science and Engineering)

Dear Gavin,

We are writing on behalf of users in the **School of Informatics**, **School of Physics and Astronomy**, **School of GeoSciences**, **School of Maths** and **School of Engineering** to express our serious concerns about the activation of Microsoft Safe Links on O365 email at the end of last year. While fully appreciating the increasing risk to the University of phishing attacks, and the necessity to mitigate this, we consider this rollout ill-conceived and mismanaged.

The adoption of Safe Links is directly affecting our staff, principally academics, and their ability to work effectively, reliably and efficiently with email, critically where this involves external organisations and collaborators, but also internal communications. In addition, it is also compromising the ability of many of our staff to assess whether the email they receive is genuine or a phishing attempt, negating many years of successful education.

We believe this has been caused primarily by the lack of consultation with Schools before the decision was unilaterally taken to activate Safe Links. In the case of the School of Informatics, with the exception of the administrative Professional Services staff, the vast majority of our Academic, Research, Technical and Computing staff as well as our Research Postgraduate students – to a total of about 900 users – *do not use* Windows and the native Outlook client. Instead, they use MacOS and Linux and consequently the mail clients available on those platforms, such as MacMail, Thunderbird, the Outlook Web client, and many others. This means that for most users' email links "protected" by Safe Links are now shown obfuscated. For example, it is not clear which of below is the genuine UPS website and which is not:

https://na01.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%3A%2F%2Fwwwapps.ups.com%2FWebTracking%2Ftrack%3Ftrack%3Dyes%26trackNums%3D1ZY8A3700336636844

https://na01.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%3A%2F%2Fwwwapps.ups.com%40WebTracking.email%3Ftrack%3Dyes%26trackNums%3D1ZY8A3700336636844

Due diligence before following a link in email is now near impossible, as this example illustrates. We are also concerned about the homogenous sledgehammer approach of using Safe Links to prevent phishing attacks, and we have identified many other significant issues as described in the Appendix.

Had full consultation and testing within schools been undertaken *before* activation, many of the issues could have been identified and addressed in advance of rollout. Similarly, had users themselves been made aware of the change suitably in advance, this is also likely to have identified issues before rollout. If all IT staff had been told about this change (as the GoCAB approval for activation required in C2311-122) *and* this was done with sufficient notice, then we would have been able to work with our users to build support for adopting Safe Links and significant buy-in could have been achieved. However, none of this happened and yet again, as with other recent centrally managed changes, our users have been ignored and this rollout has caused another negative hit on staff trust and engagement. The University must be aware of the need to consult more through, for example, the formation of the University Initiatives Portfolio Board but it seems that this type of change is perhaps perceived as too minor? It is interesting to contrast the rollout of Safe Links with the ongoing rollout of Multi Factor Authentication. The latter went through a prototyping phase with users and IT staff in schools involved in testing and then a steady deployment in stages across the University with considerable focus on raising awareness and communication. As a result, that rollout has seen next to no problems and very positive feedback both for engagement and implementation, hence, contributing to an overall positive improvement in our staff trust and engagement with the centre.

Notwithstanding some of the technical issues identified and our general concern that this creates a false sense of security for our users, we are not against the use of Safe Links in principle.

Below are proposals to alleviate the issues for our users associated with the activation of Safe Links, in order of preference, but not mutually exclusive. Due to the impact on our operations, in particular relating to our academic, teaching and research staff, we request that you consider each and either adopt these proposals or, if not, provide a statement for each explaining why you will not do so (with particular reference to the trade off in usability and time cost against security, principally in regard to the platform and operational requirements of our academic and research staff, ideally with supporting evidence) in order that we can disseminate that back to all our users.

Proposal 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.

Proposal 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 policy[1]. User quote: "*I can understand the justification for applying the Safelinks filter*

[1] SafeLinks exemptions

All *cam.ac.uk URLs are exempted from SafeLinks to improve user experience. Also, we can provide a SafeLinks exemption for specific URLs that meet the following criteria:

to web links that refer to pages outwith the University. However, the filter is being applied to links within emails originating from a University email account that refer to our own web pages! This should be unnecessary; if there are any malicious web pages hosted by University web servers, the only way Safelinks would detect them is if they are already known hazards. However, if they are known hazards and within the University domain, then the University would take them down. Therefore, there should never be any web pages hosted from within the University that are detectably malicious, and therefore no greater security is gained by munging internal web links".

Proposal 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).

Proposal 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.

Proposal 5

Allow any user within the School of Informatics (and similarly for other schools that request this) to opt out of using Safe 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.

Below are some questions that, if properly answered, we think may help alleviate some of the negative effects this change has had for our users. We request that a response from you to each of the questions below is made available so that we can disseminate this to all our users. Please bear in mind that the way these questions are answered will also of course impact on staff trust and engagement, so the responses should be considered carefully.

- The URL is work-related.
- The URL is a sub-domain or site, e.g. https://www.cambridge.science.com or https://github.com/cambridge (but not www.science.com or github.com).
- The re-written URL is causing technical problems for a system or service.

Exemptions are not provided for specific people or mailboxes.

Question 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?

Question 2

Why was it felt appropriate that no communication be made to all University users in advance of this change?

Question 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?

Question 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 adopting Safe Links and its chosen configuration?

Question 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?

Question 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?

Question 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?

Question 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?

I look forward to hearing from you on how the above-mentioned issues will be resolved. Given the pressing nature of this matter, I would appreciate it if you could please respond to our concerns by CoB Friday January 26th.

Yours sincerely,

Tim Colles

All Signatories

Tim Colles, Head of Computing for Informatics

Boris Grot, Director of Computing for Informatics

Helen Hastie, Head of School for Informatics

Joy Candlish, Director of Professional Services for Informatics

Petros Wallden, Informatics representative on College Library and Information Services Committee

Sean McGeever, Computing Manager for Physics and Astronomy

Arthur Trew, Director of IT Services for Physics and Astronomy

Jim Dunlop, Head of School for Physics and Astronomy

Louise Ferguson, Director of Professional Services for Physics and Astronomy

Duncan Colhoun, Head of IT Services for GeoSciences

Bryne Ngwenya, Head of School for GeoSciences

Chris Bevan, Director of Professional Services for GeoSciences

Steven Law, Computing Manager for Maths

Ben Goddard, Director of Information Technology for Maths

Bernd Schroers, Head of School for Maths

Fraser Millar, IT Services Manager for Engineering

Gareth Harrison, Head of School for Engineering

Appendix: Safe Links Business Impact for Informatics

The following is taken from information provided by members of Informatics staff posting to our “inf-general” mailing list, personal correspondence, and observations and opinions of Informatics computing staff.

The enabling of Microsoft Safe Links has impacted our business in various ways:

- Users can no longer determine if a link in an email is suspicious or not. The only way to now do this is to either:
    - click every link to see where it takes you (not a safe thing to do)
    - spend time to try and visually parse the likes of https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fe4bfrhhfr.blob.core.windows.net%2Feddedews%2F5560.html&data=05%7C02%7CNeil.Brown%40ed.ac.uk%7Ca3019084a2e549a1b41508dc0d3034c7%7C2e9f06b016694589878910a06934dc61%7C1%7C0%7C638399748980703986%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C41000%7C%7C%7C&sdata=txa8yPLEKHbwkXauHiCtLPt53KegamdSHZbBUreCjlo%3D&reserved=0 - taking valuable staff time for those that can and putting off those that previously did carefully check links
    - spend time implementing (or downloading unknown code from the internet) mail client filters to undo the SafeLinking.
- Users have reported that links in emails are being visited by the SafeLink servers before it is even opened by the users' mail clients. These links can be:
    - single use, so by the time the actual recipient reads the mail and decides to click on a link, it can be too late. We have at least one example of a member of staff unable to create an account on a service to access research data, because the remote account creation process uses links in emails.
    - automatically subscribing or unsubscribing people to mailing lists due to links being followed. There are least two reports of people missing meetings or actions because it was sent to a list they had unknowingly been unsubscribed from.
    - used to indicate some action the recipient wants to do. e.g. one user reports "I frequently receive emails asking me to review a paper for a journal or conference where the email contains two separate links which can be used to "conveniently" accept or decline the request with one click."
    - spam tacking links, used to confirm if a spammed email is "live" or not. Having been visited, it will confirm that the mail was "read" thus resulting in more spam.
- People are now unable to discuss URLs in an email, e.g. "which URL looks better www.inf.ed.ac.uk/informatics-futures or www.inf.ed.ac.uk/the-future-of-informatics" becomes "which URL looks better https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.inf.ed.ac.uk%2Finformatics-futures&data=05%7C02%7CNeil.Brown%40ed.ac.uk%7Cd245cefe9e3f4b3b741d08dc11f19258%7C2e9f06b016694589878910a06934dc61%7C1%7C0%7C638404976432856633%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=ikTB5ce55sxIPpDzz5rpN8ca4TVnYb3sC3yphCS%2FfLQ%3D&reserved=0 or https://eur02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.inf.ed.ac.uk%2Fthe-future-of-informatics&data=05%7C02%7CNeil.Brown%40ed.ac.uk%7Cd245cefe9e3f4b3b741d08dc11f19258%7C2e9f06b016694589878910a06934dc61%7C1%7C0%7C638404976432856633%7CUnknow

n%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2BEMEQo6vuGtTyL%2Fr0zUB84Vu3eWxPxamHGvM4ZV1D30%3D&reserved=0

- Similarly, forwarding or replying to an email containing links, does not always get "unSafeLinked" and so as well as looking unprofessional, personal data can leak due to the personal identifier in the SafeLinked URL.
- Email with plain text and html MIME attachments are handled inconsistently resulting in Safe Links not always detecting and rewriting URLs causing confusion for users.

The above covers some actual impacts caused by SafeLinks, but we also have other concerns.

- Having been encouraging users to carefully look at URLs to spot phishing links, people may now just click on any SafeLinks obfuscated URL, just to find out where it goes. This is not safe.
- Leakage of personal data, as mentioned above due to word-wrapping, or unintentional edits, a SafeLinked URL when replied to or forwarded can remain partially SafeLinked, and reveal the personal data that is embedded in the URL.
- Related to the above there are privacy concerns about what is being tracked by Microsoft. With all that extra data in the SafeLinked URL and access to any outlook.com cookies when someone clicks on the link, what is Microsoft tracking?
- Why are University services not being excluded from this. Surely, we will spot a local compromised site (and take it down) before Microsoft does. If SafeLinks is to remain, at least mention of local services in emails would not get mangled. We have requested various URLs to be excluded from SafeLinks, but that has been met with a "why?".
- We've received reports that obvious phishing sites are not being flagged as such.
- Can we get any technical details of how the service is supposed to work (at the Microsoft end). For example, my own test showed that the Microsoft servers only did an HTTP HEAD of the SafeLinked URL I clicked on. How would this be enough information to determine if the site was safe or not? Similarly, a colleague reported that the Microsoft servers fetched the full page with a GET *after* it had been sent to the client's browser. And an academic shared logs of the Microsoft servers doing a GET of the original URL before it was even received by his mail client (see the triggering links impact above).
- Are IS aware that Informatics is a multi-platform environment, with differing staff using differing platforms, mainly Linux, MacOS and Windows. A "just use Outlook" answer to solve some of the above, will not work.
- If IS are concerned about turning off SafeLinks for everyone, then they should at least allow individuals who understand phishing attacks and what a dodgy email looks like, to be able to opt out.