ESC European Society of Cardiology
European Heart Journal (2021) **42**, 2141–2153
doi:10.1093/eurheartj/ehaa345
CARDIOPULSE

Security in BioMedical Research publications

Improve platforms for submission of articles for better data protection and scientific integrity for the authors

Introduction

Plagiarism and other forms of intellectual theft are far more common in science than one would like to think.[1,2] Several ways to have access to a scientist's intellectual property exist. In this context, intellectual property means all relevant information shared when a person submits an article. This includes the manuscript, access to all the data recorded and processed during the study that permits the checking of the results in the article. It also includes the author's history of submission and reviewing tasks in that journal. One source of potential intellectual property breach and an effective way to have access to the submission data of a scientist (which is the main concern of this article) is having permanent access to the scientist's account, even if they reset the password. This is unfortunately allowed directly by the submission platform of several journals (see *Table 1*).

The challenge

The steps following a manuscript submission involve a notification of manuscript submission and thereafter a decision letter. While these notifications are widely shared among co-authors, they often, if not always, include a link that automatically logs the co-author into the account of the corresponding author. Although this link may be accompanied by a warning message such as: 'Do not share this encrypted link with others, as it will automatically log you into your account for X-based system'. We find that this link does not allow for the extra layer of security needed for the corresponding author. *Table 1* shows the e-mail including a warning message by selected Journals.

This encrypted shared URL allows someone to log on to the account of the owner (i.e. corresponding author) 'forever' even if the individual resets their password afterwards. This implies that an individual with a conflict of interest or a potential hacker can easily track someone's submissions, in clear violation of the individual privacy. Even more alarming is that it is well known that hacking has become the leading cause of breaches reported by Content Management Systems.[3] Uses of web-based applications for email, messaging, and file storage come with a risk of compromise of sensitive data, identity theft, compromise, or theft of intellectual property (such as metadata, research protocols, and preliminary results).[3] In this context, where anyone can access researcher's accounts using a single link, the effect of hacking may last for long periods.

Experience demonstrates that warning the co-author may not be sufficient enough as deleting a section of the email, while sharing the decision with the co-authors may even be considered as suspicious by

Table 1 Email associated with a warning message by selected medical journals

0-day vulnerability	Submission Platform	Journal	Number of submissions per year	Impact factor 2018	Notification of manuscript submission[b]	Decision letter (email) Revision[b]
Yes	eJournalPress	JAMA[a]	11 600	51.3	Yes	Yes
		Nature	10.768	43.1	No	Yes
		Circulation	Not available	23.1	No	Yes
		JACC	5200	18.6	Yes	Yes
No	ScholarOne	The BMJ	7000-8000	27.6	No	No
		NEJM	4500	70.7	No	No
	Editorial Manager	EHJ	Not available	24.8	No	No
		LANCET	9000	59.1	No	No

[a]Following our correspondences with the *Journal of the American Medical Association (JAMA)* they have taken steps and added the extra layer of security needed for corresponding authors in all their sub-journals.
[b]yes/no = presence/absence of a warning message ('Do not share this encrypted link with others, as it will automatically log you into your account for X-based system').
JAMA, Journal of the American Medical Association; JACC, Journal of American College of Cardiology; BMJ, British Medical Journal; NEJM, New England Journal of Medicine; EHJ, European Heart Journal.

our peers. All the more so, since there is an underlying trust between co-authors.

While a high level of trust between co-authors during manuscript submission is quite common, a major problem with providing co-authors with a login link to corresponding author accounts is that 'a co-author today may not be a friend tomorrow'. Communication among co-authors breaks down and stops because of personality conflicts, professional rivalries, or jealousies and several examples of conflicts among co-authors are documented.[4] A major challenge after terminating a collaboration may be the protection of the confidential topics and data the collaborators used to share as they mostly keep having common research topics of interest. The aim then of any reform of the policies in question that this viewpoint raises, is to avoid collaborators take primary or even exclusive credit for ongoing works just because they still have a way to follow previous colleague submissions.

It is worth highlighting that this is not an isolated problem as wide used manuscript submission and peer-review tracking systems for scientific, technical, medical, and engineering publications would argue. We identified *eJournalPress* as being the provider of the software. *eJournalPress* platforms generate. It is also useful to specify that other respected software platforms do not have these problems (Editorial Manager[5] or Scholarone[6]).

From this perspective, methods for controlling the access to article submission is needed for all platforms. Some solutions could be (i) to create links that will expire after a defined period or (ii) to create a link that will not log into the account if the person changes their password. In fact, recently, Elsevier (publisher of important scientific journals) declared that their server was accessible from the internet with Email addresses and passwords being public for some time. They resolved the issue and advised scientists with an account at Elsevier to change their password.[7] This solution would not be an option with *eJournalPress* as even after resetting the password the submission link is still available to log into the researcher's account.

The European Union regulation 2016/679 on General Data Protection Regulation (GDPR) now formally requires organizations to take privacy into account by design from the conception of a new product, technology or service (Article 25), rather than on a voluntary basis as it was under the previous regime of Directive 95/46/EC (recital 46). Their Data protection by design concept call for a satisfaction of the following requirements:

- Privacy for the user should be the number one concern for the product, technology, or service. The goal is to provide a user-centric experience, rather than one which harbours illicit data processing practices such as mass collection of data or invasive profiling.
- The basic idea is that consideration of the impact of any processing activities when developing a new product, technology, or service should be considered and from the onset and through the lifecycle of the product. Measures should be integrated into the project.
- A need to act quickly to understand the new regulatory requirement and embrace them in order to ensure their products and services are compliant for the brave, new, GDPR world.

Conclusion

While privacy and security in the era of digital health is a major issue, a major limitation to our own privacy relies on one of the most performed task of scientists to advance the field: submissions. We rely on the process of manuscript submission and the peer-review tracking system provider, as well as the journals to protect the customer (the Scientists).

As the old saying goes 'prevention is better than cure'—we therefore think that 'prevention is better than punished scientific misconducts'. We will consider this submission a success if just once instance highlighted in this viewpoint prevents data privacy violation or theft of a scientist's intellectual property.

Bamba Gaye[1,2]*, Stéphanie Khoury[1,2], Willy Sutter[1,2†], and Xavier Jouven[1,2†]

[1]Université de Paris, PARCC, INSERM, F-75015 Paris, France; and [2]Cardiology Department, Georges-Pompidou European Hospital, 56, rue Leblanc, 75015 Paris, France

*Corresponding author. Université de Paris, PARCC, INSERM, F-75015 Paris, France.

†These authors contributed equally.

Conflict of interest: none declared.

Dr Bamba Gaye
Corresponding author
Université de Paris, PARCC, INSERM
56 Rue Leblanc 75015, Paris, France
Phone :33 1 53 98 81 15
Email: bamba.gaye@inserm.fr

References

References are available as supplementary material at *European Heart Journal* online.