# Security

Malware bytes
Email phishing
Sending files
Social hacking
Password manager

## Documents in PDF

"If there’s a credible open-source equivalent to either of these options, we’d love to hear it."

Probably only Epesi (17 years old FOSS project) has this built-in out of the box function where you send a link to a file (e.g. PDF) that has its token and you know if a person downloads the file and from where, plus file version and access history… The process is as follow:
1. Task - e.g. report
2. All files used to generate the report must be included as attachments
3. Editable file like Word, Excel, Open Office, Pages - to be able to edit or recreate the document
4. Final PDF file to be distributed
5. If sent via e-mail then the link/token combination is used for security and access control. We don't send files directly as attachments. This way there is a reduced risk of attachments being too large, network traffic is reduced, files are not sent unnecessary to people who will never open them, smaller chance of email being classified as SPAM, reduced risk of virus infection etc.

https://hackaday.com/2023/06/15/the-simplest-social-engineering-hack-of-them-all/

The author of the article highlights a security issue related to organizations freely sharing their letterhead templates in editable Word documents. While not a traditional hacking technique, this practice can be exploited by individuals with malicious intent. The author shares personal experiences of receiving such documents from various organizations, including banks, universities, and even solicitors. They point out the potential risks involved, such as financial fraud or impersonation, and emphasize the need for organizations to treat letterheads as important security assets.

The article suggests a few alternatives to mitigate this issue. One option is to use PDF documents instead of Word files, as PDFs are more difficult to edit and are widely accepted as a standard electronic format. Another suggestion is to utilize secure online delivery platforms that require authenticated logins to access sensitive documents. The author also invites readers to share any credible open-source alternatives to PDF or secure delivery platforms.

Overall, the article serves as a reminder that even seemingly innocuous practices can have unintended security consequences, and organizations should be more vigilant in protecting their assets, including letterheads, to prevent potential misuse and exploitation.

Revision #3
Created 12 December 2023 03:14:49 by Karina Tylek
Updated 12 December 2023 03:19:45 by Karina Tylek