Section Introduction, Report Writing

Writing good phishing reports is a key skill in ensuring that relevant information can easily be read and understood by analysts or other individuals that were not part of the original investigation. Analysts tend to fall into two traps: writing too much, including unnecessary details which bloat the case, or not writing enough, so later individuals need to re-investigate certain parts of the case in order to fully understand what's happened. Both of these waste time. We want to ensure that your reports are concise, and give across all the information they need to without any unneeded details. It's important to note that different organizations **will have different templates, and require different information, we aim to teach students how to write a generic report that teaches you the core skills of writing investigation cases.**

This section will cover how to construct a concise yet detailed report of a phishing attack or campaign, with the following sections:

- Email header details, artifacts collected, and a description of the body content
- Users affected and actions taken to notify them
- Analysis process, tools used, and results
- Defensive measures taken
- Lessons learned

At the end of this section, we have a video that shows how we would construct a report based on a malicious email, and a practical activity where you will be conducting analysis and writing a report of your own, and comparing it to our version.