Is it ethical for "phishers" to obtain personal information?

Criterion	Marks available	Marks awarded
A: Focus and method	6	1
B: Knowledge and understanding in context	9	2
C: Critical thinking	12	2
D: Communication	3	2
E: Engagement and reflection	6	2
Total	36	9

Commentary

Criterion A: Focus and method

An issue, rather than an ethical dilemma, is identified by the candidate which severely restricts their ability to meet the requirements of the reflective project. This is reflected in the research question, which implies a simple "yes or no" response to which there is realistically only one answer. Instances where the answer might be "yes" (eg phishing by law enforcement to trap criminals or journalists phishing to get a story in the national interest) are not considered. A very limited range of evidence is cited with little or no awareness of bias or validity issues (eg a press release from an internet security company is quoted without any consideration that its purpose is to sell anti-phishing products). Though brief and unevaluated, the evidence selected is relevant and so the candidate does enough to merit a mark in the lowest band for this criterion.

Criterion B: Knowledge and understanding in context

The poor choice of research question and consistent misunderstanding of "ethical" (eg a phisher would think what they were doing was ethical "because it is their form of job") means that the candidate struggles to demonstrate understanding of the ethical dilemma. However, some simple attempts to contextualize the issue ("There will always be phishing you cannot get rid of it, you can only prevent it.") and limited understanding of its impact ("…it is not an easy thing to get rid of, once that person has your information there is no way for you to erase it or take it away from them.") are sufficient to award a mark towards the bottom of the lowest band for this criteria.

Criterion C: Critical thinking

The response is brief with some relevant ideas simply linked. Points are sometimes supported with limited evidence ("During the year of 2012-2013, phishers launched attacks that affected around 102,100 people each day"), showing straightforward understanding of the issue, but largely at a surface level. The candidate's tendency to state a personal position on, or simply describe, the issue, means the points related to the ethical context are largely self-evident ("I found out that it is very unethical that phishers are obtaining personal information.") and attempts at a conclusion are only tangentially relevant.

Criterion D: Communication

Overall, the communication is generally clear, with a simple structure grouping together information on the issue from the point of view of the perpetrator and the victim. The candidate uses, and in some cases defines, relevant terminology (phishing, identity theft, cybercrimes).

Criterion E: Engagement and reflection

For the most part, the candidate makes straight-forward, largely descriptive comments about the research and planning process showing a basic ability to explain justify choices. While there is more evidence for the candidate's engagement with the subject than with the research process, there is a suggestion that, when prompted, they are able to reflect on, rather than merely describe, their thinking (eg the supervisor's comments about source validity and the candidate's reflection on how the range of sources could have been improved). This, however, is not sufficient to justify a mark in the middle band and on balance a mark at the top of the lower band is awarded.