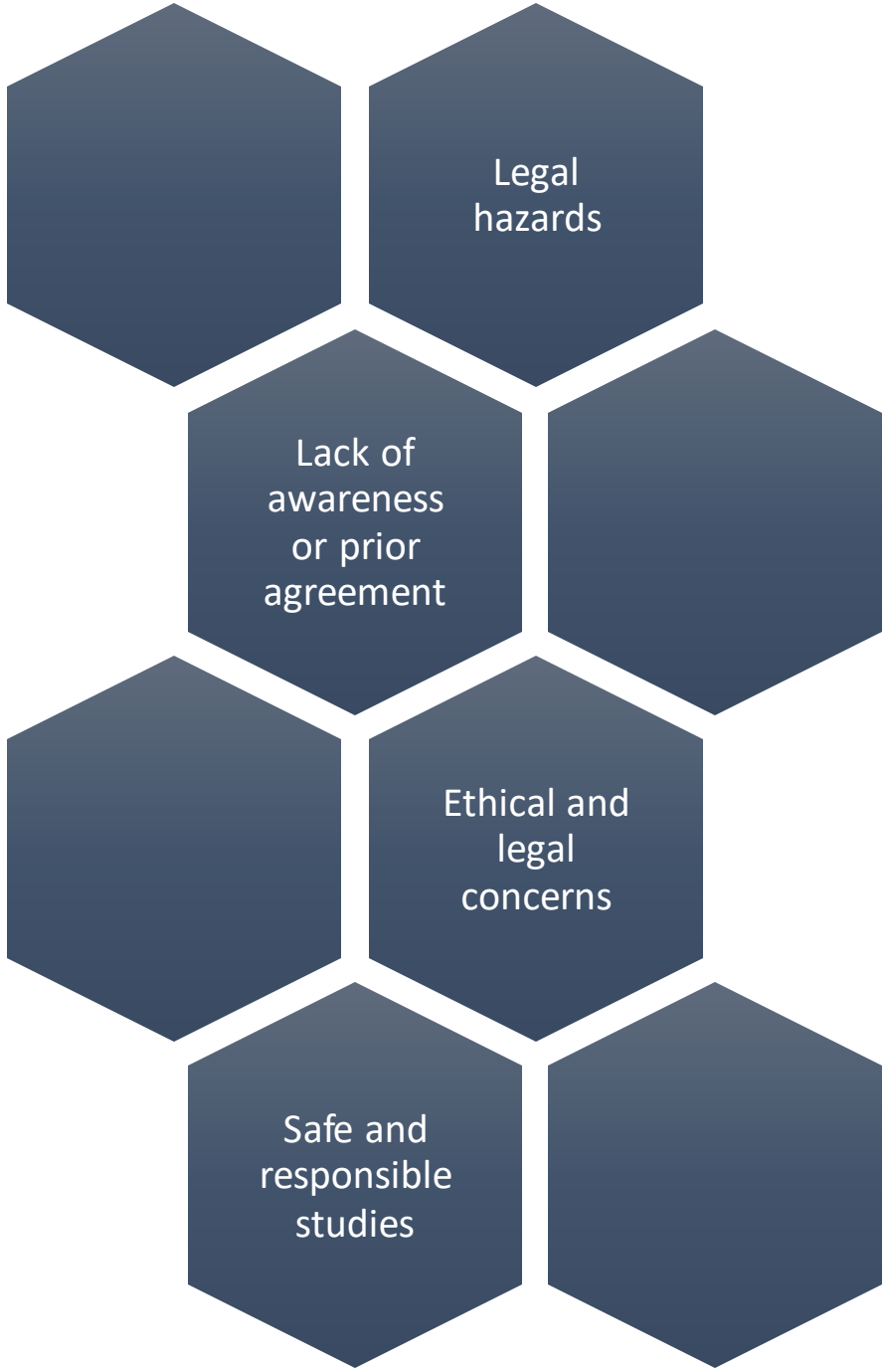
Methodologies and Ethical Considerations in Phishing Research: A Comprehensive Review

- George A. Thomopoulos, University of Patras, Greece
- Dimitrios Lyras, Independent Researcher, Athens, Greece
- Christos A. Fidas, University of Patras, Greece

Research Motivation



Goal of our research

01

To offer a thorough summary of the existing strategies and techniques employed in phishing experiments in university settings

02

To gain insights into the most effective ways to conduct experiments while minimizing risks to human subjects

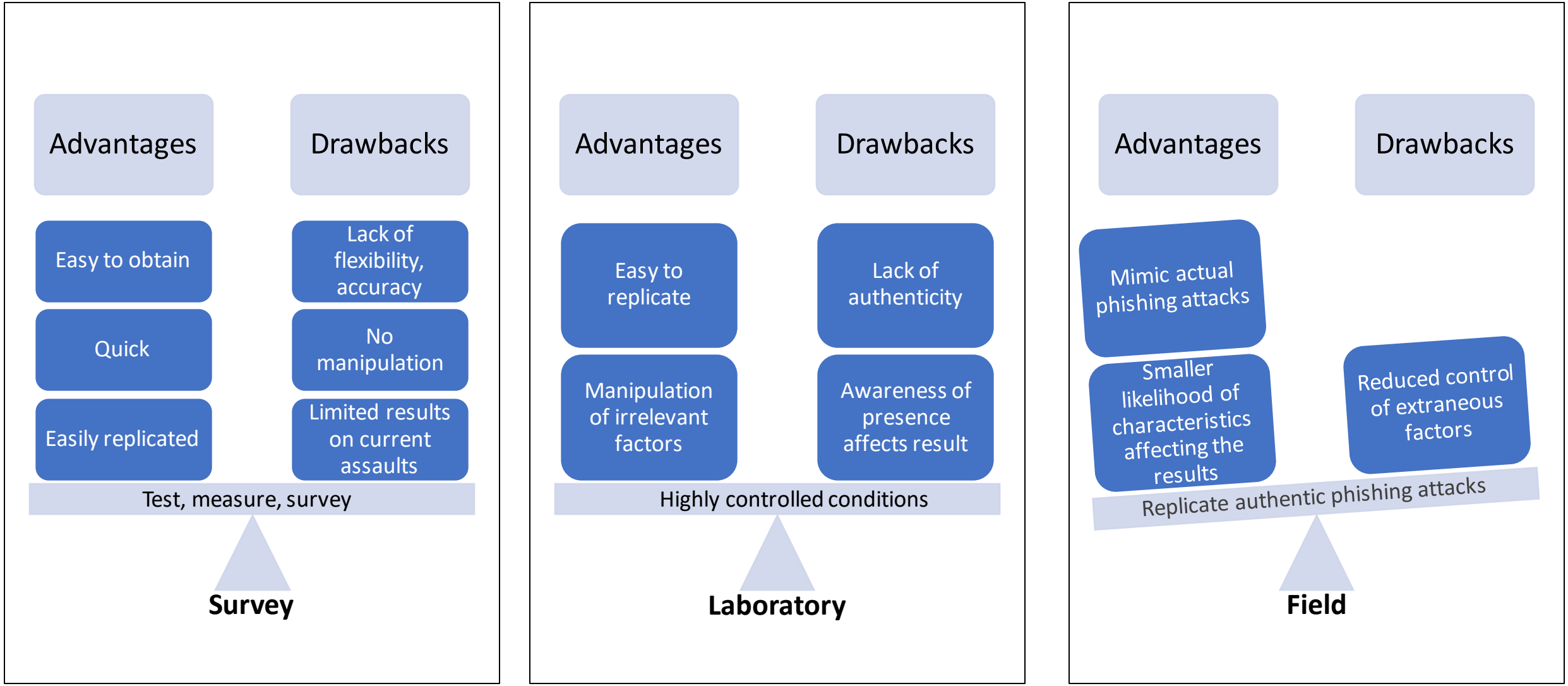
03

To highlight gaps and provide recommendations for future research

Phishing

- Illegitimate message is disguised as a legitimate
- Social Engineering practice, disclose personal information and sensitive data
- Communication methods by the attackers
  - E-mail
  - Smishing
  - Vishing
  - Social Media
  - Other

Framework of conducting experiments in phishing research



Ethics in phishing experiments

Survey studies -
Laboratory experiments

Field studies

Research Ethics: Deception

How individuals respond under authentic circumstances

Willfully conceal certain research methods

Permitted if

- low risk
- impracticable without deceit
- debriefing

Research Ethics: Informed Consent

- Freedom to choose participation
- Well Informed participants
- Requirement of laws and regulations
- Respect the decisions

Research Ethics: Informed Consent absence

Institutional Review Board (IRB) can exclude IC if:

- Knowledge of experiment may compromise the result
- Trials entail minimal hazard
- Research will not impact rights of participants
- Debriefing following experiment

Debriefing

Explain the aspects

Required by research ethics

Voluntary but typically required

Truthfulness, Psychological distress

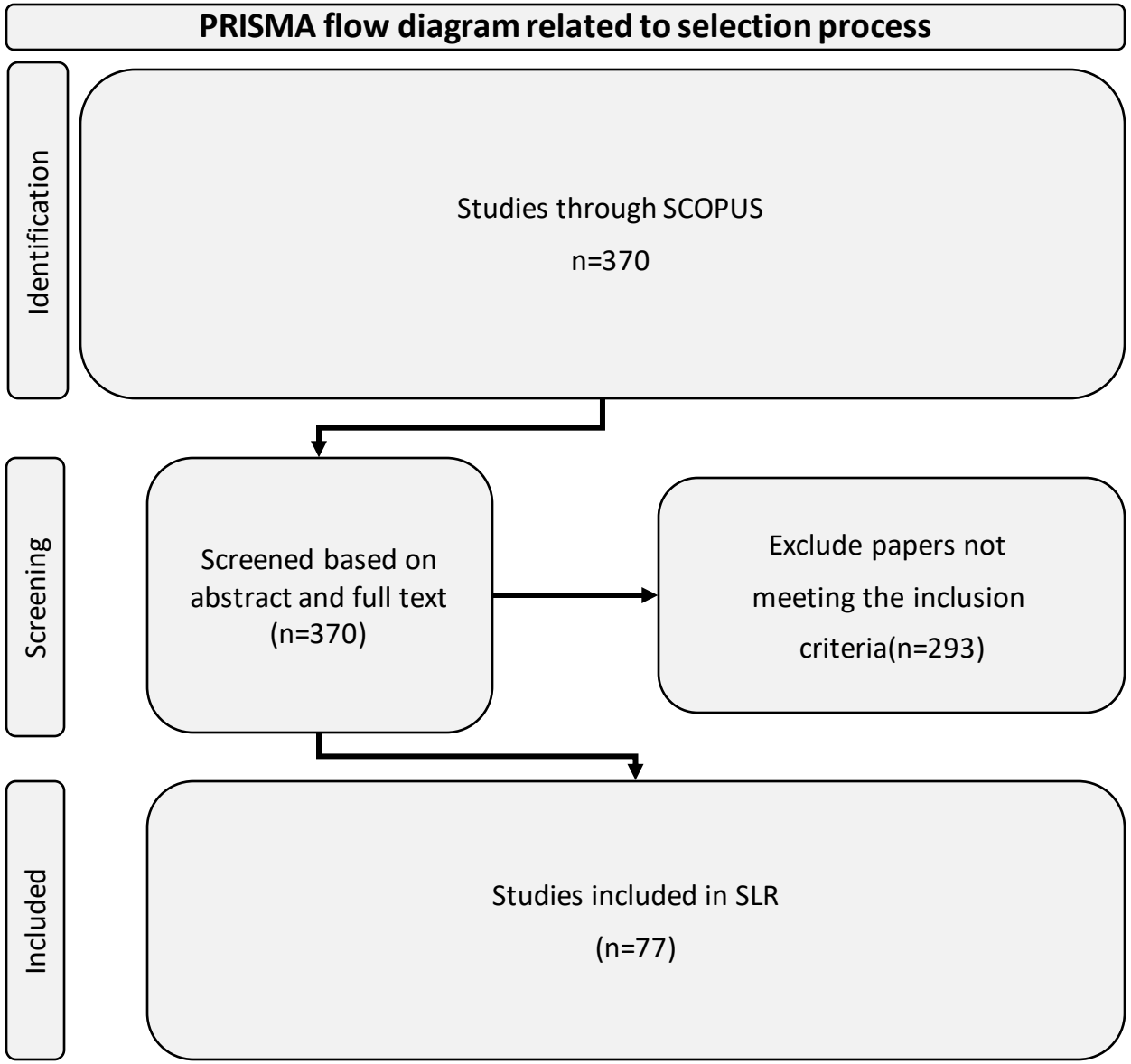
Research questions

RQ1: What methodological approaches for phishing research are followed in phishing experiments?

RQ2: What are the research ethics per methodological approach that are applied to the experiments examined?

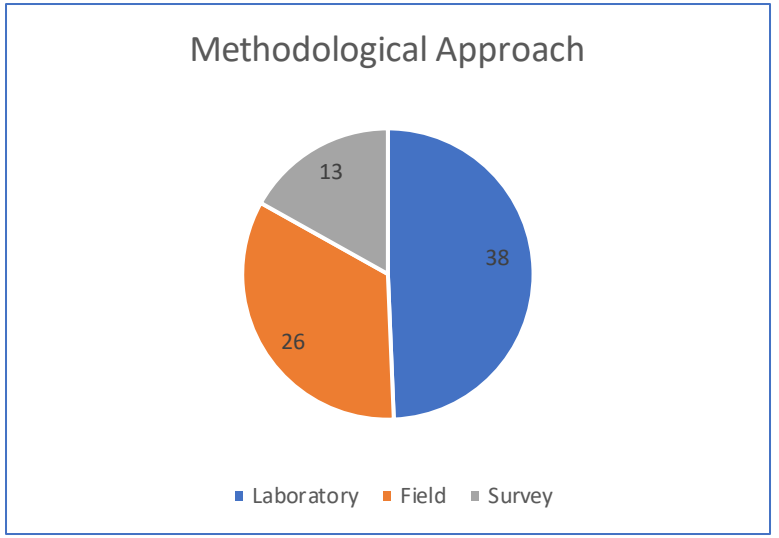
RQ3: Are there any empirical best practices per methodological approach for ensuring ecological validity in phishing experiments?

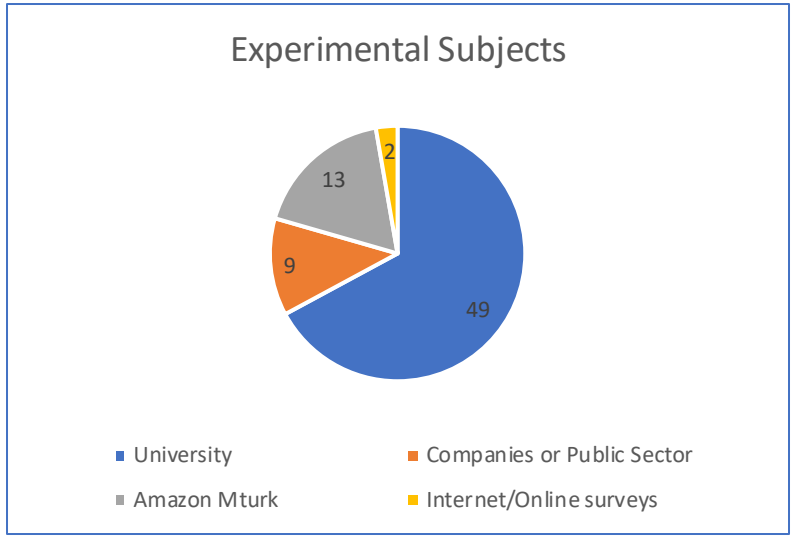
Data collection and Screening Process

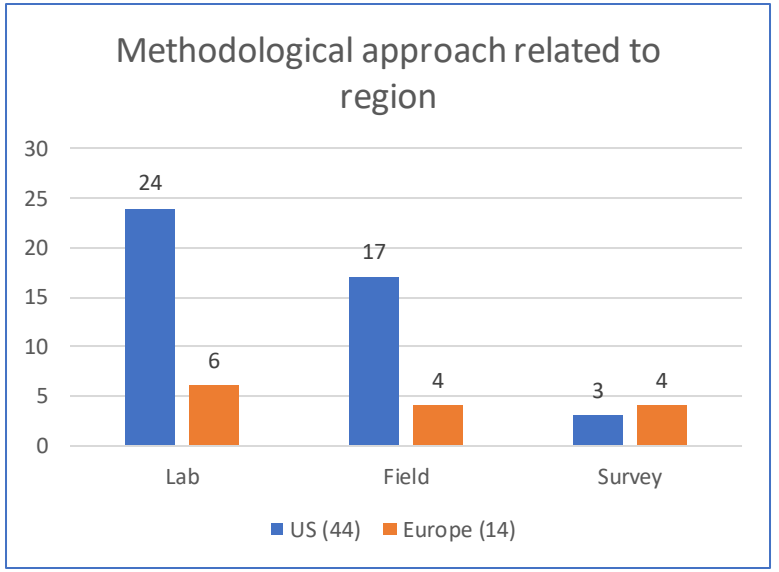


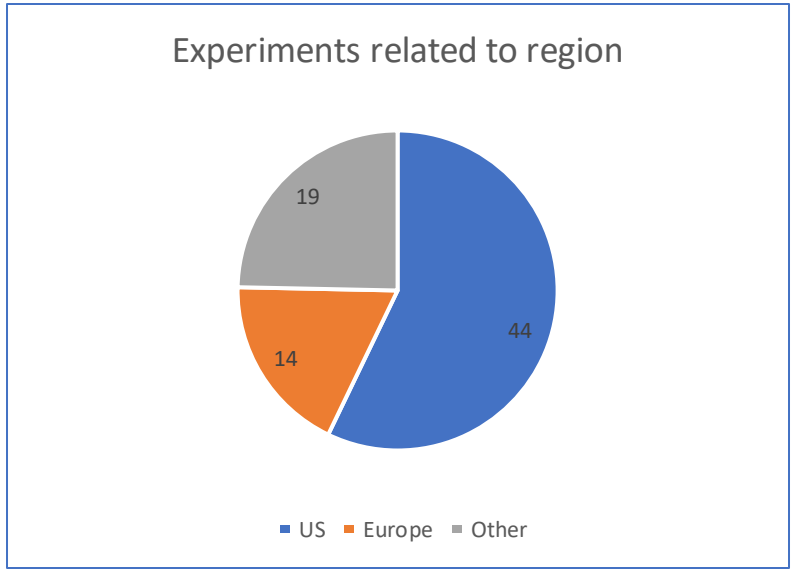
Analysis of Results

RQ1: What methodological approaches for phishing research are followed in the examined experiments?



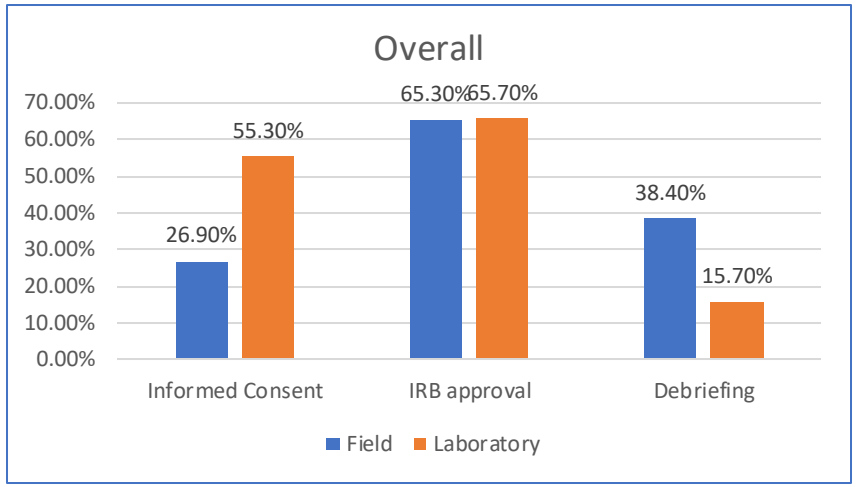


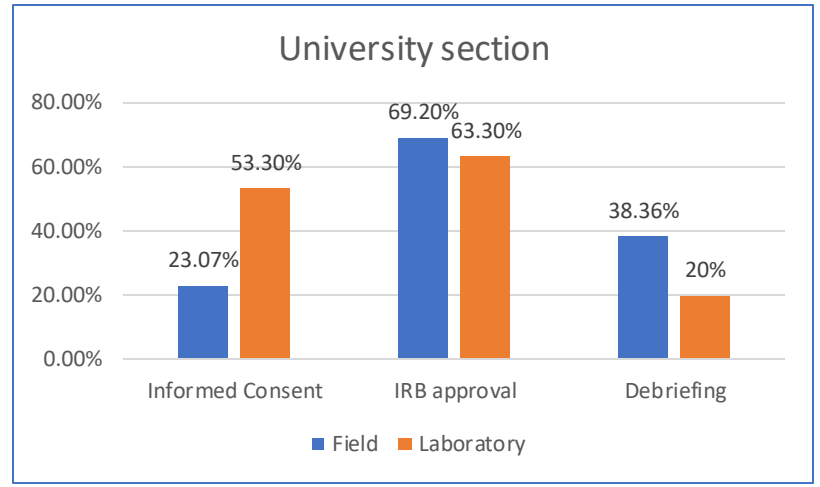


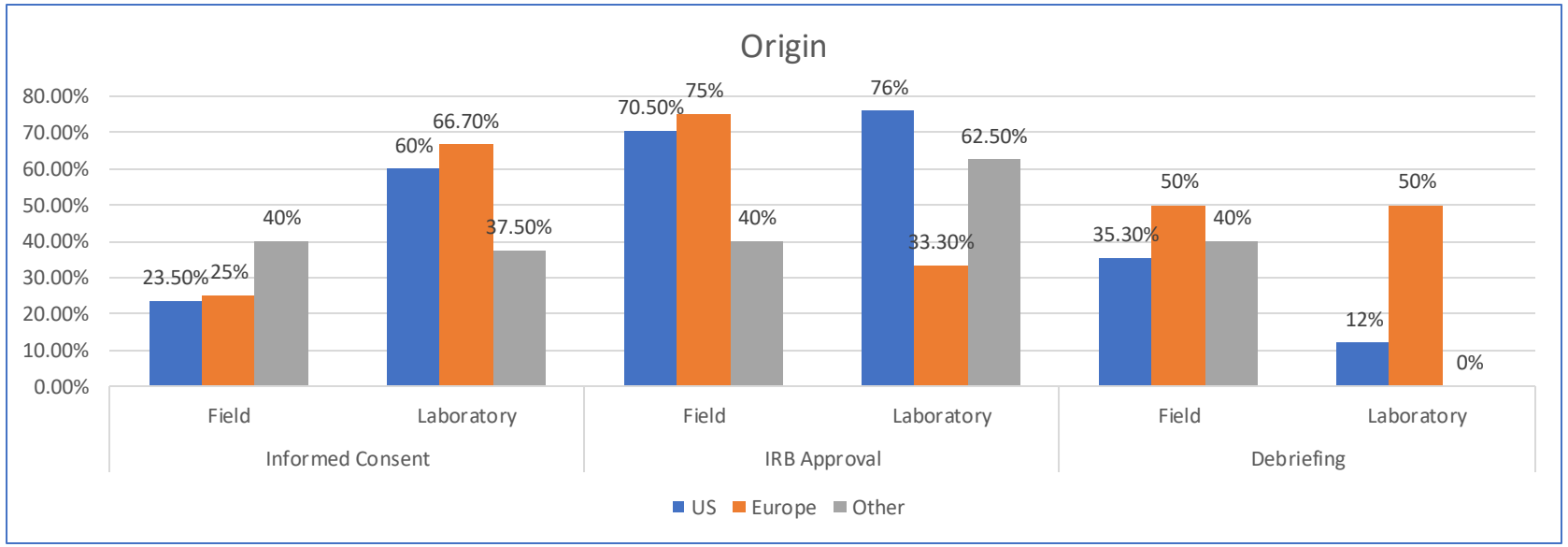


Analysis of Results

RQ2: Considering RQ1 what are the research ethics per methodological approach that are applied to experiments examined?







Analysis of Results

RQ3: Are there any empirical best practices per methodological approach for ensuring ecological validity in phishing experiments?

- Field experiments produce findings with a strong ecological validity since their environments are connected to real-world scenarios
  - Baillon A et al.
  - Nguyen et al.
  - P. K. Yeng et al.
- Laboratory experiments leading to lower scores in terms of ecological validity
  - Sarno and Neider
  - Xu et al.
  - McAlaney and Hills

Conclusion

- The majority of the experiments were conducted either in a laboratory or in a field environment
- Laboratory experiments are preferred instead of field experiments
- The percentage of those that requested and received approval from the IRB and mainly those that followed the procedure for informed consent and debriefing is rather relatively low

Suggestions

- IRBs need to assess and sanction field experiments
- Researchers should communicate with and obtain consent from their university's IRB
- In cases where phishing experiments necessitate deceit and relinquishment of informed agreement, IRBs must initially endorse such experiments considering that
  - the projected advantages of the study will surpass the expected hazards,
  - the study fulfills specific standards outlined in the regulations governing research on human subjects
  - the researchers provide a post-experiment briefing to the participants
- The members of the ethics committees along with the data protection experts and the legal professionals can contribute to a plan for supporting phishing researchers in designing studies that adhere to legal requirements

Thank you for your attention