

# Faculty of Engineering and Built Environment

Hussain Aldawood / Dr Geoffrey Skinner  
School of Electrical Engineering and Computing / Faculty of Engineering and Built Environment  
ICT Building University Drive Callaghan NSW 2308  
0451287443 / 0249854512  
[hussain.aldawood@uon.edu.au](mailto:hussain.aldawood@uon.edu.au) / [Geoff.Skinner@newcastle.edu.au](mailto:Geoff.Skinner@newcastle.edu.au)



## Information Statement for the Research Project:

### Contemporary Cyber Security Social Engineering Measures, Tools and Solutions: Explorative Interviews

Document Version 2; Dated [24/10/19]

You are invited to participate in the research project identified above which is being conducted by Hussain Aldawood, a PhD candidate from the School of Electrical Engineering and Computing at the University of Newcastle. You are being invited because you are a senior IT cyber security professional in an organization that has substantive business processes dependent on information and communication technology (ICT) systems. The research is part of Hussain Aldawood's studies at the University of Newcastle, supervised by Dr. Geoffrey Skinner from the School of Electrical Engineering and Computing.

#### ***Why is the research being done?***

Today, organizations are greatly dependent on information systems. This reliance has led to vulnerability to information security threats that put data and people at risk. Furthermore, social engineering fraud has been increasing with advancements in technology. Social engineering is defined in several studies, e.g., Orgill et al (2004), Kumar (2015), as manipulating and persuading people to disclose sensitive information through online networks or by granting access to restricted areas or systems [1, 2]. Criminals are getting more sophisticated in finding new ways to attack. As a result, organizations have been increasing their investments in cyber security initiatives to safeguard their data. On the other hand, some governments such as Australia have started legislating different laws and regulations against cyber criminals to ensure the protection of citizens and organizations from social engineering attacks and other cyber-related crimes. However, keeping up with perpetrators is challenging. Information security awareness is a crucial step towards having a secure cyber environment in which all types of computer users' (end-users, technical users, employees in different departments, etc.) skill aptitude levels can freely use technology to conduct positive and self-developing activities. This research is to find best working tools to mitigate social engineering threats beside awareness programs and then help finding reliable solutions to create such a safe work environment. The researcher would seek participants from senior IT cyber security professionals in organizations that have substantive business processes dependent on information and communication technology (ICT) systems to share their experiences of the latest practical solutions to protect from social engineering threats.

#### ***Who can participate in the research?***

We are seeking adult participants (18 years old and above) from senior IT cyber security professionals working in organizations that have substantive business processes dependent on information and communication technology (ICT) systems.

#### ***What would you be asked to do?***

Initially you will be sent an email invitation of participation that also includes this Information Statement. If you agree to participate by replying in the affirmative to the email, you will be sent a second email containing a URL Hyperlink and 6 digit code to complete an anonymous online questionnaire. The 6 digit code is only used to gain authorized (not authenticated) access to the questionnaire, and is the same non-identifiable code for all participants. The questions will be based around ones insights, opinions and experiences regarding the most up to date measures, tools and solutions against social engineering threats. We are particularly interested to know if the theoretical solutions, which we investigated from the literature, correlate with industrial and commercial solutions used to mitigate social engineering threats. We anticipate your responses will be formulated on your professional experience as it pertains to cyber security. All questions are factual and as such no sensitive or personal information will be collected in the questionnaire.

This online questionnaire will be hosted on secure infrastructure housed at the University of Newcastle, with responses stored securely in a database. The actual web server is a Research Virtual Machine sitting on a very secure sub-network behind the University firewalls. The server implements SSL and https technologies to protect the data in transit. Likewise, the database is a Microsoft SQL Server instance housed on a separate server again with the secure University of Newcastle research machine sub-network. Full data backup, retention, and recovery policies and procedures cover the research infrastructure hosting this questionnaire and its associated data.

#### ***What choice do you have?***

Participation in this research is entirely your choice and completely voluntary. Only those people who give their informed consent will be included in the project. Whether or not you decide to participate, your decision will not disadvantage you. If you do decide to participate, you may withdraw from the project at any time prior to submitting your completed

questionnaire by closing the browser window. Please note, because the completed questionnaires are not traceable to a specific user (to maintain anonymity), it is not possible to withdraw any of your individual questionnaire responses once the questionnaire has been submitted.

***How much time will it take?***

The questionnaire should take about 15 minutes to complete.

***What are the risks and benefits of participating?***

There are no anticipated risks associated with participating in this research. The collected data will be de-identified, and therefore there will be no link between you and your contribution. The findings will help contribute to the available literature on the subject, may be of benefit to find the best solutions to protect from social engineering attacks. We also cannot promise you any direct benefit from participating in this research. However, it is hoped that your contribution will potentially lead to improvements in better designing of user experiences in security related interactions with the cyber world.

***How will your privacy be protected?***

All questionnaire responses collected are anonymous, so you cannot be identified or linked to your data in any way once you have submitted your response. The online questionnaire is being hosted on secure infrastructure housed at the University of Newcastle. The actual web server is a Research Virtual Machine sitting on a very secure sub-network behind the University firewalls. The server implements SSL and https technologies to protect the data in transit. Likewise, the database is a Microsoft SQL Server instance housed on a separate server again with the secure University of Newcastle research machine sub-network. Full data backup, retention, and recovery policies and procedures cover the research infrastructure hosting this questionnaire and its associated data. The data will be kept for a minimum of 5 years, and will only be accessible to authorized members of the research team. Data will be securely destroyed in line with UON policy provisions. Please note that due to the anonymous nature of the questionnaire, you will not be able to withdraw your response after it has been submitted.

***How will the information collected be used?***

The collected data will contribute towards Hussain Aldawood's PhD thesis and may be presented in academic publications, journals or conferences.

Non-identifiable data may be also shared with other parties to encourage scientific scrutiny and to contribute to further research and public knowledge, or as required by law.

If you indicate that you would like to receive a copy of study findings, you will also be provided with a summary of the findings upon the completion of the study, which is estimated to be around mid of June of 2020. The final results of this research can be requested via emails mentioned in the top of this document. Individual participants will not be named or identified in any reports arising from the project although individual anonymous responses may be quoted.

***What do you need to do to participate?***

Please read this Information Statement and be sure you understand its contents before you consent to participate. If there is anything you do not understand, or you have questions, please contact the researcher.

If you would like to participate, please answer the questions sent to you by email and return the answers to the principal researcher or the chief investigator. Completion and submission of the email questionnaire will be taken as your implied consent to participate.

Note: Summary of findings can be requested by contacting the research team at [Hussain.aldawood@uon.edu.au](mailto:Hussain.aldawood@uon.edu.au)

***Further information***

If you would like further information please contact:

|   |   |
|---|---|
| Hussain Aldawood  | Dr Geoffrey Skinner   |
| PhD Candidate and Principal Researcher  | Chief Investigator and Supervisor   |
| Mobile: 0451287443  | Tel: (02) 4985 4512   |
| Email: <a href="mailto:hussain.aldawood@uon.edu.au">hussain.aldawood@uon.edu.au</a> | Email: <a href="mailto:geoff.skinner@newcastle.edu.au">geoff.skinner@newcastle.edu.au</a> |

**Thank you for considering this invitation.  
Your participation is highly appreciated.**

### Research Team

Hussain Aldawood  
PhD Candidate and Principal Researcher  
Mobile: 0451287443  
Email: [hussain.aldawood@uon.edu.au](mailto:hussain.aldawood@uon.edu.au)

Dr Geoffrey Skinner  
Chief Investigator and Supervisor  
Tel: (02) 4985 4512  
Email: [geoff.skinner@newcastle.edu.au](mailto:geoff.skinner@newcastle.edu.au)

### ***Complaints about this research***

This project has been approved by the University's Human Research Ethics Committee, Approval No. H-2019-0355. Should you have concerns about your rights as a participant in this research, or you have a complaint about the manner in which the research is conducted, it may be given to the researcher, or, if an independent person is preferred, to the Human Research Ethics Officer, Research Services, NIER Precinct, The University of Newcastle, University Drive, Callaghan NSW 2308, Australia, telephone (02) 49216333, email [Human-Ethics@newcastle.edu.au](mailto:Human-Ethics@newcastle.edu.au).