

論文内容の要旨

博士論文題目	Validation Agents and Persuasive Designs for Phishing Detection and Update Compliance on Smartphones
氏 名	Jema David Ndibwile

(論文内容の要旨)

Billions of smartphones and their users are vulnerable to various cyber attacks such as phishing, man-in-the-middle, and malware. Among notable reasons for these vulnerabilities are the lack of cybersecurity knowledge, lack of effective cybersecurity legislation, socioculture, socio-economic and mainly outdated (obsolete) software applications such as Operating System (OS). The desire of users to update their devices might significantly vary among users of different demographics and users in different geographic locations. However, in some attacks such as phishing, users may fall victim not only because of lack of knowledge and awareness, but also because they are not attentive enough to security indicators and visual abnormalities on the webpages they visit. This is also probably why smart device users, who have limited screen size and device capabilities than desktop users, are three times more likely to fall victim to phishing attacks.

This dissertation aims to assert the aforementioned claims by first investigating OS update behaviours and general phishing and cybersecurity awareness among different groups of smartphone users. Then, experimentally, with the use of smart eyeglasses (electro-oculographic), measures the mental effort and vigilance exhibited by users while surfing a website and while playing an Android phishing game that was developed. The results show that knowledge and awareness about phishing do not seem to have a significant impact on security behaviours, as knowledgeable participants exhibited insecure behaviours such as opening email attachments from unfamiliar senders. However, attentiveness was important as even participants with low cybersecurity knowledge could effectively identify attacks if they were reasonably attentive. The results further indicate that demographic factors such as culture, income, and geographic location highly impact behaviours of users on OS updating. Most smartphone users do not update application software on their devices despite being aware of the security implications and the concerns among those who do, vary significantly. Moreover, in the developing country settings, most users tend to avoid certain security advice and device updates because they necessitate incurring data charges that take up a high percentage of their incomes.

Based on these results, the assertion is that users are more likely to continue falling victim to phishing and other attacks due to insecure behaviours, unless persuasive designs for update

compliance and tools to lessen phishing identification burden are provided. We thus recommend implementing a lightweight algorithm into a custom Android browser for detecting phishing sites deceptively without a user interaction. The algorithm uses fake login credentials as the validation agents and monitors the destination server HTTP responses to determine the authenticity of a webpage. We present initial evaluation results of this algorithm. Lastly, we propose and evaluate the acceptability of different re-designed security notifications that integrate security advice with free information services. Additionally, we introduce the color-coded fear-appeal designs for persuading users into updating their devices' application software.

氏 名	Jema David Ndibwile
-----	---------------------

(論文審査結果の要旨)

近年、スマートフォンがひろく普及し、経済・社会活動に寄与している一方で、金銭的被害や情報漏洩などの被害も続いている。このため、スマートフォンの安全な利用法を確立することが求められている。そこで本論文では、スマートフォンの安全な利活用に関する探索的な調査を実施し、またスマートフォンにおけるセキュリティ機能および行動誘発につながる効果的なセキュリティ警告の方法を提案している。本論文の主な成果は、以下に要約される。

1. 日本とタンザニアの一般利用者を対象としたアンケート調査を行い、サイバーセキュリティに対する意識の違い、およびスマートフォンの安全な利活用に対する関心度の違いを明らかにしている。これにより、先進国のみならず途上国の利用者をも対象としたセキュリティ機能の評価の重要性を示し、また対象地域の制度や文化にあわせた行動誘発法の必要性を示している。
2. 一般利用者と IT 専門家を対象とした被験者実験を行い、フィッシングサイトの判定実験において IT に関する知識の有無にかかわらずスマートフォンの画面に対する集中度の違いが明らかな差を産むことを実証している。これにより、スマートフォンの画面に十分な注意を払うことを前提とした従来のセキュリティ対策の限界を明らかにするとともに、利用者が注意力散漫になりがちなスマートフォン利用において、セキュリティ判断を支援する機能の必要性を示している。
3. フィッシングサイトへの対策として、擬似ユーザ識別子によって自動的にログインを試み、ウェブサイトの真贋判定を支援する機能を提案し、その正確性および負荷を評価している。これにより、スマートフォンの安全な利活用のために利用者のセキュリティ判断を支援する機能が実現可能であることを実証している。

以上のように、本論文はスマートフォンの安全な利活用に対して実地調査と対照実験を行い、またこれらに基づくセキュリティ判断の支援機能を提案し、事例分析とスマートフォンへの実装によってその有効性を検証している。これらの成果は2編の学術論文および3編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。