Karlsruhe Institute of Technology

Division II – Informatics, Economics, and Society

Institute of Applied Informatics and Formal Description Methods (AIFB)

NoPhish

Security Awareness Concept: Protection from Phishing Emails and Other Fraudulent Messages

Internet fraudsters use various strategies to harm individuals, companies, or institutions. One popular and widespread method is to send them messages with dangerous content. These messages can be dangerous in different ways. They may, for example, ask the recipient to make money transfers or make (chargeable) calls and may contain dangerous links and/or dangerous attachments. Fraudulent messages can be sent in the form of emails, but also in any other form. In the case of dangerous links in e-mails, experts often speak of phishing emails.

Recognizing Dangerous Messages – and Protecting Yourself from Them

To help users better understand attacks in the form of fraudulent messages and learn how to protect themselves, the SECUSO (Security - Usability - Society) research group at KIT's Institute of Applied Informatics and Formal Description Methods (AIFB) has developed the NoPhish concept. From this concept, various measures have been derived and evaluated.

The concept comprises four topics:

- Introduction to the topic.
- Detecting implausible, fraudulent messages.
- Recognizing messages with dangerous links (including identification of the URL behind the link, structure of the URL, and tricks of the attackers).
- Detecting messages with dangerous attachments (including identification of the format of the file, list of particularly dangerous data formats, and tricks of the attackers).

The development of the NoPhish concept started at TU Darmstadt, among others, in the KMU Aware project funded by the German Federal Ministry for Economic Affairs and Energy as part of the IT Security in Business initiative and in the CRISP project funded by the German Federal Ministry of Education and Research. The concept is based on research work around the NoPhish Android app. The various measures and the concept are still being evaluated and further developed on the basis of the results. In addition, new measures are being developed. Currently, research around the NoPhish concept is ongoing in the Helmholtz Topic "Engineering Secure Systems," among others.

Nine Measures for Different Needs

So far, the NoPhish concept has been implemented and been evaluated in nine different measures varying in detail:

- Flyer with a general introduction to the topic and the most important rules for recognizing fraudulent messages.
- Training materials on the subject of fraudulent messages with many examples, further information, and exercises serving for self-study or as a starting point for disseminating knowledge, for example through presentations in the company's own organization.
- E-learning on the topic of fraudulent messages with many examples and further information for self-study. The e-learning module is made up of various levels; to advance to the next level, users have to pass a short quiz.
- Explainer videos developed together with video artist Alexander Lehmann. In less than five minutes each, these give a general introduction and explain the most important rules for identifying fraudulent messages.
- Self-testing quiz for recognizing fraudulent messages.
- Online game "Phishing Master," the somewhat different serious game for recognizing fraudulent messages.
- Info card with the most important rules for identifying phishing and other fraudulent messages in pocket format.
- Poster with the most important rules for identifying phishing and other fraudulent messages to hang up in the office or in central places.
- Challenge poster with different forms of (fraudulent) messages and the question: Is this message trustworthy? With the help of a QR code, the user can answer this question and will then land on a page showing the resolution and further tips for recognizing phishing and other fraudulent messages.

Objectives and Evaluation

The measures aim to make users aware of the dangers and at the same time teach them how to protect themselves. The two compact measures, poster and info card, serve more as a refresher. The quiz is suitable for checking the current level of knowledge. Unlike many other security awareness measures available on the Internet or offered by companies, the NoPhish measures have been empirically evaluated with regard to the achievement of objectives; the results have been published in scientific papers. The researchers evaluate goal achievement by measuring what percentage of messages seen during the study are correctly classified as phishing or legitimate messages.

Guidance on different use scenarios and rights of use can be found at https://secuso.aifb.kit.edu/downloads/Nutzungsszenarien.pdf

Companies and institutions considering the use of simulated phishing campaigns can find an analysis at https://publikationen.bibliothek.kit.edu/1000119662/74582106

Karlsruhe Institute of Technology (KIT)
Institute of Applied Informatics and
Formal Description Methods (AIFB)
Prof. Dr. Melanie Volkamer
Kaiserstr. 89
76133 Karlsruhe
Email: melanie.volkamer@kit.edu
Phone: +49 721 608-45045
www.aifb.kit.edu/web/Melanie_Volkamer

SECUSO
SECURITY · USABILITY · SOCIETY

Karlsruhe Institute of Technology (KIT) · President Professor Dr.-Ing. Holger Hanselka · Kaiserstraße 12 · 76131 Karlsruhe, Germany · www.kit.edu