Karlsruher Institut für Technologie

Bereich II – Informatik, Wirtschaft und Gesellschaft

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

NoPhish

Security Awareness Konzept: Schutz vor Phishing- E-Mails und anderen betrügerischen Nachrichten

Internetbetrüger nutzen verschiedene Strategien, um Personen, Unternehmen oder Einrichtungen zu schaden. Eine beliebte und weit verbreitete Methode besteht darin, diesen Nachrichten mit gefährlichen Inhalten zu schicken. Dabei können die Nachrichten auf unterschiedliche Art und Weise gefährlich sein. Die Nachricht kann die Empfängerin oder den Empfänger auffordern, Überweisungen vorzunehmen oder (kostenpflichtige) Anrufe zu tätigen. Sie kann gefährliche Links und/oder gefährliche Anhänge enthalten. Betrügerische Nachrichten lassen sich in Form von E-Mails, aber auch in jeder anderen Form verschicken. Im Fall von gefährlichen Links in E-Mails sprechen Fachleute oft von Phishing-E-Mails.

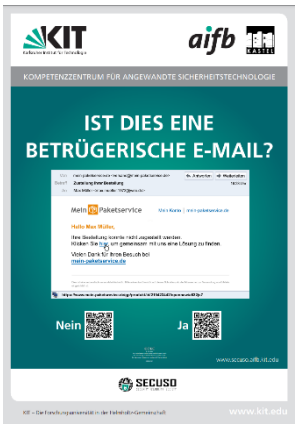

Abbildung 1

Gefährliche Nachrichten erkennen - und sich davor schützen

Damit Nutzerinnen und Nutzer Angriffe in Gestalt von betrügerischen Nachrichten besser verstehen und lernen, wie sie sich schützen können, hat die Forschungsgruppe SECUSO (Security - Usability - Society) am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des KIT das NoPhish Konzept entwickelt und daraus verschiedene Maßnahmen abgeleitet und evaluiert.
Das Konzept umfasst vier Themenbereiche:

- Einführung in das Thema
- Erkennen von unplausiblen, betrügerischen Nachrichten
- Erkennen von Nachrichten mit gefährlichen Links (einschließlich Ermitteln der URL hinter dem Link, Aufbau der URL und Tricks der Angreifer)
- Erkennen von Nachrichten mit gefährlichen Anhängen (einschließlich Ermitteln des Formats der Datei, Liste von besonders gefährlichen Dateiformaten und Tricks der Angreifer)

Abbildung 2

Die Entwicklung des NoPhish Konzepts startete an der TU Darmstadt, unter anderem im vom Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative IT-Sicherheit in der Wirtschaft geförderten Projekt „KMU Aware“ sowie im vom Bundesministerium für Bildung und Forschung geförderten CRISP Projekt. Das Konzept wiederum ist auf Forschungsarbeiten rund um die NoPhish Android App aufgebaut. Die verschiedenen Maßnahmen sowie das Konzept werden nach wie vor evaluiert und auf der Basis der Ergebnisse weiterentwickelt. Außerdem werden neue Maßnahmen erarbeitet. Derzeit läuft die Forschung rund um das NoPhish Konzept unter anderem im Helmholtz Topic „Engineering Secure Systems“.

Abbildung 3

Bislang zehn Maßnahmen für unterschiedliche Bedürfnisse

Das NoPhish Konzept wurde bisher in zehn verschiedenen Maßnahmen implementiert und evaluiert. Diese sind unterschiedlich detailliert. Konkret sind dies die folgenden Maßnahmen:

- Flyer mit einer allgemeinen Einführung ins Thema und den wichtigsten Regeln zum Erkennen von betrügerischen Nachrichten
- Schulungsunterlagen zum Thema betrügerische Nachrichten mit vielen Beispielen, weiterführenden Informationen und Übungsaufgaben zum Selbststudium oder als Ausgangspunkt für eine Verbreitung des Wissens, beispielsweise durch Vorträge im eigenen Unternehmen
- E-Learning zum Thema betrügerische Nachrichten mit vielen Beispielen und weiterführenden Informationen zum Selbststudium. Das E-Learning besteht aus verschiedenen Levels und um ins jeweils nächste Level zu gelangen, müssen Nutzerinnen und Nutzer ein kleines Quiz bestehen.
- Erklärvideos, entwickelt gemeinsam mit dem Videokünstler Alexander Lehmann, die in jeweils weniger als fünf Minuten eine allgemeine Einführung geben und die wichtigsten Regeln zur Erkennung von betrügerischen Nachrichten erklären
- Quiz zum Erkennen betrügerischer Nachrichten, mit dem Nutzerinnen und Nutzer sich selbst testen können

- Online-Spiel „Phishing Master“, das etwas andere Serious Game zum Erkennen betrügerischer Nachrichten
- Infokarte mit den wichtigsten Regeln zum Erkennen von Phishing und anderen betrügerischen Nachrichten im Hosentaschen-Format
- Poster mit den wichtigsten Regeln zum Erkennen von Phishing und anderen betrügerischen Nachrichten zum Aufhängen im Büro oder an zentralen Orten. Ein Beispiel ist in 4 zu sehen
- Challenge Poster mit verschiedenen Formen von (betrügerischen) Nachrichten und der Frage: Ist diese Nachricht vertrauenswürdig? Mithilfe eines QR-Codes kann der Nutzer diese Frage beantworten und landet dann auf einer Seite mit der Auflösung und weiteren Tipps zum Erkennen von Phishing und anderen betrügerischen Nachrichten. Ein Beispiel ist in Abbildung 1 zu sehen.
- STAR, ein humanoider Roboter, der betrügerischen Nachrichten interaktiv mit Nutzern bespricht. Beispielhaft ist STAR auf Abbildung 3 zu sehen. Auf der Seite finden Sie auch ein Video eines möglichen Ablaufs mit STAR.

Möglichkeiten zur Verknüpfung verschiedener Maßnahmen

Wir haben bereits verschiedene Vorschläge aufgestellt, wie eine Kombination der verschiedenen Maßnahmen aussehen könnte. Ein Beispiel dafür ist ein eher leichteres Programm. Leicht meint hier, dass es sich eher um kleinere und kurze Maßnahmen handelt. Es gibt aber auch weitere Programme – mehr Informationen finden Sie hier.

Ziele und Evaluation

Die Maßnahmen zielen darauf, Nutzerinnen und Nutzer für die Gefahren zu sensibilisieren und ihnen gleichzeitig zu vermitteln, wie sie sich konkret schützen können. Die beiden kompakten Maßnahmen Poster und Infokarte dienen eher der Auffrischung des Wissens. Das Quiz eignet sich zum Überprüfen des aktuellen Wissensstands. Anders als viele andere im Internet verfügbaren oder von Firmen angebotenen Security Awareness Maßnahmen sind die NoPhish Maßnahmen empirisch hinsichtlich der Zielerreichung evaluiert; die Ergebnisse sind in wissenschaftlichen Arbeiten veröffentlicht. Die Zielerreichung evaluieren die Forschenden, indem sie messen, wie viel Prozent der im Rahmen der Studie gesehenen Nachrichten korrekt als Phishing oder als legitime Nachricht klassifiziert werden.

Abbildung 4

Innovation

Das Besondere an dem NoPhish Konzept sind folgende Aspekte:

- Die Maßnahmen des NoPhish Konzept z.B. Videos, E-Learning oder Schulungsmaterial sind in zahlreichen wissenschaftlichen Arbeiten auf ihre Effektivität evaluiert worden. Nicht nur auf die Effektivität direkt nach der Maßnahme, sondern auch auf die langfristige Nutzung (bis zu 6 Monate) und Abfolge verschiedener Maßnahmen nacheinander (bis zu 12 Monate).
- Durch die verschiedenen Maßnahmen mit verschiedenen Medialen Formen kann für viele Zielgruppen eine passende Maßnahme im passenden Medium ausgewählt werden. Auch können die Maßnahmen miteinander oder nacheinander verzahnt werden. Durch die verschiedenen Maßnahmen können Nutzende mit verschiedenen Bedürfnissen und Präferenz sich aus der breiten Palette das für sie geeignetste Maßnahme aussuchen. Ebenso steht bereits eine Auswahl an Maßnahmen sowohl in der deutschen, als auch in der englischen Sprache zur Verfügung z.B. die Flyer oder Videos.
- Die Maßnahmen haben keine Voraussetzung an Wissen für die Nutzenden. Sie versuchen entsprechend bereits die grundlegende Awareness zu schaffen und darauf aufbauen das notwendige Wissen, um betrügerische von legitimen Nachrichten zu unterscheiden.
- Alle Maßnahmen bzw. Materialien sind kostenfrei auf unserer Webseite bzw. Video-Plattformen verfügbar. Dementsprechend können Bürgerinnen und Bürger jederzeit die Maßnahmen selbständig sich anschauen oder wiederholen.

Bisherige Events (Auswahl)

- Hannover Messe 2022

Auf der Hannover Messe 2022 haben wir mit STAR, dem Phishing Quiz und dem Spiel Phishing Master einen Teil der NoPhish-Materialien vorgestellt. Unser Awareness Roboter STAR hatte das Vergnügen sowohl den Präsidenten des KIT, Prof. Hanselka, als auch Bundeskanzler Olaf Scholz begrüßen zu dürfen. (Abbildung 3)

- Triangel Open Space 2022

Der Roboter STAR hat im Triangel Open Space in Karlsruhe über das Erkennen von betrügerischen Nachrichten informiert. (Abbildung 5)

Abbildung 5

- Bunde Nacht der Digitalisierung 2022

Die Bunte Nacht der Digitalisierung fand im Juli in Karlsruhe statt. Dort haben wir ein Quiz zum Erkennen von Phishing-URLs durchgeführt bei dem Teilnehmer und Teilnehmerinnen Gutscheine gewinnen konnten. (Abbildung 6)

- Benefiz-Cybersicherheitskurs 2022

SECUSO veranstaltete im Mai 2022 einen Online-Cybersicherheitskurs mit dem Thema Erkennen von Phishing E-Mails, betrügerischen Nachrichten und Fake News, u.a. in Sozialen Medien. Die Teilnahme war kostenlos, stattdessen wurde um eine freiwillige Spende für die Ukraine gebeten.

Abbildung 6

- Digitaltag 2022

Auf dem Digitaltag 2022 haben wir einen digital Selbstverteidigungskurs angeboten, in dem über Phishingmethoden und die Erkennung von Phishingangriffen aufgeklärt wurde.

- Safer Internet Day 2022

Neben der erfolgreichen Prämiere unseres dritten NoPhish-Videos, stand auf dem diesjährigen Safer Internet Day das Thema Authentifizierungsmechanismen für Kinder im Fokus. (Abbildung 7)

Abbildung 7

- Polizei Präsidium Südhessen Kooperation

Nach zwei erfolgreichen Workshops für die Polizei Hessen zum Thema Phishing im Jahr 2019 wurden im Rahmen einer Online-Fortbildung zum Thema Cybercrime der United Nations African Union Mission in Darfur (UNAMID) auch die NoPhish-Materialien behandelt. Das Polizeipräsidium Südhessen setzte die NoPhish-Videos ein, um Miterarbeiterinnen und Mitarbeiter im Umgang mit E-Mails zu schulen.

Zahlen, Daten, Fakten

Quiz zum Erkennen betrügerischer Nachrichten	29371 Aufrufe und 6170 komplette Durchläufe
Erklärvideos	ca. 15000 Aufrufe
Online-Spiel „Phishing Master“	751 Highscore Einträge
E-Learning zum Thema betrügerische Nachrichten	3920 Aufrufe

Stand: Juni 2022

Aktuelle Referenzanwender und Organisation, die auf unser Material verweisen

Behörden/Institutionen

- Bundeskanzleramt
- Bundesverwaltungsamt
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- United Nations African Union Mission in Darfur (UNAMID)
- Polizeipräsidium Einsatz in Baden-Württemberg
- Polizeipräsidium Südhessen
- Landesamt für Geoinformation und Landesvermessung Niedersachsen (LGLN)
- Verbraucherzentrale NRW e.V.
- Artilleriebataillon 295 der Bundeswehr
- Stadt Dessau-Roßlau
- Stadt Hamm
- Landkreis Marburg-Biedenkopf
- Stadtwerke Jena
- Amt für Gemeindedienst in der Evang.-Luth. Kirche in Bayern
- Landeshauptstadt Stuttgart
- Stadt Elmshorn

Hochschulen

- Karlsruher Institut für Technologie
- Eberhard Karls Universität Tübingen
- Ruhr-Universität Bochum
- Informations- und Mediendienste (ZIM) der Universität Duisburg-Essen
- Hochschule Koblenz
- Universität Würzburg
- Technische Universität Braunschweig
- Hochschule Konstanz (HTWG)
- Fernuniversität Hagen
- Hochschule Worms
- Universität Bamberg
- Universität Mannheim
- FH Münster
- Universität Freiburg
- Universität zu Köln
- Pädagogische Hochschule Karlsruhe
- Technische Universität Darmstadt
- TU Dortmund

Unternehmen

- Berliner Verkehrsbetriebe
- ASAP Holding GmbH
- HEAG
- Bayerische Gesellschaft für Innovation und Wissenstransfer mbH
- MARKANT Handels- und Industriewaren-Vermittlungs AG
- Eligo
- Könitz Porzellan GmbH
- Lemo Maschinenbau GmbH
- AVW Unternehmensgruppe
- Bayern1 Radio
- Welivesecurity by ESET

"Ich bin der Forschungsgruppe SECUSO am KIT in Karlsruhe besonders dankbar, denn sie stellen sehr gute Awareness-Materialien zur Verfügung, um sich gegen Betrüger im Internet zu schützen." (Arne Schönbohm, Präsident des BSI)

Veröffentlichungen (Auswahl)

- Phishing awareness and education – When to best remind?
  Berens, B. M.; Dimitrova, K.; Mossano, M.; Volkamer, M. 2022. Symposium on Usable Security and Privacy (USEC)
- NoPhish-Challenge-Karten – Evaluation in der Praxis
  Aldag, L.; Berens, B.; Burgdorf, M.; Lorenz, A.; Thiery, M.-C.; Volkamer, M. 2021. Datenschutz und Datensicherheit - DuD
- Evaluation der interaktiven NoPhish Präsenzschulung
  Berens, B.; Aldag, L.; Volkamer, M. 2021. Mensch und Computer 2021 Workshopband.
- An investigation of phishing awareness and education over time: When and how to best remind users.
  Reinheimer, B. M.; Aldag, L.; Mayer, P.; Mossano, M.; Düzgün, R.; Lofthouse, B.; von Landesberger, T.; Volkamer, M. 2020. Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS)
- Erklärvideo “Online-Betrug” – Nach nur fünf Minuten Phishing E-Mails nachweislich signifikant besser erkennen.
  Volkamer, M.; Renaud, K.; Reinheimer, B.; Rack, P.; Ghiglieri, M.; Gerber, N.; Mayer, P.; Kunz, A. 2019. IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung: Tagungsband zum 16. Deutschen IT-Sicherheitskongress
- Phishing Detection: Developing and Evaluating a Five Minutes Security Awareness Video
  Volkamer, M.; Renaud, K.; Reinheimer, B. M.; Rack, P.; Ghiglieri, M.; Mayer, P.; Kunz, A.; Gerber, N. 2018. Trust, Privacy and Security in Digital Business - 15th International Conference (TrustBus)

Abschlussarbeiten

Masterarbeiten:

- Lisa Stiefvater (betreut von Prof. Dr. Melanie Volkamer und Benjamin Reinheimer): Analysing and comparing phishing education/awareness videos
- Katerina Dimitrova (betreut von Prof. Dr. Melanie Volkamer und Benjamin Reinheimer): Evaluation of the effectiveness of the Ilias training on fraudulent messages.
- Gamze Canova und Clemens Bergmann (betreut von Prof. Dr. Melanie Volkamer, Prof. Ralf Tenberg und Arne Renkema-Padmos): Development and Evaluation of a Phishing Education App.

Bachelorarbeiten:

- Antonia Gebhardt (betreut von Prof. Dr. Melanie Volkamer und Benjamin Reinheimer): Vergleich von verschiedenen Phishing Awareness Materialien – eine Effektivitäts- und Effizienzanalyse.
- Alexander Thiebes (betreut von David Kelm und Prof. Dr. Melanie Volkamer): Entwicklung einer Anti-Phishing Landing Page.
- Alexandra Kunz (betreut von Prof. Dr. Melanie Volkamer und Paul Gerber): Teachable Moments in der IT-Sicherheit - Klassifizierung und Anwendungsbereiche.
- Henning Stecher (betreut von Prof. Dr. Melanie Volkamer, Michaela Kauer und Prof. Dr. Ralph Bruder): Qualitative evaluation of a website for phishing education.

Karlsruher Institut für Technologie (KIT)
Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)
Prof. Dr. Melanie Volkamer
Kaiserstr. 89
76133 Karlsruhe
E-Mail: melanie.volkamer@kit.edu
Telefon: +49 721 608-45045
www.aifb.kit.edu/web/Melanie_Volkamer