Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

NoPhish – Internetbetrug spielend erkennen lernen

Informatiker der TU Darmstadt entwickeln Lernspiel-App zur Phishing-Erkennung

Darmstadt, 15. Juni 2015. Der Begriff „Phishing“ beschreibt Tricks, mit denen Betrüger Internetnutzern geheime Daten entlocken. Wie die Betrüger vorgehen und wie die Nutzer sich vor den gängigsten Methoden schützen können, erklären IT-Sicherheitsfachleute der TU Darmstadt in der spielerischen Android-App „NoPhish“.

Passwörter, Kontodaten, Kreditkartendaten, Transaktionsnummern (TANs) – hinter diesem Fang sind sogenannte Phisher her. Ihre Köder sind gefälschte E-Mails und Webseiten, die täuschend echt das von Banken oder Online-Diensten genutzte Design nachahmen. Getäuschte Internetnutzerinnen und -nutzer werden dazu verleitet, geheime Daten einzugeben, um beispielsweise eine angedrohte Sperrung ihres Kontos zu verhindern. Die gewonnenen Daten werden dann von den Phishern missbraucht, um dem Opfer finanziell zu schaden oder dessen Identität für zwielichtige Geschäfte einzunehmen. Zielgruppe der Angriffe sind alle Internetnutzerinnen und -nutzer, nicht nur besonders vermögende Personen. Die Betrüger versenden Millionen Phishing-E-Mails, so dass schon ein geringer Prozentsatz getäuschter Nutzerinnen oder Nutzer die Methode erfolgreich macht. Zuverlässig erkennen lassen sich Phishing-Angriffe nur durch die Überprüfung der Webadresse (URL).

Mit der kostenlosen Android-App „NoPhish“ können Internetnutzerinnen und -nutzer spielerisch lernen, wie sie Webadressen richtig lesen und auf Phishing-Angriffe überprüfen können. Das Spiel beginnt mit einer leicht verständlichen Einführung über Phishing-Methoden und den Aufbau von Webadressen. Darauf folgen neun interaktive Levels, in denen die Spielerinnen und Spieler verschiedene Tricks von Phishern kennenlernen. So lernen sie in kurzer Zeit, echte Webadressen von Fälschungen zu unterscheiden. Durch den Einsatz von Übungen mit Wiederholungen und mit direktem und positivem Feedback wollen die Wissenschaftler und Wissenschaftlerinnen den Lernerfolg optimieren. Feedback zu Falsch-Eingaben gibt die Vibrationsfunktion des Smartphones. Damit die Spielerinnen und Spieler sich mit anderen messen können, ist „NoPhish“ an den Google Play Game Service angebunden. Die App ist kostenlos im Google PlayStore erhältlich und benötigt keinen Zugriff auf Daten oder Dienste des Smartphones oder Handys. Neben dem Zugriff auf die Vibrationsfunktion ist lediglich eine Berechtigung für den Internetzugriff erforderlich, um den Spielstand über Google PlayStore zu synchronisieren und so gegen andere zu spielen.

„NoPhish“ wurde im Rahmen einer Masterarbeit von Clemens Bergmann und Gamze Canova am Fachgebiet SecUSo (Security, Usability und

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Silke Paradowski
Tel. 06151 16 - 20019
Fax 06151 16 - 23750
paradowski.si@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit in der Wirtschaft

TECHNISCHE UNIVERSITÄT DARMSTADT

Society) des Fachbereichs Informatik der TU Darmstadt unter Betreuung von Prof. Dr. Melanie Volkamer und Prof. Dr. Ralf Tenberg entwickelt. Im Rahmen der Forschung am Fachgebiet SecUSo wurde die App in einer mehrstufigen Benutzerstudie evaluiert. Es konnte gezeigt werden, dass die Erkennung von Phishing-Webseiten signifikant gesteigert wird. Weitere Erkenntnisse aus den Benutzerstudien sind in die Weiterentwicklung der App eingeflossen.

Die Wissenschaftlichen Erkenntnisse im Kontext von „NoPhish“ wurden im Rahmen des ESORICS Workshops „10th International Workshop on Security and Trust Management“ und des NDSS Workshops „Usable Security 2015“ veröffentlicht und wurden im Rahmen des IFIP Sec Workshops „9th World Conference on **I**nformation **S**ecurity **E**ducation“ im Mai in Hamburg vorgestellt.

App-Download:
https://play.google.com/store/apps/details?id=de.tudarmstadt.informatik.secuso.phishedu2

MI-Nr. 38/2015, Anne Grauenhorst