ID: 276 / EPS10: 3
Einzelbeitrag
Themen: Empirische Bildungsforschung
Stichworte: IT-Sicherheitsbewusstheit, IT-Sicherheit, spielbasiertes Lernen, Spiel, Motivation

Förderung von IT-Sicherheitsbewusstheit durch spielbasiertes Lernen – eine experimentelle Studie

Dr. Michael Sailer[1], Carina Hoppenz[1], Dr. Kristian Beckers[2], Dr. Sebastian Pape[3]
[1]Ludwig-Maximilians-Universität München, Deutschland; [2]Social Engineering Academy (SEA) GmbH; [3]Chair of Mobile Business & Multilateral Security, Goethe-Universität, Deutschland

Ziele oder Fragestellungen im Kontext des theoretischen Rahmens und Forschungsstandes

IT-Sicherheit nimmt eine zunehmend zentrale Bedeutung in unserem Alltag und in unserem Arbeitsleben ein. Auch die KMK (2016) betont im Rahmen der Auseinandersetzung mit Medienkompetenzen das Thema „Schützen vor Risiken in technischer, datenschutzrechtlicher und privater Hinsicht“ und fordert einen kritischen und reflektierten Umgang mit digitalen Ressourcen. Hierbei ist es von besonderer Wichtigkeit – im Sinne einer proaktiven Sicherheitsbewusstheit – Hinweise auf mögliche sicherheitsbezogene Gefahren zu erkennen und diese für das eigene Handeln zu berücksichtigen (Egelman & Peer, 2015). Ziel der Studie ist es zu untersuchen, inwieweit ein spielbasiertes Training IT-Sicherheitsbewusstheit fördern kann. Im Spiel werden Angriffe auf die eigene IT-Sicherheit simuliert, vor denen sich der Lerner mit der richtigen Taktik verteidigen muss. Solche Angriffe, die zumeist die Ausbeutung von Vertrauen mit dem Ziel Informationen zu erhalten, anstreben, werden als Social-Engineering bezeichnet.

Methodik

In der Studie wird im Rahmen eines experimentellen Between-Subjects-Designs untersucht, inwieweit sich ein spielbasiertes online Training im Vergleich zu einem videobasierten online Training auf die IT-Sicherheitsbewusstheit und das deklarative sowie anwendungsorientierte IT-Sicherheitswissen auswirken. Eine Stichprobe von *N*=200 soll rekrutiert werden. IT-Sicherheitsbewusstheit, deklaratives und anwendungsorientiertes Wissen werden über Single-Choice-Fragen, Selbsteinschätzungen sowie Situational Judgements erhoben. Als Mediatoren werden intrinsische Motivation sowie die Erfüllung von psychologischen Grundbedürfnissen aufgenommen. Vorwissen und IT-Sicherheitsbewusstheit vor der Intervention werden darüber hinaus als Kovariate in die Untersuchung aufgenommen.

Ergebnisse bzw. Schlussfolgerungen

Die Durchführung der Studie erfolgt im Juni 2017. Ergebnisse liegen zur Tagung vor und werden präsentiert. Es wird erwartet, dass sich ein spielbasiertes online Training im Vergleich zu einem videobasierten online Training positiv auf die IT-Sicherheitsbewusstheit, das anwendungsorientierte IT-Sicherheitswissen sowie motivationale Variablen auswirken. Im Rahmen von videobasierten Trainings wird zumeist auf direkte Instruktion zurückgegriffen, die kaum konstruktive und interaktive Lernaktivitäten ermöglicht (Chi & Wylie, 2014), welche vor allem für das anwendungs- und handlungsorientierte Schützen vor (digitalen) Gefahren notwendig sind.

Zusammenfassung für das Programm

IT-Sicherheit nimmt eine zunehmend zentrale Bedeutung in unserem Alltag und in unserem Arbeitsleben ein. Im Rahmen dessen ist es von besonderer Wichtigkeit, Hinweise auf mögliche sicherheitsbezogene Gefahren zu erkennen und diese für das eigene Handeln zu berücksichtigen (Egelman & Peer, 2015). Ziel der Studie ist es zu untersuchen, inwieweit ein spielbasiertes Training IT-Sicherheitsbewusstheit fördern kann. Im Spiel werden Social-Engineering Angriffe auf die eigene IT-Sicherheit simuliert, vor denen sich der Lerner mit der richtigen Taktik verteidigen muss. Dieses spielbasierte online Training wird in einem experimentellen Between-Subjects-Designs mit einem videobasierten online Training verglichen. Eine Stichprobe von *N*=200 soll rekrutiert werden. Als Mediatoren werden intrinsische Motivation sowie die Erfüllung von psychologischen Grundbedürfnissen aufgenommen. Es wird erwartet, dass sich ein spielbasiertes online Training im Vergleich zu einem videobasierten online Training positiv auf die IT-Sicherheitsbewusstheit, das anwendungsorientierte IT-Sicherheitswissen sowie motivationale Variablen auswirken. Im Rahmen von videobasierten Trainings wird zumeist auf direkte Instruktion zurückgegriffen, die kaum konstruktive und interaktive Lernaktivitäten ermöglicht (Chi & Wylie, 2014), welche vor allem für das anwendungs- und handlungsorientierte Schützen vor (digitalen) Gefahren notwendig sind.

Literaturangaben

Chi, M. T., & Wylie, R. (2014). The ICAP framework: Linking cognitive engagement to active learning outcomes. Educational Psychologist, 49(4), 219-243.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (S. 2873-2882). ACM.

KMK (Ständige Konferenz der Kultusminister der Länder der Bundesrepublik Deutschland). (2016). Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf, letzter Aufruf 30.04.17.