Zürcher Hochschule
für Angewandte Wissenschaften

zh aw School of Engineering

Der Faktor Mensch - Erkenntnisse über effektives Anti-Phishing Training

Prof. Dr. Bernhard Tellenbach
Schwerpunktleiter Information Security
Insitutu für angewandte Informationstechnologie

Motivation

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

98%

der Cyber Angriffe beinhalten Social Engineering

Phishing ist verantwortlich für…

90%

der Malware Infektionen

72%

der Vorfälle mit gestohlenen resp. geleakten Daten

Motivation, Problemstellung und Lösungsansatz

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Viele Firmen haben inzwischen Awareness Programme
- Dies sollten möglichst wirksam gestaltet werden

- Ziel:
  - Erkenntnisse über für die Wirksamkeit eines Programms relevante Parameter
  - Erkenntnisse zu was gegenüber aktuellen Programmen geändert werden müsste

- Ansatz:
  - Meta-analyse existierender Fachliteratur (insb. Studien)

Methodik – «Datenbasis»

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Keyword Suche in Datenbanken für wissenschaftlichen Publikationen (IEEE, ACM, ScienceDirect, Wiley and GS)
- Filterung der rund 700 Paper:
  - Peer-reviewed (Qualität/Vertrauen)
  - Experimente:
    - Gruppengrösse >20
  - Experimente mit Training:
    - Kontrollgruppe muss vorhanden sein
- Geneue inhaltliche Analyse der 80 verbleibenden Arbeiten:
  - Welche trainingsform und welche parameter funktionnieren am besten?
  - Fokus auf «embedded training»

Methodik – Kategorisierung

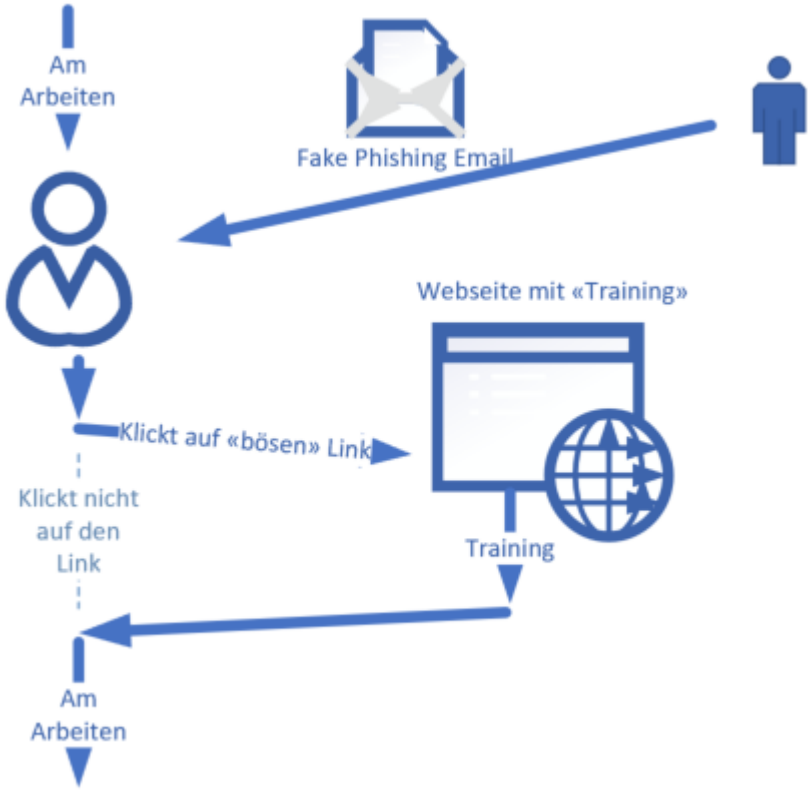
Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Welche Fragen werden untersucht?
- Mehrere Paper sollten die Frage behandeln
  - Ist die Antwort dieselbe?
- Identifikation solcher Themen/Fragen => Kategorie
  - Training impact
  - Target group impact
  - Email content and structure
  - Feedback
  - Knowledge retention

Category	Number of surveyed publications
Training Impact	24
Target Group Impact	37
Email Content and Structure	12
Feedback	18
Knowledge Retention	10

Training Impact

- Kernfrage:
  - Macht ein Anti-Phishing Trainig einen Unterschied?
- Ja, aber in unterschiedlichem Ausmaß.
- Interessantes Ergebnis:
  - Es gibt «nicht trainierbare» Benutzer
    - User, die immer klicken
    - User, die nie klicken
- Gute Trainingsergebnisse:
  - «Embedded Training», idealerweise mit initialem Kurs



Target Group Impact

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Viele verschiedene «Zielgruppen» wurden untersucht:
  - Alter, Geschlecht, Technikaffinität, extrovertierte vs. introvertierte Personen, Expertise im Umgang mit Email, ...
  - Insbesondere kognitive / psychologische Faktoren
- Alter, Geschlecht, Häufigkeit von Online-Aktivitäten und Technikaffinität: gemischte Ergebnisse (z.T. widersprüchlich)
- Ein möglicher erfolgsversprechender Ansatz:
  - Training aller Mitarbeitenden mit demselben
  - Zweiter Schritt: Differenzierung basierend auf dem Trainingserfolg durch Nutzung von Modellen wie Suspicion Cognition Automaticity Model (SCAM) oder dem Cyber Risk Index (CRI)

Email Content and Structure

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Die visuelle Erscheinung eines Emails ist wichtiger als die verwendeten Worte
  - Ein Effekt: Unser Gehirn «erkennt» Worte unabhängig von der Reihenfolge der Buchstaben solange Anfangs- und Endbuchstabe korrekt sind.
  - Thema und Inhalt müssen zu den Erwartungen an ein Email passen

Email Content and Structure (forts.)

Zürcher Hochschule für Angewandte Wissenschaften
zh aw School of Engineering

- Was sind «Hinweise» die Benutzer verwenden, um Phishing-Emails zu identifizieren?
- Deren Kenntnis erlaubt:
  - Gezieltes Training auf das Erkennen einzelner Hinweise
  - Trainings (Email-Designs) mit verschiedenen Schwierigkeitsstufen => «Gamification»

Cue	Description
Consistency	Structure and focus of information
Links	URL, https, address bar
Visual Presentation	Logos, banners, visual presentation, general design and look
Personalization	Personalization of the content inc. language and content aspects
Security	Security indicators and status bar
Spelling and Grammatical Errors	Spelling and grammar (mistakes)
Legal	Copyright information and legal disclaimers
Sender	Sender, his or her address, contact methods
Familiarity	Credibility and level of trust in source
Importance	Rational appeals
Urgency	Time pressure, overly urgent or forceful language/content
Positive and negative consequences	Emotional and motivational appeals, premise of the appeal, underlying motive of the website (and potential incentives as positive consequence)

K. Parsons et al., «Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?,» *Australasian Conference on Information Systems*, 2015.

Feedback

- Zeitpunkt des Feedbacks (auf «falsches» Verhalten)
  - Sofort und spezifisch
  - Mikrodosen
  - Beispiel: Woran hätte man das Email als Phishing Email erkennen können?
- Gestaltung des Trainingsmaterials
  - Comic, Videos, Text, Spiel, …
  - Nicht eindeutig, resp. zu wenig Daten
    - Daten wahrscheinlich «nicht Anti-Phishing-Training» spezifisch genügend vorhanden

Knowledge Retention

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Reicht ein einmaliges Training «bis es klappt»?
  - Nein, fortlaufendes Training
- Wie oft muss man das Training durchführen?
  - Grosse Bandbreite
  - Frequenz zwischen einmal pro Woche bis mind. einmal alle 5 Monate
  - Tendenz zu unter einem Monat

Parameter	Value
Approach	General recurring training (Kumaraguru et al., 2009, 2007a,b; Caputo et al., 2014; Schroeder, 2017), recurring training individualized per user (Schroeder, 2017)
Minimum interval	Seven days (Kumaraguru et al., 2008, 2010), 16 days (Jackson et al., 2007), 28 days (Kumaraguru et al., 2009)
Maximum interval	Set by management (Schroeder, 2017), less than five months (Canova et al., 2014)

Take-Home-Message

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

- Die wissenschaftliche Literatur liefert eine Vielzahl an Erkenntnissen
  - Einige bestätigen unsere Erwartungen
  - Einige sind erhellend/überraschend
  - Einige sind nicht eindeutig, resp. widersprüchlich
- Phishing-Awareness Training(-Tools) sollten mehr auf diese Erkenntnisse achten und nicht nur auf Erfahrungen oder bewährte Praktiken

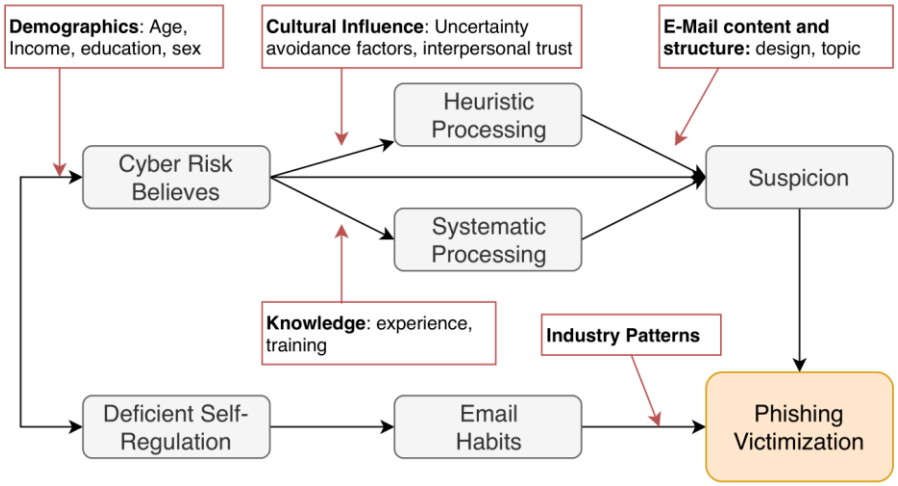
Für mehr Details:
- «Don't Click: Towards an Effective Anti-Phishing Training»
  D. Jampen, G. Gür, B. Tellenbach
- Aktuell im Peer-Review für das Journal "*Human-centric Computing and Information Sciences"* (Springer)

Ausblick

- Innosuisse Projekt mit Lucy Security: OptiPhish
- Ziel: Das «perfekte» automatisierte und smarte Anti-Phishing-Trainingssystem => What else? ☺

Danke!

SCAM and CRI



SCAM:
A. Vishwanath, B. Harrison, and Y. J. Ng, "Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility," *Communication Research*, vol. 45, no. 8, pp. 1146–1166, Feb. 2016.

Cyber Risk Index (CRI): a questionnaire with 40 questions, the result of which is used as an input for the algorithm

CRI:
A. Vishwanath, «Blunting the Phisher's Spear: A Risk-Based Approach for Defining User Training and Awarding Administrative Privileges,» *Blackhat 2016 Briefing*, 2016.