Wie anfällig sind wir für Phishing? Durchführung einer Awareness-Kampagne an fünf deutschen Hochschulen

Josephine Lechtermann, Eric Lanfer, Nils Aschenbruck

12. Februar 2025

Inhalt des Vortrags

- Die Awareness-Kampagne
  - Fragestellung & Zielsetzung
  - Hintergrund und Definitionen
  - Ablauf der Kampagne: Vorbereitung & Umsetzung
- Ergebnisse
  - Webserver-Access-Logs
  - Fragebogenauswertung
  - Fazit zu Forschungsfragen & Diskussion
- Erkenntnisse aus der Umsetzung

Die User Awareness Kampagne

Fragestellung und Zielsetzung

Fragestellung

1. Wie wirken sich Schwierigkeitsgrad und soziodemografische Daten auf die Klickrate aus?
   - Soziodemografische Faktoren: Forschungsstand bzgl. Alter, Status, Geschlecht, Fachbereich inkonsistent [1]–[3]
2. Wie effektiv ist das neu entwickelte Microlearning-Modul [4] im Vergleich zum Anti-Phishing-Video des BSI [5]?

Zielsetzung

- Sensibilisieren und informieren
- Keine personenbezogene Erhebung, keine externe Weitergabe/Speicherung personenbezogener Daten

Hintergrund und Definitionen

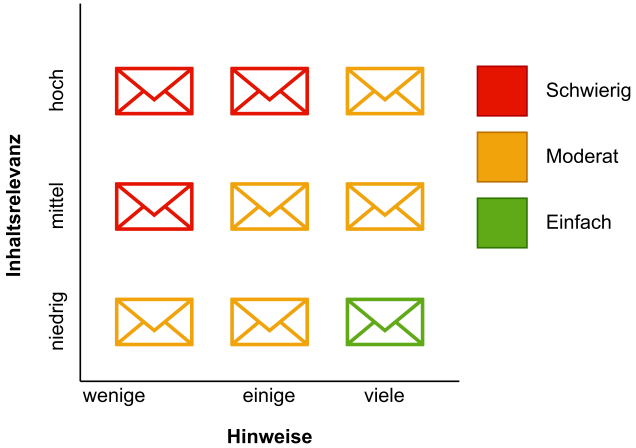


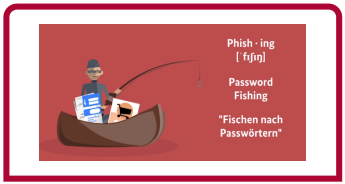
Abb.: NIST Phish Scale [6]

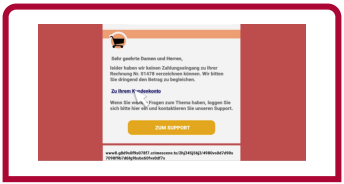
Hintergrund und Definitionen

Kategorie	Umsetzung
Fehler	Rechtschreib- oder Grammatikfehler
	Inkonsistenter Inhalt
Technische Indikatoren	Dateityp des Anhangs
	Anzeigetext $\neq$ ULR
	Domain spoofing
Visuelle Indikatoren	Fehlende/veränderte/veraltete Logos
	Unprofessionelles Aussehen
Sprache und Inhalt	Frage nach sensiblen Informationen
	Dringlichkeit, Drohungen
Verbreitete Taktiken	Angebote, die zu gut sind um wahr zu sein
	Imitation von/Bezug auf reale Arbeitsprozesse
	Bitte um Hilfe

Tabelle: Beispiele für Hinweise auf Phishing [7]

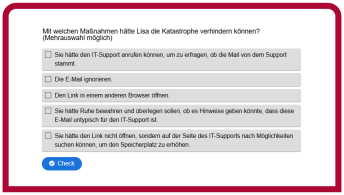
Hintergrund und Definitionen





Animiertes Erklärvideo des BSI zu Phishing [5]

Hintergrund und Definitionen



Microlearning-Module des LANIT zu Phishing [4]

Hintergrund und Definitionen

Wahl des Schulungsformats

- Außerhalb der normalen Arbeitssituation
  - Workshops, Poster, Quiz, (kleinere) Onlineschulungen [8],[9],[10].
  - Nachteil: keine Überprüfung in der realen Situation, erhöhte Aufmerksamkeit, Best Case Szenario [10], ggf. hoher Personalaufwand[3], längere Trainings werden häufig vermieden [1]
  - Vorteil: viele Beispiele/mehr Inhalt möglich [10]
- Im Alltag (eingebettetes Training)

Hintergrund und Definitionen

Wahl des Schulungsformats

- Außerhalb der normalen Arbeitssituation
- Im Alltag (eingebettetes Training)
  - Vorteile: Erprobung in der realen Arbeitssituation, bedarfsorientiertes Training [2], [3], [11], [12]
  - Nachteile: Ggf. negative Folgen wie Vertrauensverlust [13]
  - Wirksamkeit wurde wiederholt bestätigt [2], [3], [14], teils aufgrund fehlender Bearbeitung des Schulungsmaterials nicht festgestellt [11] und von Lain et al. [15] widerlegt

→ Entscheidung für eingebettetes Training insb. aufgrund hoher Teilnehmendenzahl, bedarfsorientierter Schulung, Erprobung im Alltag und geringem Personalaufwand

Ablauf der Kampagne: Übersicht

- November/Dezember 2023
- Fünf niedersächsische Hochschulen, 66887 Teilnehmende
- Je 3 simulierte Phishingmails an Mitarbeitende und Studierende
- Zwei Schwierigkeitsgrade
  - einfach: unspezifischer Inhalt, viele Hinweise auf Phishing
  - schwierig: Inhalt passt zur Hochschule, wenig Hinweise
- Eingebettetes Training: zwei Interventionsgruppen (Erklärvideo des BSI [5]/Microlearning-Modul des LANIT [4]), eine Kontrollgruppe (Error)

Ablauf der Kampagne: Vorbereitung

Absprache mit

- Datenschutzbeauftragten
- Personalrat

Information an

- Helpdesk (mit Textbausteinen)
- DNS Abuse Kontakt der verlinkten Website
- AStA
- Admins (bei ersten Nachfragen)

Image: Flaticon.com

Ablauf der Kampagne: Umsetzung

- Versand über lokale SMTP-Server im Hochschulnetzwerk (whitelisting)
- Python-Skripts, je HS lokal ausgeführt (keine Weitergabe von E-Maillisten, lokaler Versand)
  - Zuordnung der E-Mailadressen zu den Gruppen (Schwierigkeitsgrad, Schulungsmaterial)
  - Versand der entsprechenden E-Mails
  - Versand der Umfrageeinladung entsprechend der Gruppe
- Umfragen über LimeSurvey (Universität Osnabrück)

Ablauf der Kampagne: E-Mails

Einfache E-Mails

1. Paketservice
2. SoliFund Bank
3. Streamingdienst

Ablauf der Kampagne: E-Mails

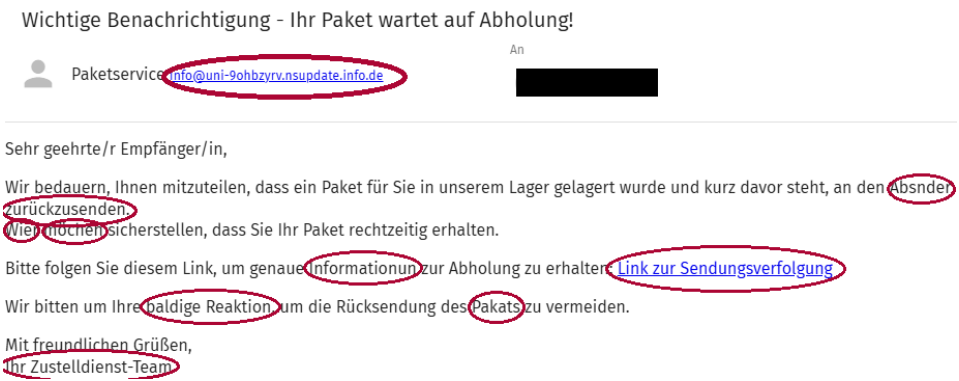
Einfache E-Mails

1. Paketservice
2. SoliFund Bank
3. Streamingdienst

Schwierige E-Mails

1. Update/Einführung Campuscard
2. Cloud-Speicherlimit erreicht
3. E-Mailpostfach voll

Ablauf der Kampagne: E-Mails



Wichtige Benachrichtigung - Ihr Paket wartet auf Abholung!

An

Paketservice info@uni-9ohbzyrv.nsupdate.info.de

[redacted]

Sehr geehrte/r Empfänger/in,

Wir bedauern, Ihnen mitzuteilen, dass ein Paket für Sie in unserem Lager gelagert wurde und kurz davor steht, an den Absnder zurückzusenden.
Wir möchten sicherstellen, dass Sie Ihr Paket rechtzeitig erhalten.

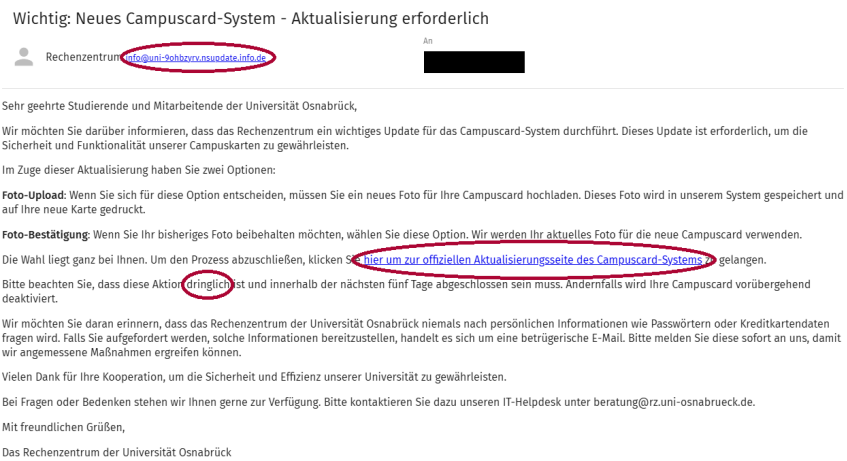
Bitte folgen Sie diesem Link, um genaue Informationun zur Abholung zu erhaltere Link zur Sendungsverfolgung

Wir bitten um Ihre baldige Reaktion um die Rücksendung des Pakats zu vermeiden.

Mit freundlichen Grüßen,
Ihr Zustelldienst-Team

Abbildung: E-Mail 1 (einfach) mit markierten Hinweisen auf Phishing

Ablauf der Kampagne: E-Mails



Wichtig: Neues Campuscard-System - Aktualisierung erforderlich

Rechenzentrum <info@uni-9ohbzyrv.nsupdate.info.de>

An [redacted]

Sehr geehrte Studierende und Mitarbeitende der Universität Osnabrück,

Wir möchten Sie darüber informieren, dass das Rechenzentrum ein wichtiges Update für das Campuscard-System durchführt. Dieses Update ist erforderlich, um die Sicherheit und Funktionalität unserer Campuskarten zu gewährleisten.

Im Zuge dieser Aktualisierung haben Sie zwei Optionen:

Foto-Upload: Wenn Sie sich für diese Option entscheiden, müssen Sie ein neues Foto für Ihre Campuscard hochladen. Dieses Foto wird in unserem System gespeichert und auf Ihre neue Karte gedruckt.

Foto-Bestätigung: Wenn Sie Ihr bisheriges Foto beibehalten möchten, wählen Sie diese Option. Wir werden Ihr aktuelles Foto für die neue Campuscard verwenden.

Die Wahl liegt ganz bei Ihnen. Um den Prozess abzuschließen, klicken Sie hier um zur offiziellen Aktualisierungsseite des Campuscard-Systems zu gelangen.

Bitte beachten Sie, dass diese Aktion dringlichst und innerhalb der nächsten fünf Tage abgeschlossen sein muss. Andernfalls wird Ihre Campuscard vorübergehend deaktiviert.

Wir möchten Sie daran erinnern, dass das Rechenzentrum der Universität Osnabrück niemals nach persönlichen Informationen wie Passwörtern oder Kreditkartendaten fragen wird. Falls Sie aufgefordert werden, solche Informationen bereitzustellen, handelt es sich um eine betrügerische E-Mail. Bitte melden Sie diese sofort an uns, damit wir angemessene Maßnahmen ergreifen können.

Vielen Dank für Ihre Kooperation, um die Sicherheit und Effizienz unserer Universität zu gewährleisten.

Bei Fragen oder Bedenken stehen wir Ihnen gerne zur Verfügung. Bitte kontaktieren Sie dazu unseren IT-Helpdesk unter beratung@rz.uni-osnabrueck.de.

Mit freundlichen Grüßen,

Das Rechenzentrum der Universität Osnabrück

Abbildung: E-Mail 1 (schwierig) mit markierten Hinweisen auf Phishing

Ablauf der Kampagne: Datenerhebung

- Links enthielten HS, Status, FB, Schwierigkeit, Gruppe (Material A/B, Kontrollgruppe)
- Auswertung der Webserver Access Logs (IP anonymisiert)
- Freiwillige Umfrage (Zuordnung HS, Status, Schwierigkeit automatisch)

Entscheidungen und Schwierigkeiten im Verlauf

- Beginn: HTTP → HTTPS Weiterleitung nicht aktiv → bereinigt
- Inhalt der schwierigen E-Mails angepasst
- Auszuwertender Zeitraum (6 x 24h pro HS) → Maximum
- Auswertung überwiegend hochschulübergreifend

Ergebnisse - Klickraten

Klickraten nach Schwierigkeitsgrad

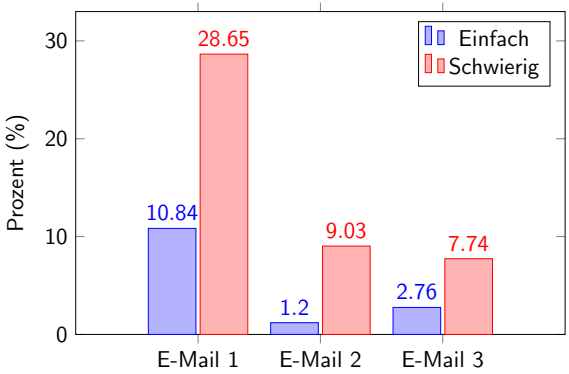


Abbildung: Klickraten pro E-Mail nach Schwierigkeitsgrad

→ Hochsignifikanter Zusammenhang zwischen Schwierigkeitsgrad und Websiteaufrufen

Klickraten nach Hochschule und Status

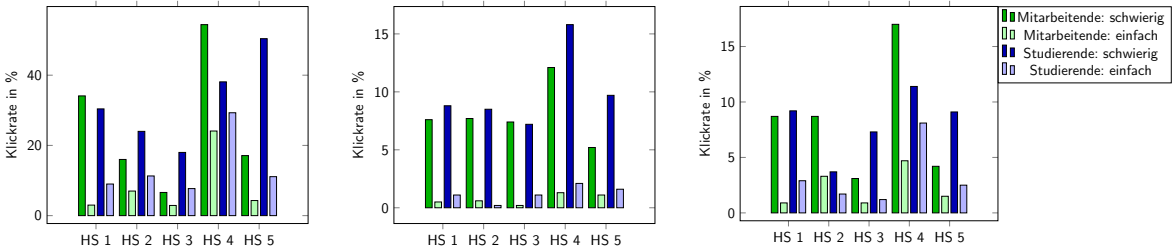


Abbildung: Klickraten E-Mail 1, E-Mail 2 und E-Mail 3 nach Hochschule, Statusgruppe und Schwierigkeitsgrad (CAVEAT: Unterschiedliche Skalierung)

Klickraten nach Hochschule und Status

Mögliche Ursachen für Unterschiede zwischen den Hochschulen

- HS 3: Vorherige Nutzung von eingebettetem Training
- Label [EXTERN]
- Wie gut passt Inhalt der E-Mails zum Hochschulalltag
- Ausrichtung der Hochschule (technisch/pädagogisch/...)

Unterschied zwischen den E-Mails:

- 1. E-Mail am schwierigsten
- Eingebettetes Training an den meisten HS noch unbekannt

Statusgruppen

	Schwierigkeit	E-Mail 1	E-Mail 2	E-Mail 3	Gesamt
Mitarbeitende	**einfach**	4,85%	0,62%	1,45%	2,31%
	schwierig	15,54%	6,96%	5,05%	9,18%
Studierende	**einfach**	12,89%	1,40%	3,20%	5,83%
	schwierig	33,14%	9,75%	8,66%	17,18%

Tabelle: Klickraten nach Statusgruppen

→ Hochsignifikanter Zusammenhang zwischen Statusgruppe und Websiteaufrufen (Chi-Quadrat: $p \approx 1.19 * 10^{-111}$)
→ Bei Überprüfung einzelner HS und einzelner E-Mails inkonsistente Ergebnisse (teils keine Signifikanz, vereinzelt mehr Aufrufe durch Mitarbeitende)

Fachbereich

Hypothese: Zusammenhang zwischen **Fachbereich beinhaltet Informatik oder Ähnliches** und **Websiteaufrufen**

- HS 1: Schwierige E-Mails: hochsignifikant, FB klickte **häufiger** auf Links
- HS 4: Einfache E-Mails: hochsignifikant, FB klickte **häufiger** auf Links
- HS 5: Schwierige E-Mails: hochsignifikant, FB klickte **seltener** auf Links

Hypothese: Zusammenhang zwischen **MINT Fachbereich** und **Websiteaufrufen** (HS 1 & 5)

- Hochsignifikant, Personen aus MINT-Fachbereichen klicken **häufiger** als andere auf Links

Schulungsmaterial

Logistische Regression, E-Mail 1 und Kontrollgruppe als Referenzwerte

- Bzgl. einfachen E-Mails: Keine Signifikanz
- Beide Schwierigkeitsgrade kombiniert: Signifikante Reduktion bei Gruppe B (LANIT)
- Bzgl. schwieriger E-Mails: Signifikante Reduktion Gruppe A (BSI), hochsignifikante bei Gruppe B (LANIT)

Gruppe A

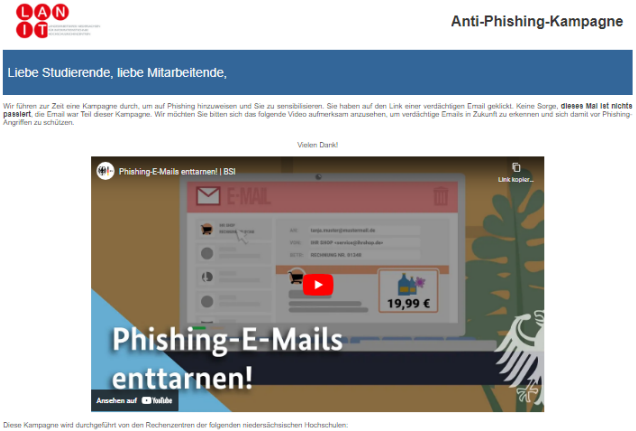


Abbildung: Website mit animiertem Informationsvideo des BSI

Gruppe B

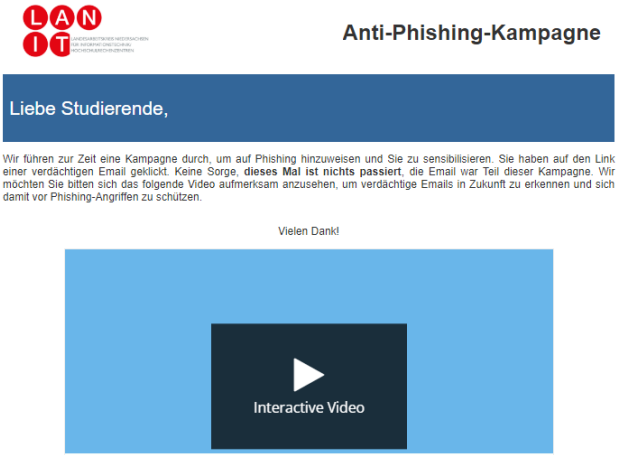


Abbildung: Website mit interaktivem Microlearning-Modul

Gruppe C

Abbildung: Website Kontrollgruppe

Schulungsmaterial - schwierige E-Mails

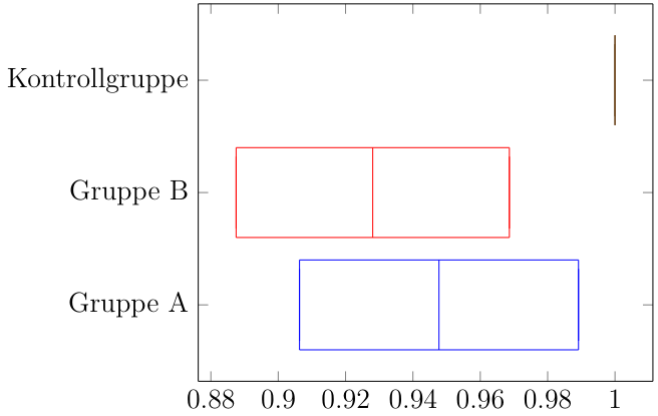


Abb.: **Odds-Ratios** - Wirksamkeit der Materialien: 95%-Konfidenzintervalle von Material A (BSI) und Material B (LANIT) im Vergleich zur Kontrollgruppe

Fragebogenauswertung

Fragebögen

Aufbau

- Einzelne Umfrage je Hochschule/Status/Schwierigkeit
- E-Mail erhalten, Link angeklickt, Bearbeitung des Schulungsmaterials
- Vorwissen
- Schulungswünsche
- Soziodemographische Daten

Rücklauf: 3192 Fragebögen, entspricht 4,8 %

- Studierende: 1984 (von 49.812, entspricht 3,98¨%)
- Mitarbeitende: 1207 (von 17.075, entspricht 7,07%)

Demografische Faktoren - sign. Zusammenh.

Alter

→ Personen **unter 30 Jahren** klickten **häufiger** auf mindestens einen Link als ohne Zusammenhang

Höchster Bildungsabschluss

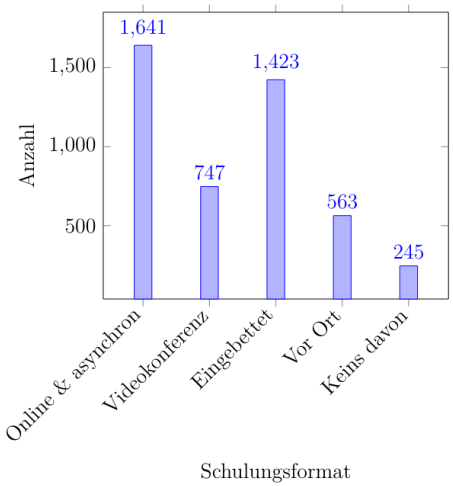
→ Personen mit allgemeinbildendem Schulabschluss, Ausbildungsabschluss oder Bachelor klickten häufiger

→ Personen mit einem Diplom, Master, einer Promotion oder einem höheren Abschluss seltener

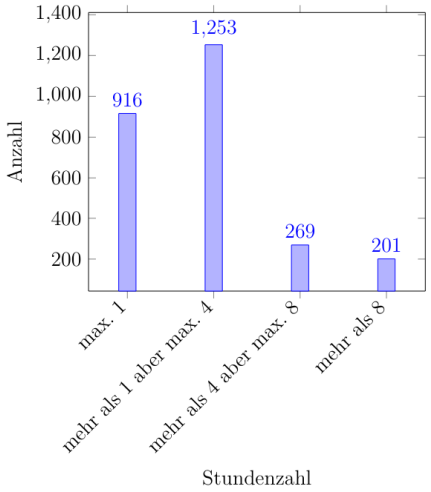
Geschlecht

→ Frauen klickten häufiger auf mindestens einen Link als Männer (Divers nicht auswertbar)

Gewünschtes Schulungsformat (N = 2575)



Gewünschte Schulungsdauer (N = 2639)



Fazit

Beantwortung der Forschungsfragen

Wie wirken sich Schwierigkeitsgrad und soziodemografische Daten auf die Klickrate aus?

Schwierigkeitsgrad:

- Hat Auswirkungen: wenig Hinweise und Alignment → mehr Websiteaufrufe

soziodemografische Faktoren:

- Zusammenhang Websiteaufrufe und Status, Alter, Geschlecht, Bildungsabschluss
- Teils Zusammenhang, aber inkonsistent: Fachbereich

Beantwortung der Forschungsfragen

Wie effektiv ist das neu entwickelte Microlearning-Modul im Vergleich zum Anti-Phishing-Video des BSI?

- Beide Materialien sind wirksam
- Es gibt Hinweise, dass das interaktive Video des LANIT wirksamer ist

Diskussion - Limitationen

- Technische Schwierigkeiten in den ersten 24 Stunden
  (E-Mail 1: nur 7770 von 13204 Websiteaufrufen erfolgreich)
- Rücklaufquote der Umfrage: 4,8 %
- Nur ca. 55 % bearbeiteten angezeigtes Material
- Effektstärken nur teilweise betrachtet
- Zusammenhang $\neq$ Kausalität, Korrelation zwischen einzelnen Faktoren
- Motivation auf Links zu klicken nicht untersucht
- Unerwünschte Wirkung von Schulungen nicht untersucht (Falsch-positiv Rate, riskantes Verhalten)

Diskussion – Einordnung in den Forschungsstand

Ergebnisse spiegeln teils den Forschungsstand wider

- Schwierigkeitsgrad [16], [17]
- Status [2]
- Wirksamkeit von (mehrfachen) Schulungen [2], [9]

Forschungsstand inkonsistent bzgl.

- Alter [1], [18]
- Geschlecht [1], [19]
- Wirksamkeit von eingebettetem Training [11], [15]

Andere Ergebnisse

- Fachbereich: Kumagaguru et al. [2] stellten keinen Zusammenhang fest
- Fachbereich: Jansson und von Solms [3] setzten voraus, dass es keinen Zusammenhang gibt

Empfehlung

Wissen hilft & Mitarbeitende **und Studierende** zu schulen ist wirksam

- Auch weniger gefährdete Gruppen haben ein Restrisiko
- Breit schulen
- Online (asynchron)/eingebettet ggf. ergänzt durch freiwillige Fortbildungen vor Ort
- (Obligatorische) Schulungen kurz halten

Erkenntnisse aus der Durchführung

- Abwägung Datenschutz vs. Präzision und Zeitaufwand
  - Vorgefertigte Lösungen (z.B. Open Source) sind vorhanden
  - Erhebung allerdings personenbezogen
- Wer sollte informiert werden?
  - Möglichst wenige, aber alle relevanten Stellen
  - Betroffene IT, Datenschutz, Personalvertretung
  - ALLE genannten Funktionsstellen (hier z.B. Poststelle)
  - Webhosting-Anbieter

Erkenntnisse aus der Durchführung

- Negative Auswirkungen möglich (Vertrauensverlust, Unzufriedenheit, Motivationsverlust)
- Hoher Personalaufwand (ggf. an unerwarteten Stellen)
  - Rechenzentrum: Vorbereitung, Durchführung
  - Helpdesk: Anfragen bearbeiten, informieren
  - Funktionsstellen: Anfragen bearbeiten

Erkenntnisse aus der Durchführung

Ausgewählte Reaktionen

- Nachfragen/Meldungen beim Helpdesk (HS 5 ca. 120, HS 3 ca. 360 wöchentlich)
- Bei der Poststelle der Hochschule nach dem Paket fragen
- Alternative Funktionsstellen kontaktieren, statt wie angegeben den Helpdesk
- Beschwerde bei RZ: Warum werden so wichtige Mails nicht zweisprachig verschickt?
- Meldung an Webhosting-Anbieter über schädliche Websitenutzung
- Rückmeldung nach der Kampagne: Unzufriedenheit und kompletter Vertrauensverlust gegenüber Rechenzentrums-E-Mails

Danke für's Zuhören, wir freuen uns über Fragen!

Literaturverzeichnis I

[1] G. Desolda, L. Ferro, A. Marrella, M. Costabile und T. Catarci, „Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Computing Surveys*, Jg. 54, S. 35, 1. Nov. 2022. DOI: 10.1145/3469886.

[2] P. Kumaraguru, J. Cranshaw, A. Acquisti u. a., „School of Phish: A Real-World Evaluation of Anti-Phishing Training," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, Ser. SOUPS '09, New York, NY, USA: Association for Computing Machinery, 15. Juli 2009, S. 1–12, ISBN: 978-1-60558-736-3. DOI: 10.1145/1572532.1572536.

[3] K. Jansson und R. von Solms, „Phishing for Phishing Awareness," *Behaviour & Information Technology*, Jg. 32, Nr. 6, S. 584–593, 1. Juni 2013, ISSN: 0144-929X. DOI: 10.1080/0144929X.2011.632650.

Literaturverzeichnis II

[4] L. N. für Informationstechnik/Hochschulrechenzentren, „Interaktive Microlearning-Module zu Phishing,“ Adresse: https://awareness.uni-osnabrueck.de/Mitarbeitende/,https://awareness.uni-osnabrueck.de/Studierende.

[5] „Animiertes Erklärvideo: Phishing,“, o.J. Adresse: https://www.bsi.bund.de/SharedDocs/Videos/DE/BSI/VerbraucherInnen/Phishing.html?nn=132646 (besucht am 26. 09. 2023).

[6] N. I. of Standards und Technology, „Introducing Phish Scale,“ *https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click*, 2020.

Literaturverzeichnis III

[7] M. Steves, K. Greene und M. Theofanos, „Categorizing human phishing difficulty: a Phish Scale,“ *Journal of Cybersecurity*, Jg. 6, Nr. 1, tyaa009, Sep. 2020, ISSN: 2057-2085. DOI: 10.1093/cybsec/tyaa009. eprint: https://academic.oup.com/cybersecurity/article-pdf/6/1/tyaa009/33746006/tyaa009.pdf. Adresse: https://doi.org/10.1093/cybsec/tyaa009.

[8] M. Volkamer, K. Renaud, B. M. Reinheimer u. a., „Developing and Evaluating a Five Minute Phishing Awareness Video,“ *Trust, Privacy and Security in Digital Business - 15th International Conference (TrustBus 2018), Regensburg, Germany, September 5–6, 2018. Ed.: S. Furnell*, S. 119, 2018, ISSN: 0302-9743. Adresse: https://publikationen.bibliothek.kit.edu/1000084441 (besucht am 05. 11. 2023).

Literaturverzeichnis IV

[9] B. M. Berens, K. Dimitrova, M. Mossano und M. Volkamer, „Phishing awareness and education – When to best remind?,“ 2022. DOI: 10.14722/usec.2022.23075.

[10] B. Reinheimer, L. Aldag, P. Mayer und M. Mossano, „An investigation of phishing awareness and education over time: When and how to best remind users,“, Adresse: https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf (besucht am 16. 04. 2024).

[11] D. D. Caputo, S. L. Pfleeger, J. D. Freeman und M. E. Johnson, „Going Spear Phishing: Exploring Embedded Training and Awareness,“ *IEEE Security & Privacy*, Jg. 12, Nr. 1, S. 28–38, Jan. 2014, ISSN: 1558-4046. DOI: 10.1109/MSP.2013.106.

Literaturverzeichnis V

[12] W. Yeoh, H. Huang, W.-S. Lee, F. Jafari und R. Mansson, „Simulated Phishing Attack and Embedded Training Campaign," *Journal of Computer Information Systems*, Jg. 62, S. 1–20, 30. Aug. 2021. DOI: 10.1080/08874417.2021.1919941.

[13] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon und L. Coventry, „Phishing simulation exercise in a large hospital: A case study," *Digital Health*, Jg. 8, S. 20 552 076 221 081 716, 2022, ISSN: 2055-2076. DOI: 10.1177/20552076221081716. pmid: 35321019.

[14] R. Dodge, K. Coronges und E. Rovira, „Information Seccurity and Privacy Research," in Gritzalis, Dimitris, Furnell, Steven und Theoharidou, Marianthi, 2012, Kap. Empirical Benefits of Training to Phishing Susceptibility.

Literaturverzeichnis VI

[15] D. Lain, K. Kostiainen und S. Capkun, „Phishing in Organizations: Findings from a Large-Scale and Long-Term Study,“ *2022 IEEE Symposium on Security and Privacy (SP)*, S. 842–859, 2021. Adresse: https://api.semanticscholar.org/CorpusID:245131301.

[16] K. Greene, M. Steves, M. Theofanos und J. Kostick, „User Context: An Explanatory Variable in Phishing Susceptibility,“, 2018. DOI: 10.14722/usec.2018.23016.

[17] M. Steves, K. Greene und M. Theofanos, „A Phish Scale: Rating Human Phishing Message Detection Difficulty,“, 24. Feb. 2019. DOI: 10.14722/usec.2019.23028.

Literaturverzeichnis VII

[18] S. Back und R. T. Guerette, „Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks," *Journal of Contemporary Criminal Justice*, Jg. 37, Nr. 3, S. 427–451, 2021, ISSN: 1043-9862. DOI: 10.1177/10439862211001628.

[19] T. Lin, D. E. Capecci, D. M. Ellis u. a., „Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content," *ACM Trans Comput Hum Interact*, 2019. DOI: 10.1145/3336141.

[20] J. A. Teixeira da Silva, A. Al-Khatib und P. Tsigaris, „Spam emails in academia: Issues and costs," *Scientometrics*, Jg. 122, Nr. 2, S. 1171–1188, 1. Feb. 2020, ISSN: 1588-2861. DOI: 10.1007/s11192-019-03315-5.

Literaturverzeichnis VIII

[21] B. für Sicherheit in der Informationstechnik, „Aktive APT-Gruppen in Deutschland,“, 2024. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html.

[22] C. Weber, „Kosten und Schäden durch Cyber-Kriminalität in Deutschland,“ *Bundeskriminalamt/Kriminalistisches Institut. Aktuelles aus der kriminalistisch-kriminologischen Forschung*, 2024.

[23] BakerHostetler, „Digital Assets and Data Management – Managing Enterprise Risks and Leveraging Data in a Digital World,“ *2020 Data Security Incident Response Report*, 2020.

Hintergrund und Definitionen

Relevanz von Phishing

- Phishing ist im akademischen Bereich ein relevantes (Informations-)Sicherheitsrisiko [20]
- Mehrere auf Forschung spezialisierte APT-Gruppen agieren in Deutschland [21]
- Errechneter Schaden für Unternehmen in Deutschland bei jährlich 321 Millionen Euro [22]
- Phishing dient häufig als Ausgangspunkt für weitere Angriffe [23]

Image: Flaticon.com