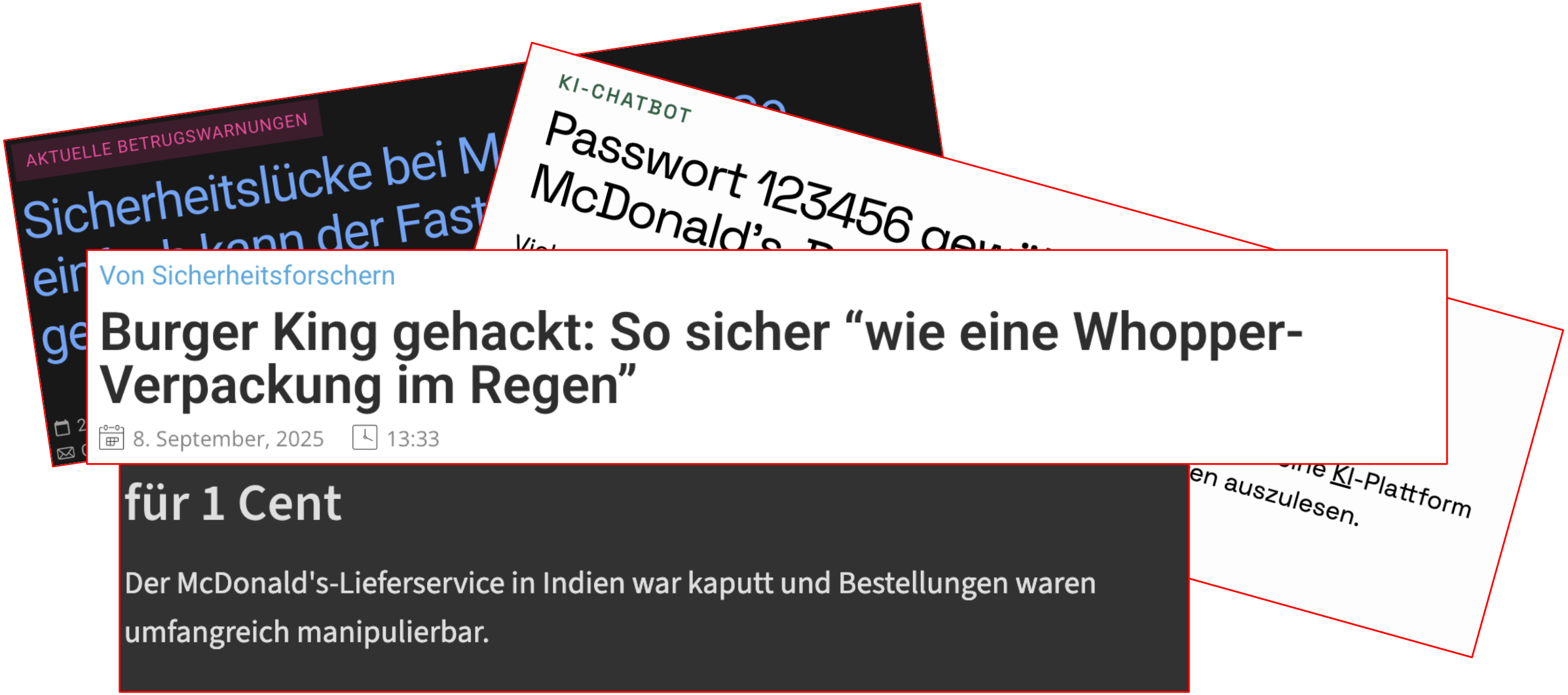
Cybersicherheit praktisch umsetzen

Business beim Burger

Sicherheitslücken – Ich liebe es

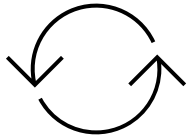


Abseits von Burgern: Angriffe auf die deutsche Wirtschaft

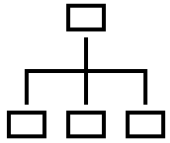
Burger Basics – Drei Sofortmaßnahmen

- Multifaktor-Authentifizierung aktivieren

- Automatische Updates aktivieren



- Passwortmanager nutzen



PhishMac

- Mitarbeitende sind ein Schlüssel zur Sicherheit.
- Aufmerksame Mitarbeitende schützen das Unternehmen vor Angriffen.
- **WICHTIG:** Die IT muss ein sicheres Fundament bieten, bei dem ein Klick auf einen Anhang oder Link nicht zum kompletten Shutdown führt

- Zwei einfache Schritte:
  - Kurze Awareness-Trainings zum Beispiel mit
    - Schulungen (Online/Inhouse)
    - Sensibilisierungstrainings
    - Postern
    - Veranstaltungen
  - Regelmäßige Phishing-Tests
    - Individuelle Lösungen sind meist effektiver als „Phishing von der Stange“
    - Prüfen Sie Ihren individuellen Bedarf

PhishMac ohne Phish?

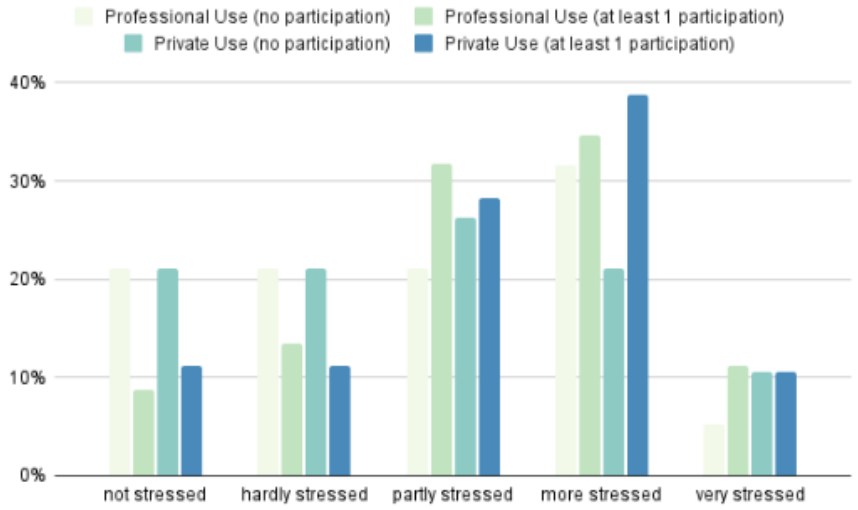


Fig. 2. Perception of stress in the private and professional context

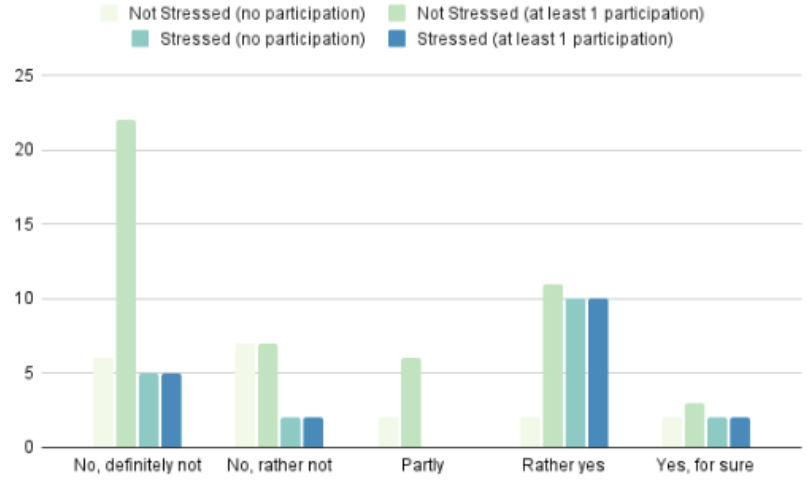


Fig. 3. Participant assessment whether they clicked on fraudulent emails. Differentiating stressed and non-stressed participants.

Das „Haar im Burger“

Wir haben 68.743 Phishing-E-Mails über einen Zeitraum von 45 Monaten analysiert, wobei wir 96 verschiedene Phishing-Kampagnen verwendet und die E-Mails in sieben übergeordnete Szenarien eingeteilt haben (Braun 2025).

Unsere Ergebnisse deuten darauf hin, dass die vorherrschende Forschung zu Phishing-Metriken durch quantitative Ergebnisse zu Klick- und Absenderaten verzerrt ist, die nicht verallgemeinerbar sind.

Table 1: The different scenarios used in the phishing emails by the service provider with an illustrative example

Scenario	Description	Example of content
Don't Miss Out (DMO)	Email contains a limited offer, opportunity, or event that the user should not miss	Information about a discount or winning a lottery
Take Care of Process (TCoP)	Email requests or demands the user to take care of a process	Email about an update of a system where the user needs to take a specific action
Account Compromised (AC)	Email pretends that a sensitive account got compromised	There was suspicious activity on an account and now action must be taken
Take Care of Email (TCoE)	Email pretends that the user needs to take care of a (most often work-related) email	There was a sending issue with the last email. The user must take care of it now
Click File/Ticket (CF/T)	Email contains a file or a (work) ticket that is general and lacks details	An email is sent with a link which allows to download "salaries_jan2024.xlsx"
Unexpected Order (UO)	Email pretends to be a dispatch, shipping, or delivery without details	User receives an email regarding a product they never ordered
Information (I)	Email offers some (obligatory or optional) information to the user	Click this link to see recent changes in the organizational chart

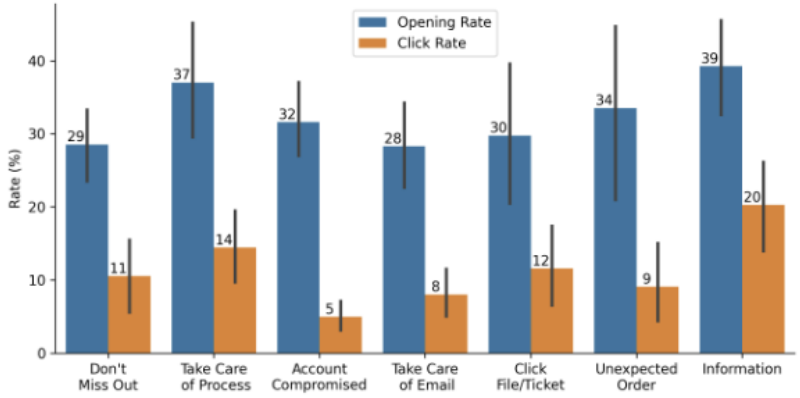


Figure 8: Average interaction rates (in percent) of the campaigns

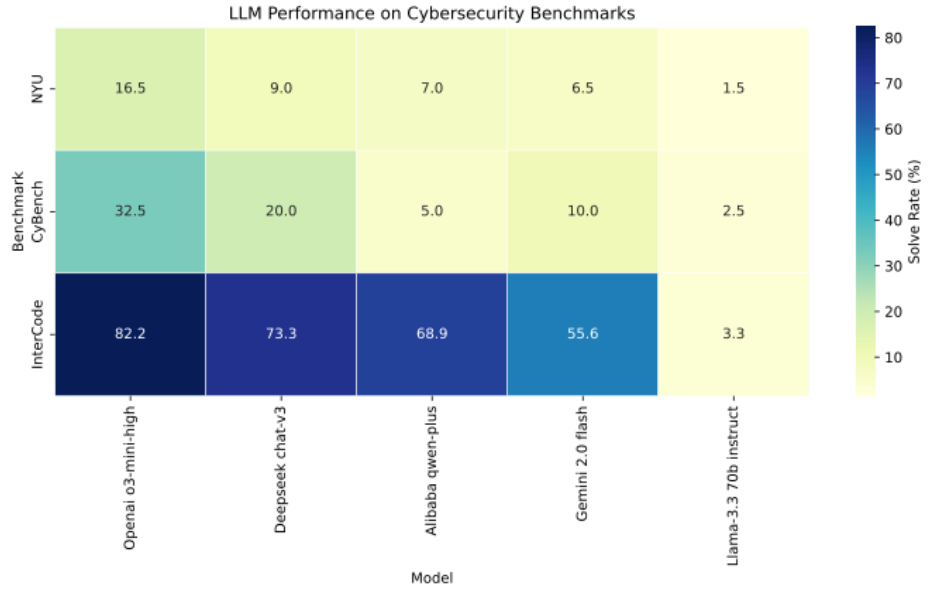
Der „Royal mit Käse“: Notfallplan für Einsteiger

- Wie wird der Vorfall eskaliert?
  - leicht zu merkende, immer erreichbare Kommunikationsmöglichkeit für Ihre Mitarbeiter:innen
- Wie bestimmen Sie die Kritikalität eines Vorfalls?
  - Staffeln Sie Vorfälle nach Kritikalität. Ist ein Vorfall bestätigt kritisch, greifen Ihre Krisenpläne
- Wie kommunizieren Sie, wenn Ihre Infrastruktur beeinträchtigt ist?
  - Haben Sie Infrastruktur die Sie zur Kommunikation mit **allen** Abteilungen nutzen können, wenn Ihre genutzte Infrastruktur nicht erreichbar ist?
- Wer ist in Ihrem Krisenstab?
  - Sammeln Sie an einem Ort alle Personen, die bei einem kritischen Vorfall mit einbezogen werden müssen. Haben Sie dort immer Telefonnummern und Funktionen zur Hand.
- Wer unterstützt Sie im Falle einer Krisensituation?
  - Sammeln Sie alle Institutionen, Dienstleister und Partner, die Ihnen im Krisenfall zur Unterstützung bereit stehen.

- Template Notfallplan für KMU: https://github.com/awareseven/kmu-incident-response/blob/main/IR-Beispiel.md

„Big Kahuna“ – Das Fazit

- Cybersicherheit ist kein Projekt, sondern ein Prozess den Sie besser heute als morgen starten
  - Heute sicher bedeutet morgen eventuell unsicher, die Technologie entwickelt sich immer weiter
- KI befähigt Verteidiger, aber auch Angreifer, komplexere Angriffe schneller und effizienter durchzuführen



An AI holds the top slot in a leaderboard that ranks people who hunt for system vulnerabilities used by hackers

Story by Nick Evanson • 2mo • 2 min read

Quellen

- https://www.it-daily.net/shortnews/burger-king-gehackt
- https://www.heise.de/news/I-f-Sicherheitsforscher-bestellt-bei-McDonald-s-fuer-1-Cent-10219043.html
- https://www.netzwelt.de/news/245447-sicherheitsluecke-mcdonalds-so-einfach-fast-food-konzern-gehackt.html
- https://www.golem.de/news/ki-chatbot-passwort-123456-gewaehrt-zugriff-auf-mcdonald-s-bewerberdaten-2507-197944.html
- https://www.it-daily.net/shortnews/cybernagriff-eu-rec-insolvenz
- https://www.stern.de/wirtschaft/news/euskirchen--hacker-treiben-servietten-fabrik-fasana-in-die-insolvenz-35812104.html
- https://www.msn.com/en-us/technology/artificial-intelligence/an-ai-holds-the-top-slot-in-a-leaderboard-that-ranks-people-who-hunt-for-system-vulnerabilities-used-by-hackers/ar-AA1HpL5L
- https://www.merkur.de/wirtschaft/verschlimmerte-lage-durch-cyberattacke-traditionsunternehmen-mit-ueber-400-beschaeftigten-ist-insolvent-zr-93353849.html
- Braun, O., Hörnemann, J., Pohlmann, N., Urban, T., & Grosse-Kampmann, M. (2025, August). Different Seas, Different Phishes–Large-Scale Analysis of Phishing Simulations Across Different Industries. In *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security* (pp. 1520-1534).
- Hörnemann, J., Braun, O., Theis, D., Pohlmann, N., Urban, T., & Große-Kampmann, M. (2024, August). Exploring the Effects of Cybersecurity Awareness and Decision-Making Under Risk. In *International Conference on Science of Cyber Security* (pp. 196-216). Singapore: Springer Nature Singapore.
- Under Submission: Haque, M. S., Abed, O., Bök, P.-B., & Große-Kampmann, M. (n.d.). Evaluating Large Language Models Regarding Their CTF Solving Capabilities. *2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC) (CCNC 2026)*.