

Die Psychologie der IT-Sicherheit: Die Hintergründe von „Phishing-Mails“



Universität Regensburg

Dr. Jonathan Mendl

Post-Doc am Lehrstuhl für Allgemeine Psychologie II
Prof. Dr. Gesine Dreisbach

Mail | Eigenschaften | Nachrichtenquelle | Diskursabfolge

Мартынова Александра Александровна <MartynovaAA@bgu.ru>

[SPAM] GIFT ✎

Antwort an: bcourtllilane@gmail.com

BC: Jonathan Mendl

Donation To You, Reply ASAP

Hallo @rz.uni-regensburg.de,

Sie haben 1 wichtige ausstehende Nachricht vom Universitätsupport.

Siehe hier*

Danke.

2024 Universität Regensburg.

"Prof. Dr. Gesine Dreisbach" <deanhead6@mail.com>

[SPAM] Do you have some minutes? ✎

BC: Jonathan Mendl

Hello,

Let me know if you are free right now.

BR

Prof. Dr. Gesine Dreisbach

Gliederung

1. Was ist Phishing?

2. Psychologische Mechanismen

- Zwei Verarbeitungssysteme nach Kahneman
- Amygdala Hijack
- Automatismen
- Kognitive Verarbeitung
- Autoritätsprinzip
- Belohnung und Bestrafung

3. Prävention

4. Fazit

1. Was ist Phishing

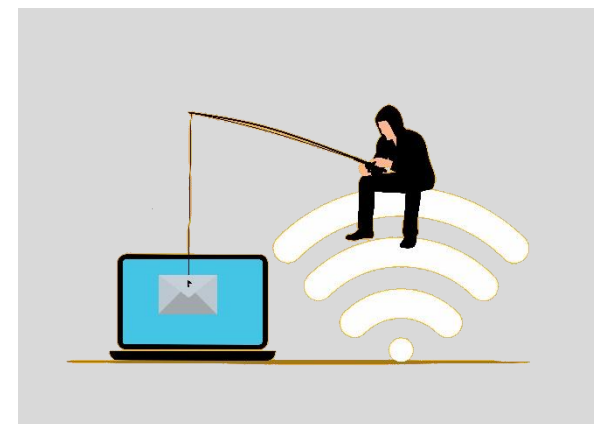
- Form des *Social Engineering*
- Ziel: Zugangsdaten
- Aufforderung, sich auf präparierter Website anzumelden

Spear-Phishing:

- Empfängerkreis ist auf Inhalt der Phishing-Mail abgestimmt

CEO-Fraud:

- Betrüger geben sich als Vorgesetzte / Führungskräfte aus



<https://pxhere.com/en/photo/1685658>

<Campus.Baecker@uni-baecker.de>

[EXT] Neu am Campus ab Juli 2025!

An

Neue Bäckerei an der Uni Regensburg!

Am 01. Juli 2025 öffnen wir unsere Türen.

Liebe Studierende und Mitarbeitende der Universität Regensburg,

wir freuen uns, euch unsere neue Bäckerei „**Der Campus-Bäcker**“ direkt auf dem Campus vorzustellen! Frisch gebackene Brote, knackige Brötchen und duftende Süßgebäcke warten auf euch.

Zur Eröffnung am **01. Juli 2025** möchten wir ein besonderes Angebot machen:

Tragt euch jetzt in unseren Newsletter ein und sichert euch zur Eröffnung wahlweise eine **Butterbreze** oder eine **Zimtschnecke** – natürlich kostenlos!

Jetzt zum Newsletter anmelden

So verpasst ihr keine Neuigkeiten und Angebote rund um „Der Campus-Bäcker“.

Wir freuen uns auf euren Besuch und wünschen ein genussvolles Sommersemester!

Euer Team vom Campus-Bäcker

service-portal.uniregensburg.eu/?rid=40f5pwh



**DER
CAMPUS-BÄCKER**
UNIVERSITÄT REGENSBURG

Newsletter-Anmeldung

Trage dich direkt mit deinem RZ-Account und Passwort ein und erhalte zur Eröffnung am Dienstag, den 01. Juli 2025 einen Gutschein für eine **Butterbreze** oder eine **Zimtschnecke**!

Anmelden

Gutschein gültig am Eröffnungstag, nur ein Gebäck pro Anmeldung.

2. Psychologische Mechanismen



Our security system has detected some irregular activity connected to your account. you will be unable to send and receive emails until this issue has been resolved

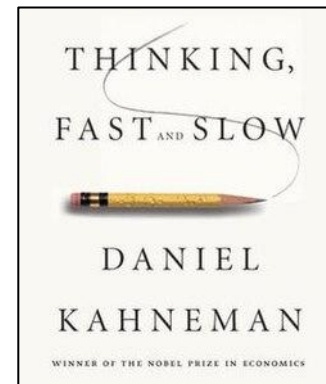
> [CLICK HERE TO VALIDATE NOW](#)

To prevent further irregular activity we will restrict access to your account within 72 hours if you did not validate your account.

Note: Mail Administrator will always keep you posted of security updates.

Mail Admin

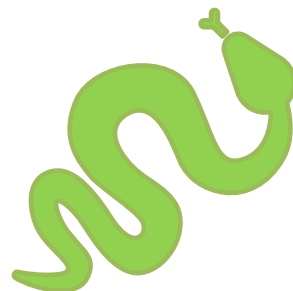
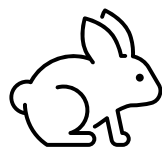
Dringlichkeit



Zwei Verarbeitungssysteme nach Kahneman

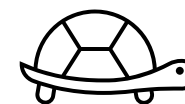
System 1

- Schnell
- Automatisch
- Intuitiv
- Unbewusst
- Fehleranfällig



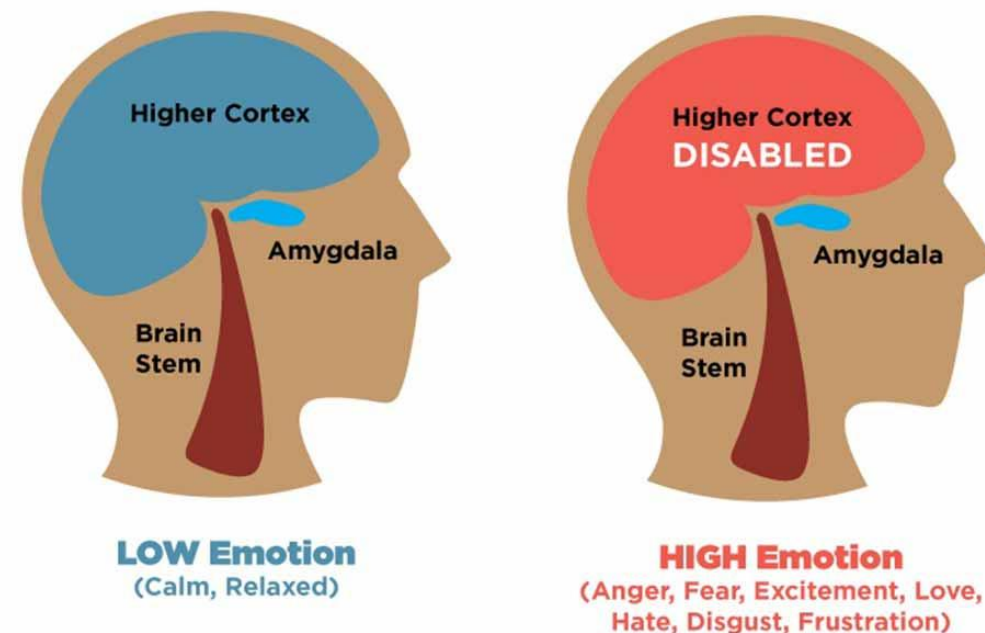
System 2

- Langsam
- Anstrengend
- Analytisch
- Bewusst
- Zuverlässig



Amygdala Hijack (Goleman, 2006)

- Emotionale Überreaktion auf Stress
- Löst Fight-or-Flight aus
- Höhere kognitive Prozesse werden blockiert



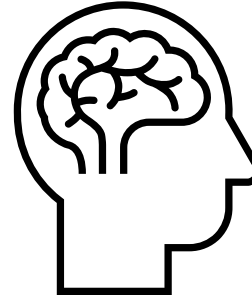
Guy-Evans, 2023

Phishing-Mails zielen häufig auf Angst / Zeitdruck ab

Zwei Verarbeitungssysteme

System 1

- Schnell
- Fehleranfällig



System 2

- Langsam
- Zuverlässig

Our security system has detected some irregular activity connected to your account. you will be unable to send and receive emails until this issue has been resolved

> [CLICK HERE TO VALIDATE NOW](#)

To prevent further irregular activity we will restrict access to your account within 72 hours if you did not validate your account.

Note: Mail Administrator will always keep you posted of security updates.

Mail Admin

Our security system has detected some irregular activity connected to your account. you will be unable to send and receive emails until this issue has been resolved

> [CLICK HERE TO VALIDATE NOW](#)

To prevent further irregular activity we will restrict access to your account within 72 hours if you did not validate your account.

Note: Mail Administrator will always keep you posted of security updates.

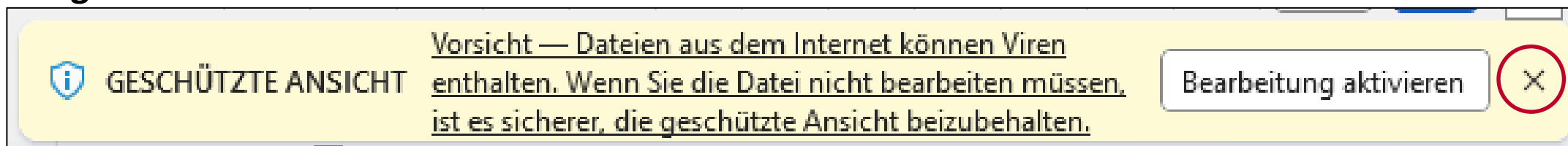
Mail Admin

Automatismen

- Gewohnheiten (auf Button klicken)
- Gut eingeübte Handlungen (Login-Daten eingeben)
- Ohne tiefere Verarbeitung



Word-Anhang und Makros



→ System 1

Zwei Verarbeitungssysteme

System 1

- Schnell
- Fehleranfällig



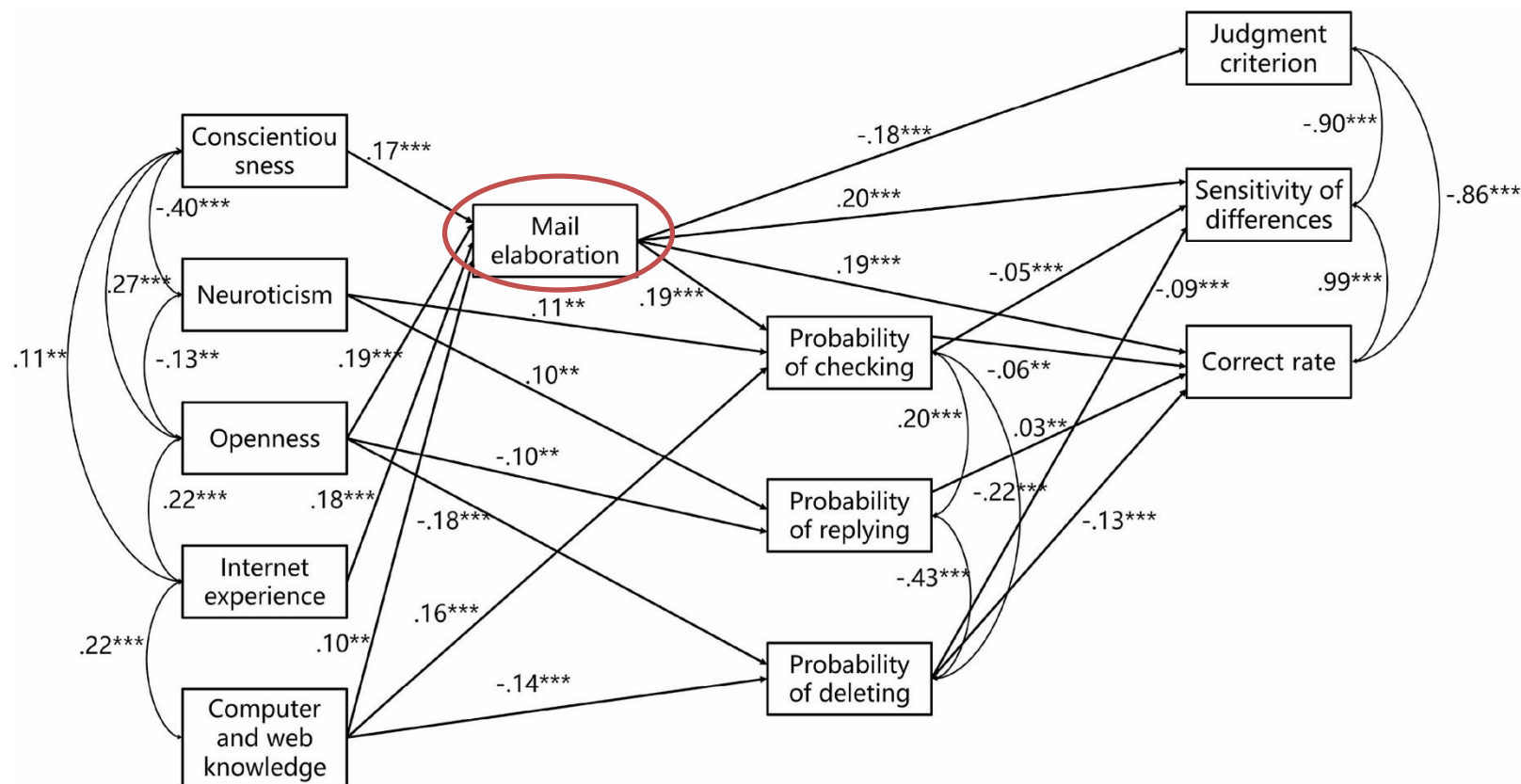
System 2

- Langsam
- Zuverlässig

Ziel: System 2 verwenden und E-Mail-Inhalt bewusst verarbeiten

Kognitive Verarbeitung

- v.a. fehlende tiefe Verarbeitung macht anfälliger für Phishing
- Kognitive Verarbeitung (*Mail elaboration*) als zentraler Faktor





Autoritätsprinzip

- E-Mail von „offizieller“ Stelle
- E-Mail von Autoritätsperson

"Prof. Dr. Gesine Dreisbach" <deanhead6@mail.com>

[SPAM] Do you have some minutes? ✎

BC: Jonathan Mendl

Hello,

Let me know if you are free right now.

BR
Prof. Dr. Gesine Dreisbach

→ Gehorsamkeit

(Milgram, 1963; Götz et al., 2023)



Wichtige Nachricht

Lieber PayPal-Kunde,

Unser System hat einen nicht autorisierten Zugriff auf Ihr PayPal-Konto festgestellt. Um Ihre Sicherheit weiterhin in vollem Umfang gewährleisten zu können, ist eine Bestätigung Ihrer Identität nötig. Bitte klicken Sie auf **Identität bestätigen**, um wieder vollen Zugriff auf Ihr PayPal-Konto zu erhalten.

Identität bestätigen

Neumann, 36C3 - Hirne Hacken



DER
CAMPUS-BÄCKER
UNIVERSITÄT REGENSBURG

Belohnung und Bestrafung

- Aussicht auf Gewinne / hohe Geldbeträge
- Negative Konsequenzen

Dear Sir,
I am prince [redacted] from Nigeria. Your help would be very appreciated.
I want to transfer all of my fortune outside of Nigeria due to a frozen account.
If you could be so kind and transfer small sum of 3 500 USD to my account,
I would be able to unfreeze my account and transfer my money outside of
Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

Please contact me to proceed

Prince [redacted]

Rechnung fehlgeschlagen - Konto gesperrt

NETFLIX

Hi [redacted]

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

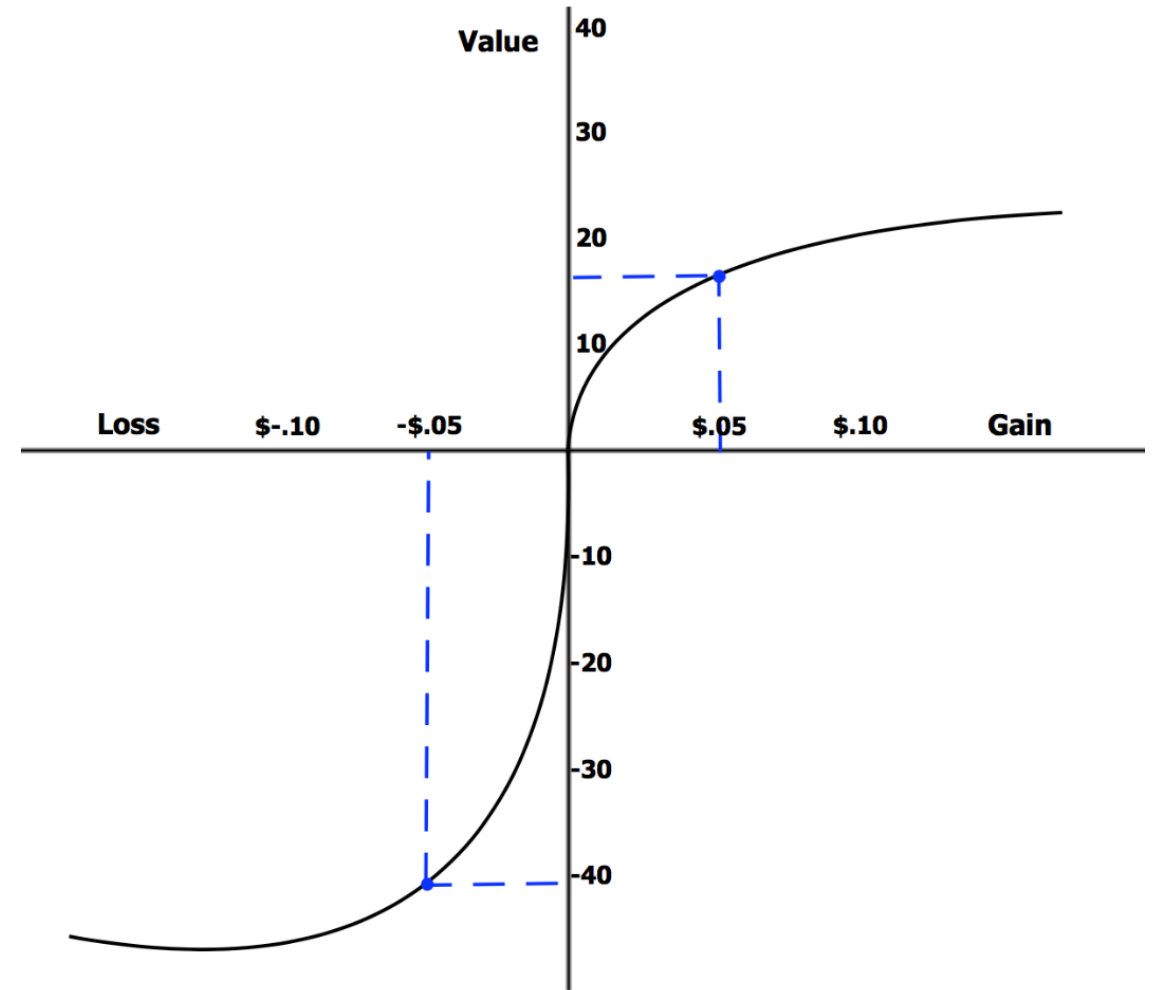
Deine Freunde bei Netflix

→ **Motivation**

<https://blog.usecure.io/de/the-most-common-examples-of-a-phishing-email>

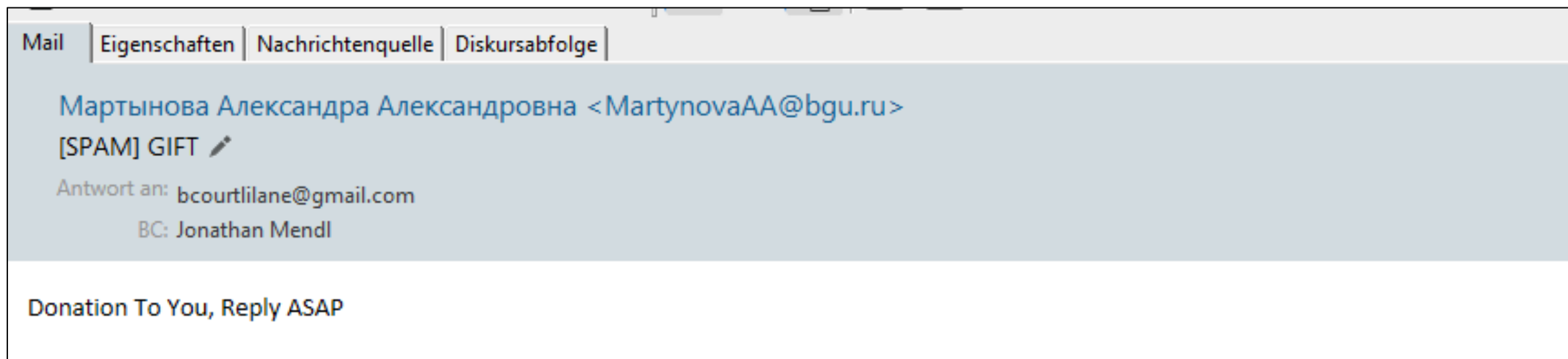
Prospect Theory

- Verluste werden subjektiv höher gewichtet

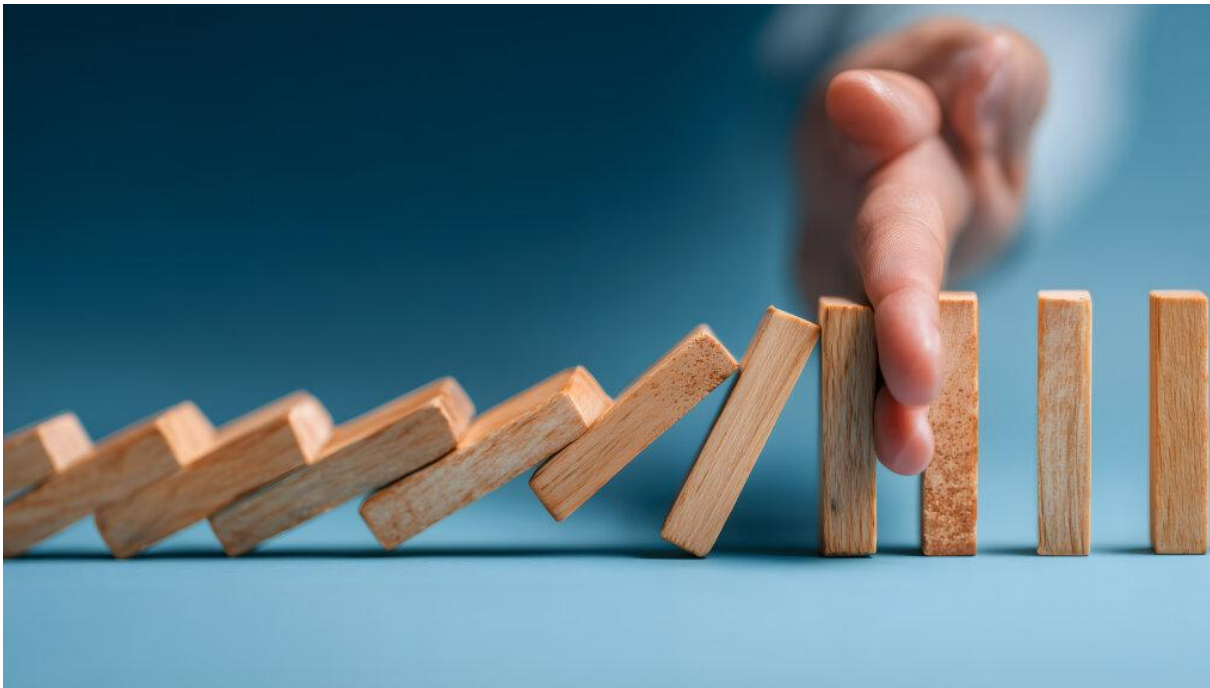


<https://commons.wikimedia.org/w/index.php?curid=67117183>

„Naivitäts-Filter“



3. Prävention



<https://ccnull.de/index.php/foto/mann-stoppt-kettenreaktion-von-dominosteinen-bei-gefahr/1124769>

Prävalenzparadox: Wenn durch Technik *kaum Phishing-Mails* bei Personen ankommen, wirken seltene Phishing-Mails umso *effektiver*

www.uni-regensburg.de/forschen/startseite

service-portal.uniregensburg.eu/?rid=40f5pwh

Domain Highlighting (Xiong, et al., 2017)

- Domain Highlighting spielt keine Rolle, aber...
- Bessere Einschätzung, wenn Adressleiste betrachtet wurde



amazon.com
facebook.com
google.com
instagram.com

Training durch Selbsterfahrung

- Künstliche Phishing Emails versenden
- Falls man auf Link klickt → Aufklärung und Training

Überwiegend positive Befunde:

Training verbessert Erkennung von Phishing Emails, aber

- spezifisch
- instabil

Take-Five-Programm

Stop: Kurz innehalten und nachdenken

Challenge: Könnte es Betrug sein?

Protect: Betrug melden

Viktimisierung: Schamgefühl bei Opfern von Phishing Attacken (Cross, 2015) → verhindert schnelle Meldung



3-Sekunden-Sicherheits-Check

1. Absender bekannt?
2. Betreff und Text sinnvoll?
3. Anhang erwartet?

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html

<https://www.uni-regensburg.de/informationssicherheit/it-sicherheit/sicherheitswarnungen>

4. Fazit

- Das Problem „Phishing“ wächst (→ KI)
- Mensch ist größte Schwachstelle
- Prävention durch Aufklärung





- Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, 12(1), 28–38. <https://doi.org/10.1109/MSP.2013.106>
- Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187–204. <https://doi.org/10.1177/0269758015571471>
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, 139, 103671. <https://doi.org/10.1016/j.cose.2023.103671>
- Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, 97, 103526. <https://doi.org/10.1016/j.apergo.2021.103526>
- Götz, F. J., Mitschke, V., & Eder, A. B. (2023). Conflict experience and resolution underlying obedience to authority. *Scientific Reports*, 13(1), 11161. <https://doi.org/10.1038/s41598-023-38067-z>
- Goleman, D. (2006). *Emotional intelligence: The groundbreaking book that redefines what it means to be smart; why it can matter more than IQ* (10. anniversary reissue ed). Bantam Books.
- Guy-Evans, O. (2023). Amygdala Hijack: How It Works, Signs, & How To Cope. *SimplyPsychology*. September, 18, 2023. <https://www.simplypsychology.org/amygdala-hijack.html>.
- Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40(2), 265–281. <https://doi.org/10.1108/OIR-04-2015-0106>
- Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10(1), 33. <https://doi.org/10.1186/s13673-020-00237-7>
- Kahneman, D. (2011). *Thinking, fast and slow* (1st ed). Farrar, Straus and Giroux.
- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263. <https://doi.org/10.2307/1914185>
- Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 61(1), 1331–1333. <https://doi.org/10.1177/1541931213601815>
- Milgram, S. (1963). Behavioral Study of obedience. *The Journal of Abnormal and Social Psychology*, 67(4), 371–378. <https://doi.org/10.1037/h0040525>
- Neumann, L. (2017). Menschliche Faktoren in der IT-Sicherheit. In F. Abolhassan (Ed.), *Security Einfach Machen: IT-Sicherheit als Sprungbrett für die Digitalisierung* (pp. 85-98). Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-14945-1_9
- Neumann, L. (2018). Wenn Hacker Menschen hacken. *Report Psychologie*, 11/12.2018, 462-464.
- Wang, P., & Lutchkus, P. (2023). Psychological tactics of phishing emails. *Issues In Information Systems*, 24(2), 71–83. https://doi.org/10.48009/2_iis_2023_107
- Xiong, A., Proctor, R. W., Yang, W., & Li, N. (2017). Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages? *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 59(4), 640–660. <https://doi.org/10.1177/0018720816684064>