Mittelstand 4.0
Kompetenzzentrum
Usability

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Phishing und Social Engineering – Werden Sie klüger als der Angler.

Michelle Walther, MSc.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Agenda

- Kompetenzzentrum Usability
- Social Engineering
  - Phasen
  - Taxonomie
- Phishing
  - Spear-Fishing
- Wie erkenne ich Phishing E-Mails?

Mittelstand 4.0
Kompetenzzentrum
Usability

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Mittelstand-
Digital

IT SICHERHEIT
VERBRAUCHERINFORMATIK

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Kompetenzzentrum Usability

Region
Nord

Mensch-KI
Zusammenarbe

Region
Ost

Digitalisierung
agiler
Arbeitsformen

Region
Mitte

Kooperationslösunge
für Unternehmens-
netzwerke

Region
Süd

Lösungen für Innovation
und Zukunft der Arbeit im
Mittelstand

Einfach nutzen,
positiv erleben.

Partner

NORDAKADEMIE
×
ERGOSIGN

Mittelstand 4.0
Kompetenzzentrum
Usability

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Mittelstand-
Digital

IT SICHERHEIT
VERBRAUCHERINFORMATIK

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

UUX in der Mensch-KI Zusammenarbeit

- Ziele / Mission
  - **Vermittlung von Methoden und Instrumenten**
  - **KI-Technologien erlebbar machen**
  - **Direkte praktische Unterstützung in Projekten**
  - **Schaffung realer Erprobungswelten**

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

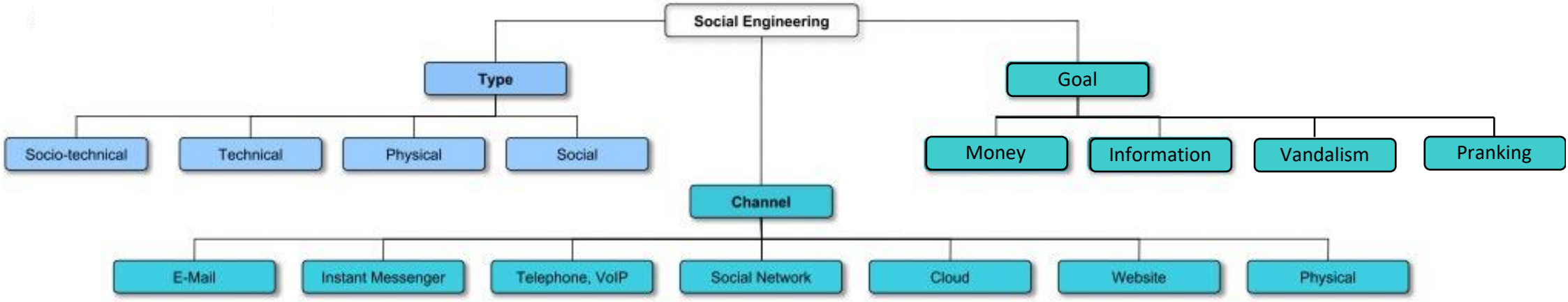
Social Engineering

- Angreifer bedient sich oft einer falschen Identität und einer falschen Legende, um seine wahren Absichten zu verbergen und eine glaubhafte Situation vorzutäuschen (Fox 2014)
- Handlungsverleitung durch Anreize, Mitleid oder Druck
- Gezieltes Ausnutzen menschlicher Bedürfnisse (z.B. nach Produkten, nach Geldanlagen, nach Liebe, etc.) und pro-soziales Verhaltensweisen (z.B. Menschen in Not zu helfen) (Nohlberg 2008; Nohlberg und Kowalski 2008)

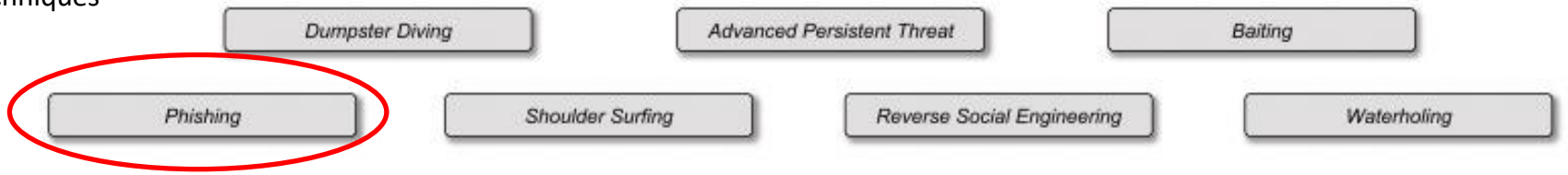
Social Engineering Phasen

- Pre-attack (Mouton et al., 2016; Mouton, 2018; Nohlberg, 2008)
  - Opfer suchen
    - Angriffsformulierung
    - Planentwicklung und Taktikauswahl
    - Zielsetzung und Aufklärung
    - Recherche und Informationsbeschaffung
- Attack (Mouton, 2018; Algarni et al.,2013)
  - Opfer kontaktieren
    - Beziehungen aufbauen (Fälschung der Identität)
    - Beziehung ausnutzen (Überredung, mentale Tricks)
- Post-attack (Mouton, 2018; Bhagyavati, 2007)
  - Opfer hinhalten (vorallem bei Kaufbetrug)
    - Spuren verwischen
    - Informationen verwenden

Social Engineering Taxonomie



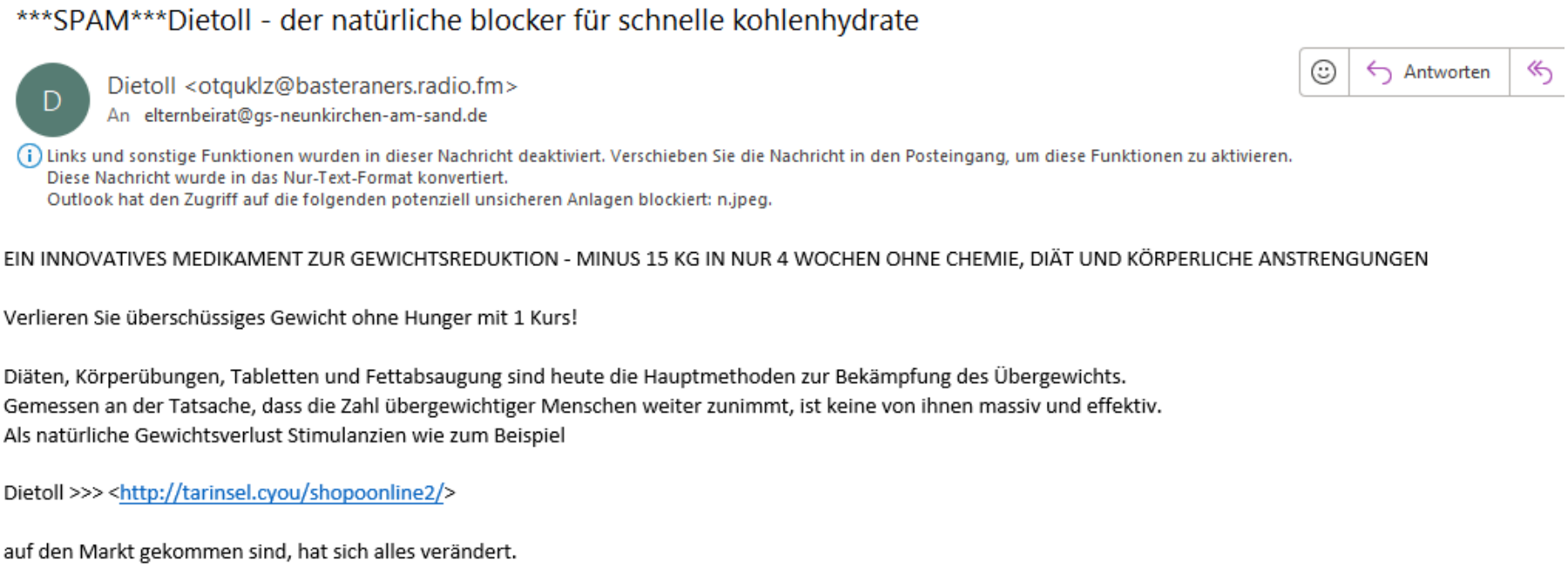
Techniques



nach Krombholz et. al., 2015

Phishing

- Eine Art von Betrug, bei dem versucht wird, mit Hilfe von Werkzeugen (z.B. falsche Webseiten) persönliche Informationen der Benutzer zu stehlen, z.B. Anmeldedaten für den Zugang zu geschützten Systemen (Dhamija, Tygar, und Hearst 2006)
- Die gefälschten Webseiten werden oft via E-Mail an die potentiellen Opfer geschickt unter der Prämisse von Webshops oder Banken zu sein (Ma et al., 2009)


SPAMDietoll - der natürliche blocker für schnelle kohlenhydrate

Antworten

D Dietoll <otquklz@basteraners.radio.fm>
An elternbeirat@gs-neunkirchen-am-sand.de

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.
Outlook hat den Zugriff auf die folgenden potenziell unsicheren Anlagen blockiert: n.jpeg.

EIN INNOVATIVES MEDIKAMENT ZUR GEWICHTSREDUKTION - MINUS 15 KG IN NUR 4 WOCHEN OHNE CHEMIE, DIÄT UND KÖRPERLICHE ANSTRENGUNGEN

Verlieren Sie überschüssiges Gewicht ohne Hunger mit 1 Kurs!

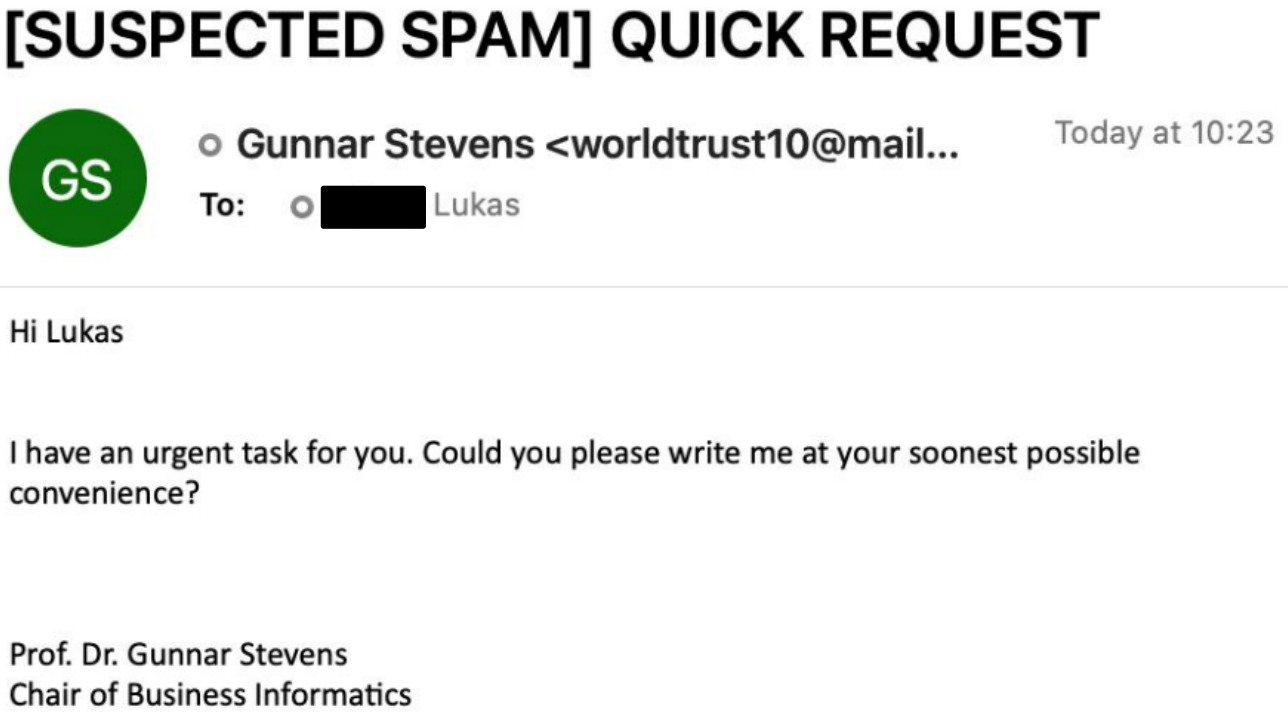
Diäten, Körperübungen, Tabletten und Fettabsaugung sind heute die Hauptmethoden zur Bekämpfung des Übergewichts.
Gemessen an der Tatsache, dass die Zahl übergewichtiger Menschen weiter zunimmt, ist keine von ihnen massiv und effektiv.
Als natürliche Gewichtsverlust Stimulanzien wie zum Beispiel

Dietoll >>> <http://tarinsel.cyou/shopoonline2/>

auf den Markt gekommen sind, hat sich alles verändert.

Spear-Phishing

- Gezielte Angriffe auf Organisationen und Firmen
- Hoher Aufwand
- Schwierig zu erkennen
- Kommt oft „aus den eigenen Reihen“



[SUSPECTED SPAM] QUICK REQUEST

GS

Gunnar Stevens <worldtrust10@mail...

Today at 10:23

To: [redacted] Lukas

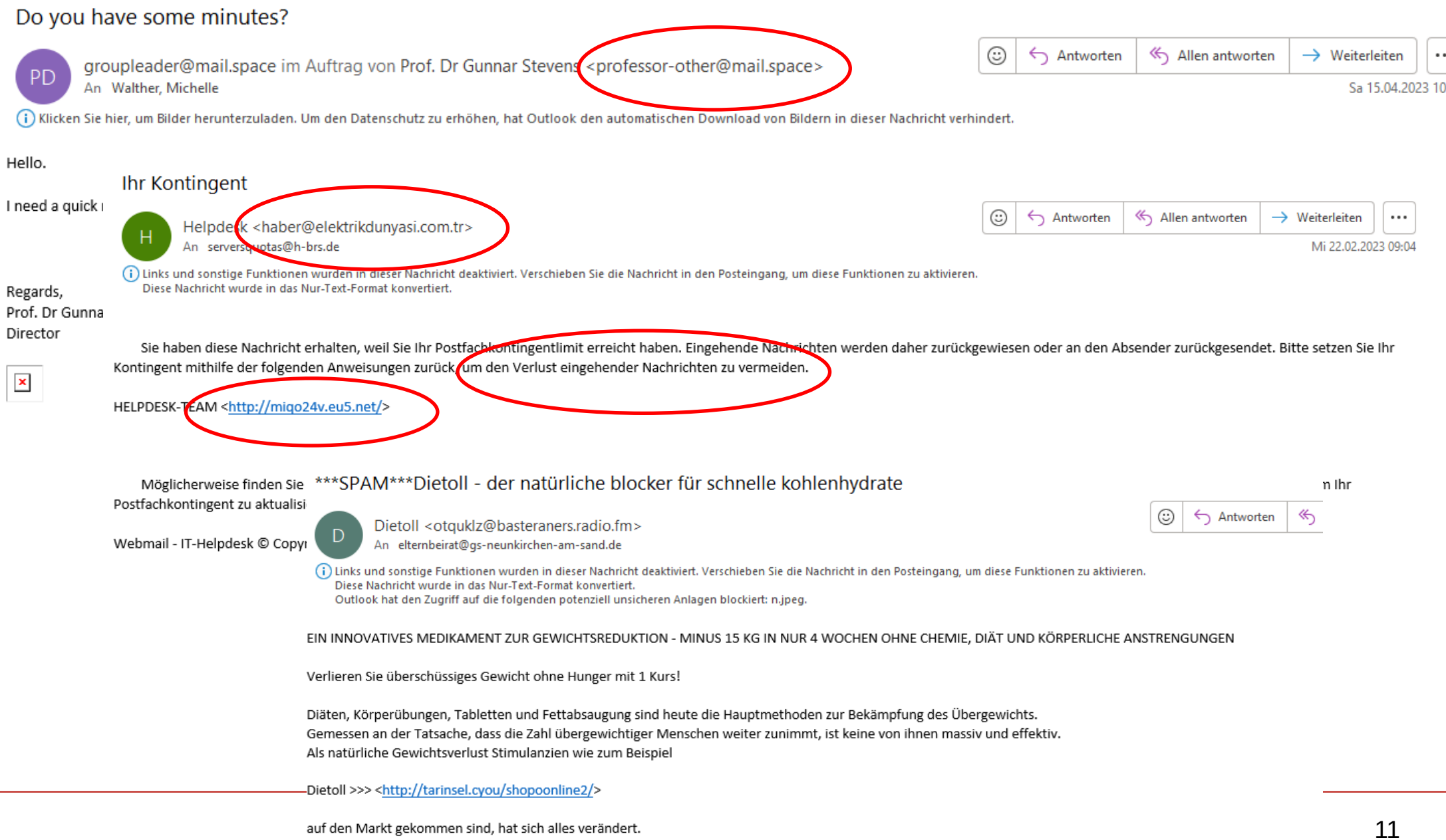
Hi Lukas

I have an urgent task for you. Could you please write me at your soonest possible convenience?

Prof. Dr. Gunnar Stevens
Chair of Business Informatics

Wie erkenne ich Phishing E-Mails?

- Dringender Handlungsbedarf: "Wenn Sie Ihre Daten nicht umgehend aktualisieren, dann gehen sie unwiederbringlich verloren“ (BSI, 2022)
- Drohungen: „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …" (BSI, 2022)
- Sie sollen vertrauliche Daten wie die PIN für Ihren Online-Bankzugang oder eine Kreditkartennummer eingeben (BSI, 2022)
- Die E-Mail enthält Links oder Formulare (BSI, 2022; Fette et al., 2007)
  - Die URL des Hyperlinks stimmt nicht mit der echten URL der Organisation überein (Singh et al., 2019; Fette et al., 2007)
  - Es sind mehrere Links in der Email enthalten (Fette et al., 2007; Ma et al., 2009)
- Die Mail scheint von einer bekannten Person oder Organisation zu stammen, die Email Adresse ist aber eine andere (BSI, 2022)
- Der Text hat kein bestimmtes Layout und/oder HTML (Fette et al., 2007)



Do you have some minutes?

PD groupleader@mail.space im Auftrag von Prof. Dr Gunnar Stevens <professor-other@mail.space>
An Walther, Michelle

Antworten | Allen antworten | Weiterleiten

Sa 15.04.2023 10

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Hello.

I need a quick

Ihr Kontingent

H Helpdesk <haber@elektrikdunyasi.com.tr>
An serversquotas@h-brs.de

Antworten | Allen antworten | Weiterleiten

Mi 22.02.2023 09:04

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Regards,
Prof. Dr Gunna
Director

Sie haben diese Nachricht erhalten, weil Sie Ihr Postfachkontingentlimit erreicht haben. Eingehende Nachrichten werden daher zurückgewiesen oder an den Absender zurückgesendet. Bitte setzen Sie Ihr Kontingent mithilfe der folgenden Anweisungen zurück, um den Verlust eingehender Nachrichten zu vermeiden.

HELPDESK-TEAM <http://miqo24v.eu5.net/>

Möglicherweise finden Sie
Postfachkontingent zu aktualisi

Webmail - IT-Helpdesk © Copyı

SPAMDietoll - der natürliche blocker für schnelle kohlenhydrate

n Ihr

D Dietoll <otquklz@basteraners.radio.fm>
An elternbeirat@gs-neunkirchen-am-sand.de

Antworten

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.
Outlook hat den Zugriff auf die folgenden potenziell unsicheren Anlagen blockiert: n.jpeg.

EIN INNOVATIVES MEDIKAMENT ZUR GEWICHTSREDUKTION - MINUS 15 KG IN NUR 4 WOCHEN OHNE CHEMIE, DIÄT UND KÖRPERLICHE ANSTRENGUNGEN

Verlieren Sie überschüssiges Gewicht ohne Hunger mit 1 Kurs!

Diäten, Körperübungen, Tabletten und Fettabsaugung sind heute die Hauptmethoden zur Bekämpfung des Übergewichts.
Gemessen an der Tatsache, dass die Zahl übergewichtiger Menschen weiter zunimmt, ist keine von ihnen massiv und effektiv.
Als natürliche Gewichtsverlust Stimulanzien wie zum Beispiel

Dietoll >>> <http://tarinsel.cyou/shopoonline2/>

auf den Markt gekommen sind, hat sich alles verändert.

Ablauf von sciebo Shares / Expiration of a sciebo Share

I info@sciebo.de
An Walther, Michelle

Antworten | Allen antworten | Weiterleiten | ...

Fr 07.04.2023 20:50

Signiert von Probleme mit der Signatur. Klicken Sie auf die Signaturschaltfläche, um Details anzuzeigen.

Sehr geehrte*r Michelle Walther,

die Shares, die Sie von verbraucherinformatik.pbox@uni-siegen.de über sciebo empfangen haben, laufen am 01.01.1970 ab.

Bitte sichern Sie diese Daten, wenn Sie sie weiter nutzen wollen. Informationen über die mit Ihnen geteilten Dateien finden Sie in der sciebo-Weboberfläche unter "Mit Ihnen geteilt".

Bei Fragen hierzu antworten Sie nicht auf diese E-Mail, sondern verwenden Sie unser Kontaktformular: https://www.sciebo.de/de/kontakt/index.html

Mit freundlichen Grüßen
Ihr sciebo-Team

Dear Michelle Walther

the shares you have received from verbraucherinformatik.pbox@uni-siegen.de via sciebo will expire on 01-01-1970.

Please save these data to another place, if you will continue to use them. Information about the files shared with you, could be found in sciebo web interface under "Shared with you".

If you have any questions, please do not reply to this e-mail, but use our contact form: https://www.sciebo.de/en/contact/index.html

Kind regards,
Your sciebo team

--
sciebo
die Campuscloud

https://www.sciebo.de

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Wie unterstütze ich meine Mitarbeitenden beim erkennen von Phishing E-Mails?

- Workshops
- Poster
- Kampagnen
- Nap Attacken (Ethische Hacker)
- Online Kurse z.B. ”PhishGuru” (Singh et al., 2019)

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Ansprechpartnerin:

Michelle Walther
Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20
Sankt Augustin
+49 2241 865 9921
m.walther@kompetenzzeentrum-usability.digital

Kompetenzzentrum Usability

Das Team

Mittelstand 4.0
Kompetenzzentrum
Usability

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Mittelstand-
Digital

IT SICHERHEIT
VERBRAUCHERINFORMATIK

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Ihr Ansprechpartner:

Dr. Daryoush Daniel Vaziri
Telefon: +49 2241 865-9654
E-Mail: d.vaziri@kompetenzzentrum-usability.digital

Michelle Walther

m.walther@kompetenzzentrum-usability.digital

David Golchinfar

d.golchinfar@kompetenzzentrum-usability.digital

Darius Hennekeuser

d.hennekeuser@kompetenzzentrum-usability.digital

- **Kompetenzzentrum Usability** gehört zu **Mittelstand-Digital**. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.
- Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital.
- Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Literatur

- Algarni, Abdullah, Yue Xu, Taizan Chan, und Yu-Chu Tian. 2013. „Social engineering in social networking sites: Affect-based model“. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 508–15.
- Bhagyavati, B. 2007. „Social Engineering“. Chapter. Cyber Warfare and Cyber Terrorism. IGI Global. 2007. https://doi.org/10.4018/978-1-59140-991-5.ch023.
- BSI 2022. Wie erkenne ich Phishing E-Mails und Webseiten? https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html
- Dhamija, Rachna, J. D. Tygar, und Marti Hearst. 2006. „Why phishing works“. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–90. CHI ’06. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1124772.1124861.
- Fette, I., Sadeh, N., & Tomasic, A. 2007. Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web* (pp. 649-656).

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Literatur

- Fox, Dirk. 2014. „Social engineering im online-banking und E-Commerce“. *Datenschutz und Datensicherheit-DuD* 38 (5): 325–28.
- Krombholz, Katharina, Heidelinde Hobel, Markus Huber, und Edgar Weippl. 2015. „Advanced social engineering attacks“. *Journal of Information Security and applications* 22: 113–22.
- Ma, L., Ofoghi, B., Watters, P., & Brown, S. 2009. Detecting phishing emails using hybrid features. In *2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (pp. 493-497). IEEE.
- Mouton, Francois. 2018. „Social Engineering Attack Detection Model“. University of Pretoria.
- Mouton, Francois, Louise Leenen, und Hein S. Venter. 2016. „Social engineering attack examples, templates and scenarios“. *Computers & Security* 59: 186–209.
- Nohlberg, Marcus. 2008. „Securing information assets: understanding, measuring and protecting against social engineering attacks“. PhD Thesis, Institutionen för data-och systemvetenskap (tills m KTH).
- Nohlberg, Marcus, und Stewart Kowalski. 2008. „The cycle of deception: a model of social engineering attacks, defenses and victims“.
- Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. 2019. Training to detect phishing emails: Effects of the frequency of experienced phishing emails. In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 63, No. 1, pp. 453-457). Sage CA: Los Angeles, CA: SAGE Publications.