Opfererfahrungen im Internet – Schutz- und Risikofaktoren

Rutger Leukfeldt/Susanne van't Hoff-de Goede/Rick van der Kleij/
Steve G.A. van der Weijer

Inhalt

I. Einführung 64

II. Online-Verhalten und Viktimisierung durch Cyberkriminalität 66
1. Unsicheres Online-Verhalten als Prädiktor für Online-Viktimisierung 66
2. Erklärung des Online-Verhaltens 68
a) Motivation 68
b) Wissen/Bewusstsein 70
c) Gelegenheit 71
d) Andere Faktoren 72

III. Messung des Online-Verhaltens 73
1. Forschung zum selbstberichteten Verhalten 73
2. Forschung zum tatsächlichen Online-Verhalten 75
3. Selbstberichtetes Verhalten versus tatsächliches Verhalten 76

IV. Studie über Online-Verhalten und Viktimisierung 77
1. Überblick über das Forschungsinstrument 77
2. Messungen von sieben Clustern des Online-Verhaltens 79
3. Detaillierte Beschreibung der Messung des tatsächlichen Online-Verhaltens 81
4. Experimente 83

V. Diskussion 84

Literaturverzeichnis 87

Appendix 91

Zusammenfassung

Der Anstieg der Opfererfahrungen durch Internetkriminalität unterstreicht die Notwendigkeit zu verstehen, wie sich Menschen online verhalten und wie unsicheres Online-Verhalten mit Viktimisierung zusammenhängen kann. Bisherige Studien haben sich oft auf selbstberichtete Verhaltensweisen oder Einstellungen zu vorsichtigem Online-Verhalten verlassen. Studien, die sowohl das tatsächliche Online-Verhalten als auch erklärende Faktoren in einer grossen Stichprobe gemessen haben, sind rar. In diesem Beitrag wird das Forschungsinstrument der *Online Behaviour and Victimization Study* vorge-

stellt. Das Kapitel skizziert die Entwicklung dieses Instruments, das ein bevölkerungsbasiertes Befragungsexperiment verwendet. Mit diesem Instrument kann das tatsächliche Verhalten von Internetnutzern gemessen werden. Während des Ausfüllens der Umfrage werden die Befragten mit (fiktiven) Cyber-Risikosituationen konfrontiert, wodurch die Forscher analysieren können, wie die Befragten mit diesen Situationen umgehen. Darüber hinaus wurden auf der Grundlage von Theorien und einer umfangreichen Literaturstudie, die in diesem Beitrag kurz skizziert wird, Messungen für zahlreiche erklärende Faktoren in die Studie aufgenommen, darunter Wissen (Bewusstsein), Gelegenheit und Motivation. Schließlich wird die frühere Viktimisierung durch Cyberkriminalität gemessen, was es ermöglicht, den Zusammenhang zwischen dem tatsächlichen Online-Verhalten und der Online-Viktimisierung zu untersuchen.

I. Einleitung

Cyberkriminalität ist weit verbreitet und ihre Auswirkungen können für die Opfer erheblich sein.[1] Cybersecurity-Experten haben versucht, die Viktimisierung mit technischen Maßnahmen wie Antivirenscannern und Firewalls zu reduzieren. Diese Maßnahmen haben jedoch oft nur eine begrenzte Wirkung und ein Großteil der Viktimisierung kann auf menschliches Verhalten zurückgeführt werden.[2] Beispielsweise geben Internetnutzer auf einer Phishing-Website[3] möglicherweise Informationen ein, die sie nicht eingeben sollten, und ermöglichen es Kriminellen so, diese Informationen zu missbrauchen. Daher ist die Erforschung von Internetnutzern unerlässlich, um die Viktimisierung zu reduzieren.[4]

Wenn wir Viktimisierung durch Cyberkriminalität verhindern wollen, müssen wir zunächst die Viktimisierung erklären. Frühere Studien zur Viktimisierung durch Cyberkriminalität haben sich auf die Erstellung eines Risikoprofils für die Opfer konzentriert und versucht, Faktoren zu identifizieren, die das Risiko einer Viktimisierung erhöhen könnten. In diesen Studien stehen oft persönliche Merkmale und Routinetätigkeiten im Mittelpunkt, indem z. B. angenommen wird, dass bestimmte Routinetätigkeiten, wie die Nutzung sozialer Medien, potenzielle Opfer für Cyberkriminelle sichtbarer machen. Mit Blick auf

1 Cross/Richard/Smith; Jansen/Leukfeldt, cybercrime; Leukfeldt/Notté/Malsch.

2 Jansen; Leukfeldt, Research.

3 Phishing ist eine Form des Online-Betrugs, bei der Kriminelle die E-Mails oder Websites bekannter Unternehmen und Organisationen imitieren, um die Opfer in die Irre zu führen, damit sie an Benutzernamen und Passwörter gelangen und Zugang zu den Online-Konten erhalten.

4 Leukfeldt, Research; Rhee/Kim/Ryu; Talib/Clarke/Furnell.

alle bisherigen Studien scheint es jedoch nicht möglich zu sein, ein eindeutiges Risikoprofil zu erstellen.[5] Cyberkriminelle sind offenbar nicht allzu wählerisch und suchen sich ihre Opfer nicht besonders aus: Jede Person ist ein potenzielles Opfer von Cyberkriminalität. Ausserdem scheinen bestimmte Online-Aktivitäten nur mit dem Risiko verbunden zu sein, Opfer bestimmter Formen von Cyberkriminalität zu werden. Es scheint keine Routineaktivitäten zu geben, die per Definition risikoerhöhend sind.[6] Es ist daher nicht möglich, ein Profil risikobehafteter persönlicher Merkmale oder Routinetätigkeiten für die Viktimisierung durch Cyberkriminalität zu benennen.

Die aktuelle Studie konzentriert sich auf das Verhalten von Internetnutzern, um damit Online-Viktimisierungen zu erklären. Es ist weithin anerkannt, dass der Mensch das „schwächste Glied" in der Cybersecurity ist. Unsicheres Online-Verhalten, wie z. B. die Verwendung von schwachen Passwörtern und nicht regelmäßig aktualisierte Software, kann das Risiko einer Viktimisierung durch Cyberkriminalität erhöhen.[7] Das Wissen darüber, wie sich Bürger gegen Cyberkriminalität schützen, ist jedoch spärlich[8] Es ist immer noch unbekannt, wie gut sich Internetnutzer vor Cyberkriminalität schützen, zum Teil weil das, was Menschen über ihr Online-Verhalten sagen oder denken, nicht immer mit dem tatsächlichen Online-Verhalten übereinstimmt.[9] Dieses Wissen ist jedoch für die empirische Fundierung möglicher Verhaltensinterventionen unerlässlich. Es ist daher notwendig, mehr Erkenntnisse darüber zu gewinnen, wie sich Internetnutzer tatsächlich online verhalten und welche Faktoren damit verbunden sind.

In diesem Beitrag wird die Entwicklung des Forschungsinstruments für die *Online Behaviour and Victimization Study* skizziert, das das tatsächliche Online-Verhalten zusammen mit möglichen erklärenden Faktoren messen kann. Der Mehrwert dieses Forschungsinstruments liegt auf der Hand: Wir gehen über bestehende Studien hinaus, die oft auf Selbstberichten basieren, indem wir sowohl das wahrgenommene als auch das tatsächliche Verhalten in einer gross angelegten Stichprobe messen. Außerdem zielen wir nicht nur auf die Erklärung der Viktimisierung bestimmter Formen von Cybercrime ab, sondern auch auf mehrere Cluster von Online-Verhalten. Schließlich gibt es viele Verhaltensweisen, die das Risiko für bestimmte Cyberkriminalität erhöhen. Ausserdem muss es nicht gleichzeitig so sein, dass ein bestimmtes Verhalten

5 Bossler/Holt, On-Line Activities; Bossler/Holt, effect; Holt/Bossler;Sheng et al.; van de Weijer/Leukfeldt.

6 Leukfeldt/Yar.

7 Leukfeldt, Phishing; Shillair et al.

8 Für einen Überblick siehe z.B. Leukfeldt, Research.

9 Crossler et al.; Debatin et al.

immer zu einer bestimmten Form der Viktimisierung führt. Einmal auf eine Phishing-E-Mail hereinzufallen, kann zu einem leeren Bankkonto führen, ein anderes Mal kann es zu einer Ransomware-Infektion[10] führen oder der Beginn eines Spear-Phishing-Angriffs[11] auf das Unternehmen sein, in dem das Opfer arbeitet.[12] Daher misst das in diesem Kapitel vorgestellte Forschungsinstrument objektiv eine Reihe von Verhaltensweisen, von denen wir wissen, dass sie in direktem Zusammenhang mit der Viktimisierung verschiedener Cyberkriminalität stehen, wie z. B. die Weitergabe persönlicher Informationen und die Verwendung schwacher Passwörter. Darüber hinaus ist dieses Forschungsinstrument innovativ, weil es verschiedene Erklärungen für Online-Verhalten und Viktimisierung misst, während bestehende Studien oft nur Einstellungen oder Wissen untersuchen. Schliesslich beinhaltet das Instrument mehrere Experimente, um beispielsweise zu ermitteln, ob von Kriminellen verwendete Überredungstechniken die Wahrscheinlichkeit erhöhen, dass sich Personen online unsicher verhalten.

II. Online-Verhalten und Viktimisierung durch Cyberkriminalität

1. Unsicheres Online-Verhalten als Prädiktor für Online-Viktimisierung

Unsicheres Online-Verhalten kann direkt zu einem erhöhten Risiko der Viktimisierung beitragen. Opfer von Online-Banking-Betrug scheinen beispielsweise oft versehentlich ihre persönlichen Daten an Betrüger weitergegeben zu haben, z. B. durch Klicken auf einen Hyperlink in einer Phishing-E-Mail oder die Eingabe von Informationen auf einer Phishing-Website.[13]

Eine wichtige Voraussetzung für Online-Sicherheit ist daher sicheres Online-Verhalten (d. h. Cyber-Hygiene-Verhalten).[14] Menschen, die sich online sicher – oder cyberhygienisch – verhalten, halten sich an „goldene" Regeln (Best Practices). Sie meiden zum Beispiel unsichere Webseiten, vermeiden das Klicken auf unzuverlässige Hyperlinks, verwenden starke Passwörter und halten ihre technischen Sicherheitsmassnahmen auf dem neuesten Stand.[15] Basie-

---

10 Ransomware ist eine Schadsoftware, die einen Computer blockiert oder Dateien verschlüsselt. Erst wenn die betroffene Person ein Lösegeld zahlt, kann sie den Computer oder die Dateien wieder nutzen.

11 Spear-Phishing ist ein gezielter Phishing-Angriff gegen eine Person oder eine bestimmte Gruppe von Personen.

12 Siehe z.B. Leukfeldt/Kleemans/Stol; Lusthaus.

13 Jansen; Jansen/Leukfeldt, People; Jansen/Leukfeldt, Phishing.

14 Cain/Edwards/Still.

15 Cain/Edwards/Still; Crossler/Bélanger/Ormond; Symantec.

rend auf früheren empirischen Studien haben wir für diese Studie sieben zentrale Verhaltenscluster identifiziert: das Passwortmanagement, das Sichern wichtiger Dateien, das Installieren von Updates, die Verwendung von Sicherheitssoftware, die Aufmerksamkeit im Internet, die Offenlegung von persönlichen Informationen im Internet und der Umgang mit Anhängen und Hyperlinks in E-Mails. Wenn Internetnutzer innerhalb der einzelnen Cluster ein sicheres Verhalten an den Tag legen, kann es sie vor der Viktimisierung durch Cyberkriminalität schützen.[16]

Frühere Studien, die sowohl auf selbstberichteten Verhaltensweisen als auch auf tatsächlichem Verhalten in experimentellen Umgebungen basieren, haben gezeigt, dass viele Menschen sich online nur in begrenztem Masse sicher verhalten oder sogar offensichtlich unsicheres Online-Verhalten zeigen, und zwar bei jedem der sieben Verhaltenscluster. Viele Menschen haben keinen Malware-Scanner[17] oder eine Firewall auf ihrem Heimcomputer oder halten diese nicht auf dem neuesten Stand.[18] Darüber hinaus sind junge Menschen lax mit der Sicherheit ihres Smartphones.[19]

Obwohl die Verwendung von einzigartigen, starken Passwörtern eine wichtige Sicherheitsmassnahme ist, haben Studien gezeigt, dass 50-60% der Passwörter plattformübergreifend wiederverwendet werden und dass viele Menschen ihre Passwörter mit anderen teilen würden.[20] Ein weiteres Beispiel für unsicheres Online-Verhalten ist, dass Menschen in grossem Umfang persönliche Informationen in sozialen Medien teilen,[21] die genutzt werden können, um Phishing-E-Mails glaubwürdiger zu machen (Spear-Phishing) oder um Identitätsbetrug zu begehen. Zum Beispiel gaben viele der Befragten in der Studie von Talib/Clarke/Furnell ihren vollständigen Namen und ihre E-Mail-Adresse (62%), ihr Geburtsdatum (45%) oder ihre vollständige Adresse (7%) in einem sozialen Online-Netzwerk an. Schliesslich sind abweichende Online-Verhaltensweisen, wie illegales Herunterladen, Online-Mobbing und Bedrohung anderer, weit verbreitet und tragen zur Online-Viktimisierung bei, möglicherweise insbesondere bei jungen Menschen.[22]

---

16 Für weitere Informationen siehe Cain/Edwards/Still; Crossler/Bélanger/Ormond; van Schaik et al.

17 Malware ist bösartige Software, die sich unaufgefordert und meist unbemerkt auf Ihrem Computer installiert. Beispiele für Malware sind Viren, Trojanische Pferde, Würmer und Spyware.

18 Cain/Edwards/Still; van Schaik et al.

19 Jones/Heinrichs; Tan/Aguilar.

20 Alohali et al.; Cain/Edwards/Still;Kaye.

21 Christofides/Muise/Desmarais; Debatin et al.; Talib/Clarke/Furnell.

22 Bossler/Holt, On-Line Activities; Holt/Bossler; Maimon/Louderback; Ngo/Paternoster.

Eine weitere Schlussfolgerung, die aus der Literatur gezogen werden kann, ist der Mehrwert der Fokussierung auf das Verhalten und nicht auf spezifische Cyberkriminalität. Hacking-Viktimisierung kann zum Beispiel durch viele verschiedene Verhaltensweisen verursacht werden. Zum Beispiel können Menschen gehackt werden, weil sie persönliche Informationen weitergegeben, Malware heruntergeladen oder ihre Sicherheitsvorkehrungen nicht auf dem neuesten Stand gehalten haben. Darüber hinaus können diese Verhaltensweisen auch zur Viktimisierung anderer Formen von Cyberkriminalität führen, wie z. B. Online-Betrug oder Identitätsbetrug. Studien, die sich auf spezifische Straftaten konzentrieren, geben nur einen kleinen Einblick in die Komplexität von Online-Verhalten und Cyberkriminalität. Durch die Fokussierung auf das Online-Verhalten hingegen kann potenziell einer breiten Palette von Cyberkriminalität entgegengewirkt werden.

2. Erklärung des Online-Verhaltens

Obwohl sicheres Online-Verhalten von grosser Bedeutung sein kann, um die Viktimisierung durch Cyberkriminalität zu verhindern, ist unsicheres Online-Verhalten weit verbreitet. Wie lässt sich dies erklären?

Auf der Grundlage von zwei Theorien, die zuvor zur Erklärung von Verhalten entwickelt wurden, der Protection Motivation Theory (PMT)[23] und dem COM-B-Framework (Capability, Opportunity, Motivation, Behaviour),[24] können mehrere Elemente unterschieden werden, die jeweils eine Rolle bei unsicherem Online-Verhalten spielen können. Dabei handelt es sich um die *Motivation* für sicheres Online-Verhalten, das *Wissen* über sicheres Online-Verhalten (d. h. das Bewusstsein) und die *Gelegenheit* für sicheres Online-Verhalten. Nach der Erörterung dieser Faktoren und früherer Studien über ihre Beziehungen zum Online-Verhalten wird sich dieses Kapitel auch mit anderen potenziell relevanten Faktoren befassen.

a) Motivation

Nach der Protection Motivation Theory wird unser Schutzverhalten davon beeinflusst, inwieweit wir motiviert sind, uns zu schützen.[25] Es ist anzunehmen, dass Menschen mit einer hohen Schutzmotivation vorsichtiger handeln und Massnahmen zum Schutz ihrer Sicherheit ergreifen.[26] Die Theorie argumen-

23 Floyd/Prentice-Dunn/Rogers; Norman/Boer/Seydel.

24 Michie/van Stralen/West.

25 Floyd/Prentice-Dunn/Rogers; Norman/Boer/Seydel.

26 Crossler/Bélanger; Floyd/Prentice-Dunn/Rogers.

tiert, dass die Schutzmotivation von der Bewertung der eigenen Bewältigungsmöglichkeiten und der Bewertung der Bedrohung beeinflusst wird, d. h. von der Bewertung der Bedrohung durch eine Person und den Massnahmen gegen diese Bedrohung.[27] Sowohl die Bewertung der Bedrohung als auch die Bewertung der Bewältigungsmöglichkeiten haben mehrere Komponenten. Die Komponenten der Bedrohungsbeurteilung sind die wahrgenommene Verwundbarkeit (Einschätzung der eigenen Verwundbarkeit gegenüber der Bedrohung) und der wahrgenommene Schweregrad (Einschätzung des Schweregrads der Bedrohung). Die Bewertung der Bewältigungsmöglichkeiten umfasst die Komponenten Reaktionswirksamkeit (ob eine Massnahme gegen die Bedrohung wirksam sein wird), Selbstwirksamkeit (ob man in der Lage ist, eine wirksame Massnahme einzusetzen) und Reaktionskosten (ob sich die geschätzten Kosten der Massnahmen lohnen).

Die Protection Motivation Theory wurde bereits auf das Online-Verhalten angewandt. Frühere Studien ergaben, dass die geschätzte Reaktionswirksamkeit, die Selbstwirksamkeit und die Reaktionskosten wichtige Prädiktoren für sicheres Online-Verhalten zu sein scheinen.[28] Allerdings steht die wahrgenommene Gefährdung möglicherweise nicht in der erwarteten Weise mit sicherem Online-Verhalten in Zusammenhang. Personen, die sich selbst als anfällig für Online-Angriffe einschätzen, verhalten sich nicht anders[29] und verhalten sich möglicherweise sogar weniger sicher.[30] Im Zusammenhang mit der wahrgenommenen Verwundbarkeit fanden Boss et al.[31] heraus, dass die Angst vor Viktimisierung die Motivation von Computernutzern, ihre Dateien zu sichern, nicht zu beeinflussen scheint, während sie ihre Bereitschaft, Anti-Malware-Software zu verwenden, zu erhöhen scheint. Schliesslich finden die meisten Studien einen Zusammenhang zwischen wahrgenommener Schwere und Online-Verhalten.[32] Downs, Holbrook und Cranor[33] fanden jedoch in ihrer Stichprobe von 232 Computernutzern nicht, dass die geschätzte Schwere der Folgen eines erfolgreichen Phishing-Angriffs ein Prädiktor für das Vorsichtsverhalten ist.

Leider gibt es nur sehr wenige Studien, die über die Untersuchung der Schutzmotivation und -einstellung hinausgehen und das Online-Verhalten messen.

---

27 Floyd/Prentice-Dunn/Rogers.

28 Arachchilage/Love; Crossler/Bélanger; Crossler/Bélanger/Ormond; Jansen/van Schaik; Rhee/Kim/Ryu; van Schaik et al.; Workman/Bommer/Straub.

29 Jansen.

30 Crossler/Bélanger.

31 Boss et al.

32 Crossler/Bélanger/Ormond; Jansen; Jansen/van Schaik.

33 Downs/Holbrook/Cranor.

Die wenigen, die dies taten, konzentrierten sich hauptsächlich auf das selbstberichtete Präventivverhalten. Es bleibt unklar, wie die Motivation mit dem tatsächlichen Online-Verhalten zusammenhängen könnte.

b) Wissen/Bewusstsein

Der theoretische COM-B-Framework[34] legt nahe, dass neben der Motivation auch die Fähigkeit (d. h. das Wissen über Online-Sicherheit), die auch als Bewusstsein bezeichnet wird, für ein sicheres Online-Verhalten erforderlich ist. Beispiele dafür sind Wissen über Online-Bedrohungen, Informationssicherheit, Sicherheitsmassnahmen und die Fähigkeit, schädliche URLs zu erkennen.

Frühere Studien, die untersuchten, inwieweit das Wissen über IT- und Cybersicherheit das Online-Verhalten beeinflusst, lieferten widersprüchliche Ergebnisse.[35] Arachchilage und Love[36] zeigten beispielsweise, dass Wissen, wie das Erkennen einer unzuverlässigen URL, die Selbstwirksamkeit erhöht und zu einem Phishing-Risikovermeidungsverhalten beitragen kann. Darüber hinaus sind Personen, die in der Lage sind, URLs zu bewerten, Internet-Symbole und Internet-Begriffe zu verstehen, tendenziell weniger anfällig für Phishing-Angriffe.[37] Darüber hinaus scheinen Personen, die sich als IT-Experten bezeichnen, weniger wahrscheinlich ein unsicheres Online-Verhalten an den Tag zu legen.[38] Andererseits fanden Ovelgönne et al.[39] heraus, dass Softwareentwickler häufiger ein riskantes Online-Verhalten an den Tag legen als andere Befragte. Obwohl dies in einigen Fällen damit zusammenhängen könnte, dass Menschen ihr Wissen über Internetsicherheit überschätzen und sich dadurch zu Unrecht als IT-Experten einstufen,[40] fanden Cain/Edwards/Still[41] heraus, dass Menschen, die sich selbst als IT-Experten einschätzen, sich online weniger sicher verhalten. Darüber hinaus wurde kein Unterschied im Präventivverhalten zwischen Personen, die in IT oder Cybersicherheit geschult waren, und solchen, die dies nicht waren, festgestellt. Diese Studien haben einen wichtigen Schritt zur Erforschung der Beziehung zwischen Wissen und Online-

34 Michie/van Stralen/West.

35 Alohali et al.; Arachchilage/Love; Cain/Edwards/Still; Downs/Holbrook/Cranor; Holt/Bossler; Ovelgönne et al.; Parsons et al., Determining; Shillair et al.

36 Arachchilage/Love.

37 Downs/Holbrook/Cranor.

38 Alohali et al.

39 Ovelgönne et al.

40 Debatin et al.

41 Cain/Edwards/Still.

Verhalten gemacht. Die Ergebnisse sind jedoch noch unschlüssig, und es sind weitere Forschungsarbeiten erforderlich, insbesondere zur Untersuchung des tatsächlichen Online-Verhaltens und seines Zusammenhangs mit dem Wissen.

c) Gelegenheit

Gemäß dem COM-B-Framework reichen Wissen und Motivation allein möglicherweise nicht aus, um ein sicheres Online-Verhalten hervorzurufen. Es werden auch Gelegenheiten benötigt, die sich auf das soziale und materielle Umfeld beziehen, die ein Verhalten möglich oder unmöglich machen.[42] Während der Zusammenhang zwischen Gelegenheit und Verhalten die Aufmerksamkeit von Forschern in anderen Bereichen, wie z. B. dem Ernährungsverhalten, auf sich gezogen hat,[43] ist der Einfluss der Gelegenheit auf das Online-Verhalten nur wenig erforscht. Das soziale Umfeld bezieht sich darauf, wie die Menschen um uns herum unser Verhalten beeinflussen. So stehen beispielsweise die Privatsphäre-Einstellungen der Nutzer sozialer Online-Netzwerke im Zusammenhang mit der Anzahl der Online-Freunde mit privaten Profilen.[44] Darüber hinaus zeigten Herath/Rao,[45] dass der soziale Einfluss von direkten Kollegen und Managern einen großen Einfluss auf sicheres Online-Verhalten in Unternehmen haben kann. Soweit ersichtlich wurde die Beziehung zwischen dem sozialen Umfeld und dem Online-Verhalten im privaten Umfeld jedoch nicht weiter untersucht.

Das materielle Umfeld bezieht sich auf die Verfügbarkeit von finanziellen Ressourcen, Zeit und Hilfsmitteln, die sichere Praktiken unterstützen. Viele Unternehmen bieten ihren Mitarbeitern Hilfsmittel an, wie z. B. Datenschutzbildschirme, die ein sicheres Online-Verhalten ermöglichen sollen. Solche Hilfsmittel und Ressourcen können dazu beitragen, das Selbstvertrauen der Mitarbeiter in das gewünschte Verhalten (Selbstwirksamkeit) zu stärken.[46] Die Rolle, die das materielle Umfeld für das Online-Verhalten außerhalb von Unternehmen spielt, war bisher selten Gegenstand von Studien. Es ist daher unklar, wie das materielle Umfeld das Online-Verhalten in einem privaten Umfeld beeinflusst, in dem nicht die gleichen Hilfsmittel wie in einem Unternehmen zur Verfügung stehen; die Bürgerinnen und Bürger müssen selbst aktiv Sicherheitsmassnahmen beschaffen, installieren und auf dem neuesten Stand halten. Finanzielle Möglichkeiten sind daher ein relevanter Faktor: Personen, die wis-

42 Michie/van Stralen/West.
43 Michie/van Stralen/West.
44 Lewis/Kaufman/Christakis.
45 Lewis/Kaufman/Christakis.
46 Lewis/Kaufman/Christakis.

sen, dass sie keine persönlichen Fotos mit kostenlosen Übertragungswebsites verschicken sollten (Wissen), und die motiviert sind, eine sicherere – kostenpflichtige – Option zu nutzen (Motivation), brauchen auch einen finanziellen Spielraum, um dies tun zu können (Möglichkeit).

d) Andere Faktoren

Ein weiterer Faktor, der das Online-Verhalten beeinflussen kann, sind frühere Erfahrungen, wie z. B. frühere Opfererfahrungen im Internet. Frühere Erfahrungen können ein wichtiger Prädiktor für zukünftiges Verhalten sein.[47] Menschen können ihr Online-Verhalten anpassen, nachdem sie Opfer eines Cyberangriffs geworden sind, und beginnen, sich sicherer zu verhalten. So scheinen sich beispielsweise Facebook-Nutzer, die negative Erfahrungen gemacht haben, weil sie persönliche Informationen auf der Plattform geteilt haben, der Risiken stärker bewusst zu werden und sich besser zu schützen.[48] Allerdings weisen nicht alle Studien in diese Richtung, und eine frühere Viktimisierung führt nicht immer direkt zu einer Änderung des Online-Verhaltens.[49]

Es wurde auch argumentiert, dass Online-Verhalten mit der Selbstkontrolle zusammenhängt.[50] Die Theorie der Selbstkontrolle besagt, dass Menschen mit geringer Selbstkontrolle impulsiv sind, Risiken nicht vermeiden und sich hauptsächlich auf das Kurzfristige konzentrieren,[51] was ihr Risiko erhöht, Opfer von Internetkriminalität zu werden.[52] Der Zusammenhang zwischen Selbstkontrolle und Online-Viktimisierung kann jedoch auch indirekt durch andere Faktoren wie Motivation,[53] größere Online-Aktivität,[54] kriminelles Verhalten und Umgang mit Straftätern bestehen.[55] Es bleibt jedoch unklar, ob und wie die Beziehung zwischen Selbstkontrolle und Online-Viktimisierung durch das Online-Verhalten beeinflusst wird oder wie die Selbstkontrolle mit dem Online-Verhalten zusammenhängt.

Ein weiterer potenziell wichtiger Prädiktor für das Online-Verhalten ist der „locus of control" (Kontrollüberzeugung), ein Begriff, der sich auf das Verant-

---

47 Debatin et al.; Rhee/Kim/Ryu; Vance/Siponen/Pahnila.
48 Christofides, Muise, & Desmarais; Debatin et al.
49 Cain/Edwards/Still.
50 Bossler/Holt, effect; Ngo/Paternoster.
51 Gottfredson/Hirschi.
52 Ngo/Paternoster.
53 Floyd/Prentice-Dunn/Rogers.
54 van Wilsem.
55 Bossler/Holt, effect.

wortungsgefühl der Menschen in Bezug auf ihre eigene Sicherheit bezieht.[56] Ob jemand sich selbst für verantwortlich hält (d. h. „internal locus of control", d.h. der Ort der Kontrolle liegt innerhalb des Individuums) oder diese Verantwortung auf andere überträgt, z. B. auf die Polizei oder die Bank (d. h. „external locus of control", d.h. der Ort der Kontrolle liegt ausserhalb des Individuums), kann sich auf die Massnahmen auswirken, die sie ergreifen, um einen Cyberangriff zu verhindern, d. h. auf die Art und Weise, wie sie sich online verhalten.[57] Es wird erwartet, dass jemand mit einem hohen internen Kontrollzentrum Verantwortung übernimmt und motiviert ist, seine Online-Sicherheit selbst in die Hand zu nehmen. In der Tat haben frühere Studien einen positiven signifikanten Zusammenhang zwischen Kontrollüberzeugung und sicherem Online-Verhalten festgestellt.[58] Es ist jedoch auch möglich, dass eine grössere Kontrollüberzeugung zu einem falschen Gefühl der Sicherheit führt. Wenn Menschen sich zutrauen, Angriffe von Cyberkriminellen selbst abwehren zu können, unterschätzen sie möglicherweise die Online-Risiken,[59] was zu unsicherem Online-Verhalten führen kann.

III. Messung des Online-Verhaltens

Das Online-Verhalten und der Grad, in dem es sicher oder unsicher ist, wurde bisher auf zwei Arten gemessen. Einige Forscher haben das wahrgenommene Verhalten gemessen, indem sie die Befragten gefragt haben, wie sie sich normalerweise verhalten oder wie sie sich in einer fiktiven Online-Situation verhalten würden. In anderen Studien wurde das tatsächliche Online-Verhalten beobachtet. In diesem Abschnitt wird ein Überblick über die in früheren Studien verwendeten Methoden gegeben.

1. Forschung zum selbstberichteten Verhalten

Die meisten früheren Studien zum Online-Verhalten konzentrierten sich auf das selbstberichtete Verhalten. Die Befragten in diesen Studien wurden anhand von Items (z. B. „Ich öffne E-Mails von unbekannten Absendern") oder Fragen („Wie viel Prozent Ihrer Passwörter ändern Sie alle drei Monate?") zu ihrem Verhalten befragt.[60] Ein Beispiel für ein Forschungsinstrument, das mit Antwortvorschlägen arbeitet, ist der Human Aspects of Information Security

---

56 Rotter.

57 Debatin et al.; Jansen; Workman/Bommer/Straub.

58 Jansen; Workman/Bommer/Straub.

59 Rhee/Kim/Ryu.

60 Cain/Edwards/Still; Crossler/Bélanger.

Questionnaire (d. h. HAIS-Q).[61] Dieses Instrument misst insbesondere das Wissen, die Einstellungen und das wahrgenommene Verhalten zu einer Reihe von relevanten Themen, wie z. B. Passwortmanagement.

Selbstberichtete Verhaltensweisen können auch in der Fragebogenforschung mithilfe von Vignetten und Rollenspielen untersucht werden.[62] Diese Methoden ermöglichen es, die Befragten zu dem Verhalten zu befragen, das sie ihrer Meinung nach in einer fiktiven, von den Forschern vorgegebenen Situation zeigen würden.[63] Ein wichtiger Vorteil dieser Forschungsmethode besteht darin, dass sie es den Forschern ermöglicht, situative Faktoren zu ermitteln, die in der Fragebogenforschung zu Verzerrungen führen könnten. In einem Rollenspiel können die Forscher einerseits bestimmte Faktoren bei allen gleichsetzen (z. B. „Stellen Sie sich vor, Ihr Name ist Tom Johnson und Sie arbeiten in einer Bäckerei"). Andererseits können die Forscher Faktoren manipulieren, indem sie Untergruppen von Befragten eine angepasste Situation präsentieren. So können die Forscher beispielsweise zwischen Untergruppe eins („Stellen Sie sich vor, Sie sind noch nie Opfer eines Verbrechens geworden") und Untergruppe zwei („Stellen Sie sich vor, Sie wurden in der Vergangenheit in einem Online-Webshop betrogen") unterscheiden. Basierend auf den skizzierten Umständen werden die Befragten gefragt, wie sie in dieser Situation handeln würden.[64]

Die Fragebogenforschung hat als Forschungsmethode mehrere Vorteile. Zum Beispiel sind die Kosten für Befragungen relativ gering, während damit eine grosse repräsentative Forschungspopulation erreicht werden kann. Die Antworten auf standardisierte Fragen eignen sich auch für die quantitative Analyse, um erklärende Faktoren zu unterscheiden und Antworten zwischen den Befragten leicht vergleichen zu können.

Die Erforschung des Verhaltens anhand von Fragebögen und Vignetten hat jedoch auch Nachteile. Bei Studien zum selbstberichteten Verhalten konzentrieren sich die Forscher darauf, wie sich die Menschen nach eigenen Angaben typischerweise online verhalten oder wie sie sich in einer hypothetischen Situation verhalten würden. Obwohl die meisten Menschen angeben, dass Cybersicherheit wichtig ist,[65] entspricht ihr selbst angegebenes Verhalten nicht

61 Parsons et al., Determining; Parsons et al., Human.

62 Downs/Holbrook/Cranor; Jong/Leukfeldt/van de Weijer; Sheng et al..

63 Vance/Siponen/Pahnila.

64 Downs/Holbrook/Cranor; Jong/Leukfeldt/van de Weijer; Sheng et al..

65 Madden/Rainie.

immer ihrem tatsächlichen Verhalten.[66] Wenn sich die Forschung ausschließlich auf das selbstberichtete Online-Verhalten konzentriert, kann sie ein falsches Bild davon vermitteln, wie sich Menschen tatsächlich online verhalten.

2. Forschung zum tatsächlichen Online-Verhalten

Anstelle des selbstberichteten Verhaltens kann die Forschung auch das tatsächliche Verhalten messen. Bisherige Studien, in denen das tatsächliche Verhalten gemessen wurde, sind im Bereich der Cybersicherheit rar. Die Studien, die durchgeführt wurden, konzentrieren sich meist auf Phishing-Viktimisierung. In diesen Studien werden häufig Phishing-Tests durchgeführt, bei denen sowohl gefälschte Phishing-E-Mails als auch legitime E-Mails verwendet werden, um den Grad der Anfälligkeit für Phishing zu messen, d. h. um die Widerstandsfähigkeit gegenüber Phishing-Angriffen zu testen.[67] Indem gemessen wird, wie oft die Hyperlinks in den E-Mails angeklickt werden und wie oft Personen, die darauf klicken, tatsächlich vertrauliche oder persönliche Informationen auf einer legitimen oder einer Phishing-Website hinterlassen, kann ermittelt werden, wie sicher sich Menschen online in Bezug auf Phishing verhalten. Ein wichtiger Einwand gegen diese Methode ist, dass Menschen zu Forschungszwecken in die Irre geführt werden, da die Teilnehmer an einem Phishing-Test oft nicht im Voraus ihre Zustimmung zur Teilnahme gegeben haben.

Kaptein et al.[68] untersuchten, wie leicht es ist, Menschen dazu zu bringen, persönliche Informationen preiszugeben. Genauer gesagt untersuchten sie E-Mail-Adressen, die Cyberkriminelle bei Phishing-Angriffen verwenden. Die Teilnehmer füllten zunächst eine Umfrage aus, die aus so genannten Dummy-Fragen bestand: Die Fragen spielten keine Rolle. Die eigentliche Messung fand statt, nachdem die Befragten die Umfrage abgeschlossen hatten. Die Befragten wurden gebeten, E-Mail-Adressen von Freunden und Bekannten anzugeben, die möglicherweise ebenfalls an der Umfrage teilnehmen wollten. Bei dieser Aufforderung wurden verschiedene Überredungstechniken angewandt. So wurde den Befragten beispielsweise mitgeteilt, dass andere Befragte bereits verschiedene E-Mail-Adressen an die Forscher weitergegeben hatten (Social Proof) oder dass sie die Ergebnisse der Studie zugeschickt bekämen, wenn sie mindestens eine E-Mail-Adresse angeben würden (Reziprozität). Die Anwendung einer Überzeugungstechnik führte dazu, dass deutlich mehr E-Mail-Adressen gewonnen wurden.

---

66 Smith/Louis; Spiekermann/Grossklags/Berendt.

67 Siehe z.B. Cain/Edwards/Still für einen Überblick.

68 Kaptein et al.

Junger/Montoya Morales/Overink[69] sind noch einen Schritt weiter gegangen. Sie untersuchten, wie einfach es ist, Menschen dazu zu verleiten, persönliche Daten anzugeben, die für eine effektivere Form des Phishings verwendet werden können, nämlich das Spear-Phishing, bei dem die persönlichen Daten des Opfers verwendet werden, um ihm ein falsches Gefühl der Sicherheit zu vermitteln. Im Rahmen der Studie wurden Personen auf der Straße angesprochen, um an einer Umfrage teilzunehmen. In dieser Umfrage wurde eine Reihe von Fragen zum Online-Einkaufsverhalten gestellt: ob sie schon einmal etwas online gekauft hatten, und wenn ja, wo und was. Sie wurden auch gebeten, einen Teil ihrer persönlichen Identifikationsnummer und E-Mail-Adresse anzugeben. Überraschenderweise waren die Menschen bereit, den Interviewern solche persönlichen Informationen zu geben. Mit diesen Informationen lässt sich möglicherweise ein sehr gezielter und effektiver (Spear-)Phishing-Angriff durchführen.

Diese Art von Studien hat jedoch auch einige Nachteile. Obwohl sie bessere Messungen des tatsächlichen Online-Verhaltens liefern, werden die Studien oft in kleinem Massstab durchgeführt und es werden nur wenige andere Faktoren erhoben. Daher kann das beobachtete tatsächliche Online-Verhalten nicht auf erklärende Faktoren zurückgeführt werden. Ausserdem sind Messungen des tatsächlichen Verhaltens nicht in allen Situationen durchführbar, zum Beispiel wenn wir wissen wollen, wie sich Menschen während eines tatsächlichen Ransomware-Angriffs verhalten. Darüber hinaus können solche Messungen kostspielig und zeitaufwändig sein.

3. Selbstberichtetes Verhalten versus tatsächliches Verhalten

Das Online-Verhalten kann also auf verschiedene Weise gemessen werden. Wir argumentieren, dass Messungen des tatsächlichen Verhaltens den Selbstberichten über das Verhalten vorzuziehen sind. Selbstberichte können von der Realität abweichen, weil sie an die Erinnerung der Befragten appellieren oder weil die Befragten möglicherweise sozial erwünschte Antworten geben. Daher können Messungen des tatsächlichen Online-Verhaltens einen wichtigen Beitrag zu unserem Wissen über die Umstände leisten, die das Online-Verhalten beeinflussen.[70] Allerdings haben solche Messungen auch praktische Nachteile. Für jede Studie muss daher die am besten geeignete Methode zur Messung des Online-Verhaltens im Hinblick auf Kosten und Nutzen bestimmt werden.

---

69 Junger/Montoya Morales/Overink.

70 Maimon/Louderback.

Eine Kombination des Besten aus beiden Welten kann durch ein „bevölkerungsbasiertes Umfrageexperiment", auch „experimentelle Umfrage" genannt, erreicht werden.[71] Diese Methode verbindet die Vorteile der Fragebogenforschung, wie die Möglichkeit, eine grosse repräsentative Stichprobe zu untersuchen, mit den Vorteilen der experimentellen Forschung, bei der das tatsächliche Verhalten gemessen und kausale Zusammenhänge ermittelt werden können.[72] In der Praxis besteht eine solche experimentelle Umfrage häufig aus einem Online-Fragebogen mit integrierten Experimenten. Die Befragten können durch diese Experimente manipuliert werden (z. B. durch Auferlegung von Zeitdruck). Darüber hinaus können während der Umfrage Messungen des tatsächlichen Verhaltens vorgenommen werden....

IV. Studie über Online-Verhalten und Viktimisierung

1. Überblick über das Forschungsinstrument

Ziel der Studie über Online-Verhalten und Viktimisierung war es, ein Forschungsinstrument zu entwickeln, mit dem das tatsächliche Online-Verhalten gleichzeitig mit möglichen Erklärungsfaktoren, die sich aus der Literatur ergeben haben, gemessen werden kann. Es wurde ein bevölkerungsbasiertes Erhebungsexperiment verwendet, das aus einem Fragebogen mit Fragen und Vignetten zum selbstberichteten Online-Verhalten und den in Abschnitt II.2. diskutierten Erklärungsfaktoren (in Tabelle 1 dargestellt) sowie aus Messungen des tatsächlichen Online-Verhaltens mit experimentellen Manipulationen besteht. Darüber hinaus werden Hintergrundmerkmale der Befragten (z. B. Alter, Geschlecht, Bildungsniveau, beruflicher Status), die Stimmung der Befragten (z. B. das Ausmaß, in dem sich jemand optimistisch oder deprimiert fühlt) und das verwendete Gerät gemessen, um als Kontrollvariablen einbezogen zu werden. Abbildung 1 zeigt schematisch die Reihenfolge, in der die verschiedenen Abschnitte der Umfrage den Befragten vorgelegt werden.[73] Die verwendeten Items basieren auf bestehenden Fragebögen, die, falls erforderlich, ins Niederländische übersetzt und an den spezifischen Kontext dieser Studie angepasst wurden. Wenn kein Fragebogen zur Verfügung stand, wie z. B. für die Messung der Chancen, wurde ein Fragebogen von den Forschern selbst entwickelt.

---

71 Mutz.

72 Mullinix et al.

73 Eine englische Übersetzung des niederländischen Originalfragebogens ist auf Anfrage bei den Autoren erhältlich.

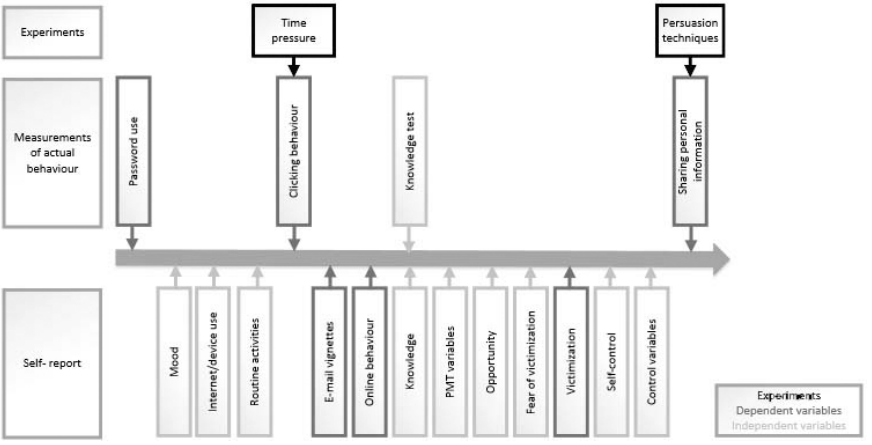

Abbildung 1: Schematischer Überblick über die Reihenfolge der Erhebungsabschnitte

Teil der Befragung	**Theoretische Grundlage**	**Thema**
Motivation	**PMT und COM-B**	**Motivation zum Schutz**
Wissen	COM-B	Selbsteinschätzung des Wissens über Online-Sicherheit
		Wissenstest (objektiv)
Gelegenheit	COM-B	Materielles Umfeld
		Soziales Umfeld
Stimmungslage		Stimmungslage (PANAS)
Viktimisierung		Kriminalitätsfurcht
	PMT	Frühere Online-Viktimisierung
Selbstkontrolle		Self-control (BSCS)
Gerät		Art des Geräts, das zum Ausfüllen der Umfrage verwendet wurde
		Nutzung von Online-Geräten
		Sicherheitsmassnahmen
Zeitdruck		Zeitdruck
Überredungstechnik		Autorität
		Reziprozität

Teil der Befragung	Theoretische Grundlage	Thema
Motivation	**PMT und COM-B**	**Motivation zum Schutz**
Einschätzung der Bedrohung	PMT	Wahrgenommene Verwundbarkeit
		Wahrgenommener Schweregrad
Einschätzung der Coping-Fähigkeiten	PMT	Wirksamkeit der Reaktion
		Selbstwirksamkeit
		Reaktionskosten
Locus of Control		Kontrollüberzeugung
Kontrollierende Faktoren		Geschlecht
		Bildungsgrad
		Alter
		Tägliche Aktivität/Beschäftigung
		Zusammenlebend (ja/nein)
		Kinder (< 16 Jahre) im Haushalt
Routineaktivitäten		Internet-Nutzung
		Online-Aktivitäten

Tabelle 1: Überblick über die Themen der Umfrage, die nicht das Online-Verhalten betreffen

2. Messung von sieben Clustern des Online-Verhaltens

Das in diesem Kapitel vorgestellte Forschungsinstrument misst sieben Verhaltenscluster, die auf der Literaturstudie basieren. In dieser experimentellen Umfrage wird das Online-Verhalten auf drei Arten gemessen. Erstens werden alle Verhaltenskomplexe durch Selbstauskünfte gemessen (siehe Tabelle 2 und Items in Anhang 1). Zweitens wurden echte Phishing-E-Mails so angepasst, dass sie als Vignetten verwendet werden konnten, um den Umgang der Befragten mit (Phishing-)E-Mails zu messen. Den Befragten werden drei E-Mails gezeigt, die an eine fiktive Person adressiert sind: zwei Phishing-E-Mails, die angeblich von einer Bank und einer Festivalorganisation stammen, und eine legitime E-Mail von einem Internetanbieter. Die Befragten wurden gebeten, so zu tun, als seien sie diese fiktive Person. Die Befragten wurden dann gebeten, aus neun Optionen zu wählen, wie sie auf jede dieser E-Mails reagieren wür-

den (z. B. antworten, auf einen Link klicken usw.). Die Befragten verhalten sich unsicher, wenn sie angeben, die verlinkte Website aus einer oder beiden Phishing-E-Mails zu öffnen.

Drittens werden die Befragten beim Ausfüllen der Umfrage mit (fiktiven) Cyber-Risikosituationen konfrontiert (siehe IV.2. für weitere Einzelheiten), um das tatsächliche Online-Verhalten in den Clustern „Passwortmanagement", „Online-Wachsamkeit" und „Online-Weitergabe von persönlichen Informationen" zu messen. Es erwies sich aus mehreren Gründen als unmöglich, das tatsächliche Online-Verhalten innerhalb der anderen Verhaltenskategorien zu messen. Erstens ist die Nachahmung von Cyberkriminalität nicht immer möglich oder moralisch gerechtfertigt, z. B. bei der Prüfung technischer Präventivmassnahmen. In einigen Fällen hat es sich auch als technisch nicht machbar erwiesen, eine Messung in zufriedenstellender Weise in den Fragebogen einzubauen. Daher wurde ein pragmatischer Ansatz gewählt und beschlossen, das Verhalten nur dann objektiv zu messen, wenn dies praktisch machbar und moralisch vertretbar ist. Tabelle 2 gibt einen Überblick über die Art und Weise, wie die einzelnen Online-Verhaltensgruppen in der Erhebung gemessen werden.

Online-Verhalten	**Methode**		
	Selbstauskunft Fragebogen	**Selbstauskunft Vignette**	**Objektive Messung**
1. Passwort-Verwaltung	Ja		Ja: Passwort-Stärke Keine experimentelle Variante
2. Sichern wichtiger Dateien	Ja		
3. Installation von Updates	Ja		
4. Verwendung von Sicherheitssoftware	Ja		
5. Online-Wachsamkeit	Ja		Ja: Klick-Verhalten Experimentelle Variante: Zeitdruck
6. Online-Offenlegung von persönlichen Informationen	Ja		Ja: Offenlegung von persönlichen Informationen Experimentelle Varianten: Überzeugungstechniken

Online-Verhalten	Methode		
	Selbstauskunft Fragebogen	**Selbstauskunft Vignette**	**Objektive Messung**
7. Umgang mit Anhängen und Hyperlinks in E-Mails	Ja	Ja	

Tabelle 2: Überblick über die Messungen des Online-Verhaltens nach Verhaltensclustern

3. Detaillierte Beschreibung der Messungen des tatsächlichen Online-Verhaltens

Die Messungen des tatsächlichen Online-Verhaltens in der experimentellen Erhebung der Online Behaviour and Victimization Study werden nun im Detail beschrieben. Es gibt drei objektive Messungen des Online-Verhaltens, die in der Umfrage enthalten sind (Tabelle 2). Beim Ausfüllen der Umfrage wurden die Befragten ohne ihr Wissen mit drei simulierten Cyber-Risikosituationen konfrontiert, und es wurde erfasst, wie die Befragten mit diesen Situationen umgehen. Zunächst wurden die Befragten zu Beginn des Fragebogens gebeten, aus Gründen des Datenschutzes einen Benutzernamen und ein Passwort zu erstellen (siehe Abbildung 2). Das gewählte Passwort wurde zwar nicht registriert, aber die Stärke des gewählten Passworts wurde gemessen. Dies ermöglicht es, die Stärke der Passwörter zu bestimmen, die die Befragten zum Schutz ihrer persönlichen Daten wählen. Am Ende der Umfrage wurde den Befragten eine Kontrollfrage gestellt, um herauszufinden, ob sie normalerweise eine ähnliche Art von Passwort wählen würden: „Haben Sie ein ähnliches Passwort gewählt wie das, das Sie normalerweise zum Schutz Ihrer persönlichen Daten wählen würden?“

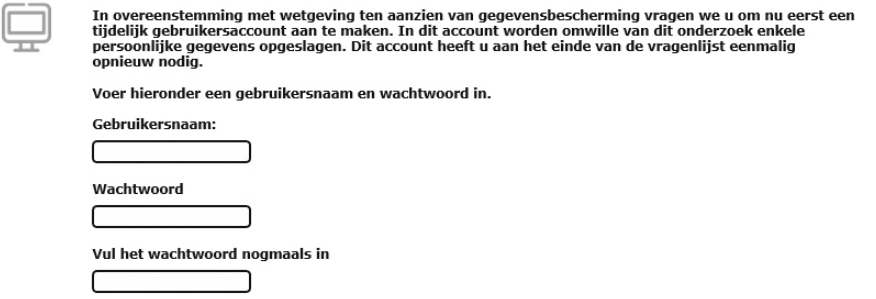

Abbildung 2: Screenshot der Messung der Passwortverwaltung[74]

Im weiteren Verlauf der Umfrage wurde gemessen, inwieweit die Befragten online aufmerksam sind. Die Befragten wurden gebeten, sich ein kurzes Video anzusehen, bevor sie die nächste Frage beantworten. Das Video wurde jedoch nicht abgespielt. Plötzlich erschien ein Pop-up-Fenster mit dem Hinweis, dass eine Software namens „Vidzzplay“ heruntergeladen werden muss (siehe Abbildung 3). Diese Software stammt angeblich aus einer unbekannten Quelle (und ist daher unzuverlässig). Hier können die Forscher sehen, welche Wahl die Befragten treffen: die Software herunterladen (unsichere Wahl), nicht herunterladen (sichere Wahl) oder die Frage überspringen (sichere Wahl).

[74] Ransomware ist eine Schadsoftware, die einen Computer blockiert oder Dateien verschlüsselt. Erst wenn die betroffene Person ein Lösegeld zahlt, kann sie den Computer oder die Dateien wieder nutzen.

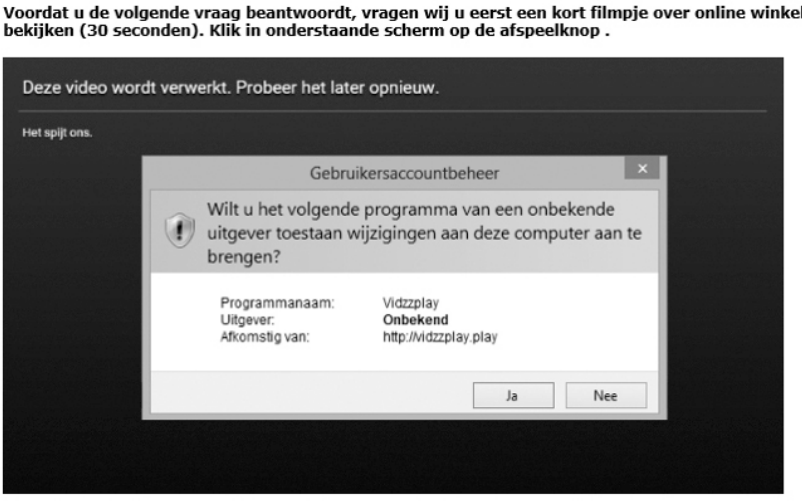

Abbildung 3: Screenshot der Messung der Online-Wachsamkeit[75]

Drittens wurden die Befragten am Ende des Fragebogens gebeten, persönliche Daten anzugeben. Dieser Teil begann mit Standardfragen wie dem Familienstand, aber der Datenschutzwert der Informationen stieg mit jeder Frage, z. B. nach dem vollständigen Namen, dem Geburtsdatum und der E-Mail-Adresse, und endete mit der Frage nach den letzten drei Ziffern ihres Bankkontos. Bei jeder Frage hatten die Befragten die Möglichkeit, auf die Schaltfläche „Ich möchte lieber nichts sagen" zu klicken, was als sichere Wahl gilt. Wenn die Befragten ihre persönlichen Daten ausfüllten, wurde der Inhalt ihrer Antwort nicht registriert, sondern nur, dass sie die Frage beantwortet hatten. Je mehr Arten von persönlichen Informationen die Befragten angaben, desto unsicherer ist ihr Verhalten.

4. Experimente

In zwei der Messungen des tatsächlichen Online-Verhaltens waren experimentelle Bedingungen enthalten (Tabelle 2). In diesen Fällen wurden verschiedenen Untergruppen von Befragten Variationen einer objektiven Messung des tatsächlichen Online-Verhaltens vorgelegt. Im ersten Experiment wurde bei der objektiven Messung des „Klickverhaltens", bei der die Befragten aufge-

[75] Spear-Phishing ist ein gezielter Phishing-Angriff gegen eine Person oder eine bestimmte Gruppe von Personen.

fordert werden, Software herunterzuladen, die Hälfte der Befragten unter Zeitdruck gesetzt. Die Befragten wurden gebeten, einen Teil der Umfrage in höchstens fünf Minuten auszufüllen. In der Versuchsbedingung wurde den Befragten gesagt, dass diese Zeit für frühere Befragte nicht ausreichend war, und sie wurden aufgefordert, schnell zu arbeiten. Die anderen Befragten wurden darüber informiert, dass fünf Minuten ausreichend sind und dass sie in ihrem eigenen Tempo weiterarbeiten können. Dann wurden die Befragten zu ihren Online-Routineaktivitäten befragt. Danach wurden die Befragten gebeten, sich ein Video anzusehen, und es erschien ein Pop-up mit der Bitte um Erlaubnis für einen Software-Download (Messung des tatsächlichen Klickverhaltens). Im Anschluss daran wurden Kontrollfragen zum erlebten Zeitdruck gestellt.

Das zweite Experiment fand während der objektiven Messung der „Online-Offenlegung persönlicher Daten" statt, bei der die Befragten aufgefordert wurden, persönliche Daten wie ihre Adresse und die letzten drei Ziffern ihrer Kontonummer einzugeben. Es wurden verschiedene Überzeugungstechniken eingesetzt, um die Bereitschaft der Befragten zur Weitergabe persönlicher Daten zu manipulieren (⅓ die Überzeugungstechnik „Autorität", ⅓ die Überzeugungstechnik „Gegenseitigkeit", ⅓ keine Überzeugungstechnik). Allen Befragten wurde gesagt: „Wir würden Ihnen gerne einige abschliessende Fragen stellen". Ein Drittel der Befragten ging zu den Fragen nach persönlichen Informationen über, ohne eine Überzeugungstechnik anzuwenden. In der Kategorie Reziprozität (ein Drittel der Befragten) wurde den Befragten die Chance auf einen Gutschein versprochen, wenn sie alle Fragen zu persönlichen Informationen vollständig beantworten. In der Kategorie Autorität (ein Drittel der Befragten) drängten die Forscher die Befragten aufgrund der Bedeutung der wissenschaftlichen Studie dazu, alle persönlichen Angaben vollständig zu machen.

V. Diskussion

In diesem Beitrag wurde die Entwicklung eines Forschungsinstruments für die Studie *Online Behaviour and Victimization Study* beschrieben. Die zu Beginn dieser Studie durchgeführte Literaturrecherche zeigt deutlich, dass es an Studien mangelt, die das tatsächliche Online-Verhalten messen. Eine Erklärung dafür ist, dass dieser Forschungsbereich noch relativ jung ist. Die meisten Studien, die durchgeführt wurden, können als explorativ angesehen werden oder testen hauptsächlich, ob bestehende kriminologische oder psychologische Modelle zur Erklärung des selbstberichteten unsicheren Online-Verhaltens oder der Viktimisierung von Internetkriminalität verwendet werden

können.[76] Die verfügbaren Studien, in denen das tatsächliche Online-Verhalten gemessen wurde, hatten mit Einschränkungen zu kämpfen, da beispielsweise eine nicht repräsentative Stichprobe verwendet wurde. Darüber hinaus haben diese Studien zwar wertvolle Ergebnisse zur Prävalenz unsicheren Online-Verhaltens geliefert, sich aber nur selten auf ein breites Spektrum an erklärenden Faktoren ausgerichtet. Ein möglicher Zusammenhang zwischen Faktoren wie Wissen und Motivation und der Prävalenz des tatsächlichen (objektiv gemessenen) Online-Verhaltens ist bisher kaum untersucht worden. Auch der Zusammenhang zwischen unsicherem tatsächlichen Online-Verhalten und Online-Viktimisierung wurde bisher kaum untersucht. In einigen Studien wurde zwar beschrieben, dass Online-Viktimisierung auf unsicheres Online-Verhalten zurückgeführt werden kann, wie z. B. die Weitergabe persönlicher Informationen im Internet, doch bleibt unklar, wie unsicheres Online-Verhalten das Risiko der Online-Viktimisierung beeinflusst oder wie dies mit individuellen oder kontextuellen Faktoren zusammenhängen könnte.

Mit der *Online Behaviour and Victimization Study* wurde daher ein Forschungsinstrument entwickelt, das in verschiedener Hinsicht neue Möglichkeiten für das Forschungsfeld bietet. Es wurde bewusst entschieden, sowohl das selbstberichtete als auch das tatsächliche Online-Verhalten zu messen. Schliesslich wissen wir, dass, obwohl die meisten Menschen angeben, Cybersicherheit sei wichtig, das tatsächliche Verhalten der Menschen nicht immer mit ihren Einstellungen oder ihrem wahrgenommenen Verhalten übereinstimmt. Durch die Verwendung eines bevölkerungsbasierten Umfrageexperiments – eine Methode, die die Vorteile der Fragebogenforschung mit den Vorteilen von Experimenten verbindet – ist der Mehrwert dieses Forschungsinstruments offensichtlich: Dieses Instrument ermöglicht es, über bestehende Studien hinauszugehen, indem es das tatsächliche Online-Verhalten in einer grossen repräsentativen Stichprobe misst. Darüber hinaus ist dieses Instrument auch in anderer Hinsicht innovativ: Wir zielen nicht nur darauf ab, die Viktimisierung bestimmter Formen von Cyberkriminalität zu erklären, sondern auch mehrere Cluster von Online-Verhalten. Schließlich sind es Verhaltensweisen, die das Risiko für alle Arten von Online-Kriminalität erhöhen.

Bei der Konzeption der experimentellen Umfrage ergaben sich mehrere ethische Fragen, die im Einzelnen erörtert werden sollten. Während der experimentellen Umfrage werden den Befragten verschiedene fiktive Cyber-Risikosituationen präsentiert. Die Befragten werden auch aufgefordert, ein Passwort zu erstellen und persönliche Daten einzugeben. Darüber hinaus wurde befürchtet, dass (im Vergleich zu anderen Studien) auffällige Fragen und

[76] Für einen Überblick siehe Leukfeldt, Research.

Situationen die Befragten abschrecken würden, was zu einer hohen Zahl von Abbrüchen oder Kontakten mit dem Helpdesk führen könnte.[77] Eine Ethikkommission der Universität hat daher das Instrument genehmigt. Die Abfrage eines Passworts und persönlicher Daten ist ethisch zulässig, wenn die Antworten nicht registriert werden. So bleibt den Forschern beispielsweise unbekannt, welches Passwort die Befragten wählen, nur wie stark dieses Passwort ist. Darüber hinaus werden die persönlichen Daten, die die Befragten ausfüllen, nicht an die Forscher weitergegeben, sondern nur, ob die Befragten eine bestimmte Frage zu persönlichen Informationen beantworteten oder nicht. Schliesslich wurden alle Befragten (so weit wie möglich) im Voraus durch eine „informierte Zustimmung" informiert und anschliessend durch eine „Nachbesprechung" über die Cyber-Risikosituationen und Manipulationen informiert, denen sie „ausgesetzt" waren (unabhängig davon, ob die Befragten die Umfrage abgeschlossen haben oder nicht).

Wie jedes Messinstrument hat auch dieses Forschungsinstrument seine Grenzen. Erstens misst das Forschungsinstrument sowohl abhängige als auch erklärende Faktoren zum gleichen Zeitpunkt. Um kausale Zusammenhänge zwischen Verhalten und Viktimisierung zu untersuchen, ist eine zweite Welle der Datenerhebung erforderlich, bei der insbesondere die Viktimisierung durch Internetkriminalität im Zeitverlauf gemessen wird.

Zweitens haben die objektiven Messungen und Experimente auch jeweils ihre eigenen Grenzen. Aufgrund der Länge des Fragebogens war es nicht möglich, objektive Messungen und Experimente für alle sieben Verhaltenscluster aufzunehmen. Darüber hinaus wird zwar die Passwortstärke ermittelt, aber es bleibt unbekannt, ob das Passwort einmalig ist und vom Befragten nie in anderen Anwendungen verwendet wird, was eine zweite Voraussetzung für eine sichere Passwortverwaltung ist. Darüber hinaus werden die Informationen, die die Befragten weitergeben, gemäß der Datenschutz-Grundverordnung[78] nicht aufgezeichnet, so dass nicht überprüft werden kann, ob es sich um tatsächliche/richtige Daten handelt. Bei der Messung, ob die Befragten unsichere Software heruntergeladen haben oder nicht (d. h. beim Klickverhalten), verwendet das Instrument ein Popup-Fenster im Stil des Windows-Betriebssystems. Nicht-Windows-Benutzer sind mit dem Pop-up weniger vertraut, was sie möglicherweise misstrauischer macht und die Wahrscheinlichkeit verringert, dass sie

[77] Bei einem Pilotversuch mit dem Forschungsinstrument trat dieser Effekt jedoch nur selten auf.

[78] Allgemeine Datenschutz-Verordnung (General Data Protection Regulation GDPR), <https://gdpr-info.eu/>.

die Frage bejahen. Diese objektive Messung muss weiterentwickelt werden, und zwar mit verschiedenen Pop-ups, die technisch gesehen echte Pop-ups sind und an verschiedene Geräte und Betriebssysteme angepasst werden.

Drittens: Obwohl die Methode – eine Umfrage mit Experimenten – für diese Art von Forschung sehr gut geeignet ist, ist es möglich, dass sich die Befragten in der Online-Umgebung der Umfrage sicher fühlen. Infolgedessen treffen sie möglicherweise schneller unsichere Entscheidungen als in tatsächlichen Cyber-Risikosituationen im wirklichen Leben. Dies kann bedeuten, dass der Prozentsatz des unsicheren Verhaltens in der häuslichen Umgebung geringer ist als durch das Forschungsinstrument ermittelt. Es ist jedoch wichtig zu erwähnen, dass der Zweck des Forschungsinstruments darin besteht, das Online-Verhalten in einer scheinbar sicheren Umgebung zu messen – Kriminelle imitieren oft auch eine sichere Umgebung (z. B. eine Online-Bank oder einen Webshop) und verleiten Menschen dazu, auf einen Hyperlink zu klicken oder persönliche Informationen preiszugeben.

Schließlich ist es möglich, dass sich Teilnehmer von Nicht-Teilnehmern in Bezug auf nicht registrierte Eigenschaften unterscheiden. Angesichts des Ziels der Studie werden die Befragten im Voraus nicht vollständig über den Inhalt der Studie informiert. Die Befragten erwarten, dass sie nur Fragen darüber beantworten, was sie online tun. Bestimmte Fragen könnten Teilnehmer, die misstrauisch sind, abschrecken. Daher könnten Befragte, die misstrauischer/aufmerksamer sind, die Studie schneller abbrechen.

Trotz der hier erwähnten Einschränkungen ermöglicht dieses Forschungsinstrument die Untersuchung des selbstberichteten Online-Verhaltens und des tatsächlichen Online-Verhaltens sowie der Unterschiede zwischen beiden und die Erklärung des Auftretens von unsicherem Online-Verhalten und der Viktimisierung durch Internetkriminalität. Dies ist relevant für künftige Interventionen, die darauf abzielen, das Online-Verhalten sicherer zu machen…

Literaturverzeichnis

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior. *Information and Computer Security*. https://doi.org/10.1108/ICS-03-2018-0037

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Mis Quarterly*, 39(4).

Bossler, A. M., & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3(1), 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research*, 27(6), 714–731.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, (518).

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database*, 45(4), 51–71.

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, 32, 90–101.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups – 2nd annual eCrime researchers summit* (pp. 37–44). New York, New York, USA: ACM Press.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30,(2,), 407–429.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125.

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, 29(4), 420–436.

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Doctoral thesis. Gildeprint.

Jansen, J., & Leukfeldt, R. (2015). How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. In *Proceedings – 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015* (pp. 24–31).

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*, 6(2), 205–228.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, 25(2), 165–180.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, 53(2), 22–30.

Jong, L., Leukfeldt, R., & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift Voor Veiligheid*, 17(1–2), 66–78.

Junger, M., Montoya Morales, A. L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66.

Kaptein, M., Markopoulos, P., De Ruyter, B., & Aarts, E. (2009). Can you be persuaded? Individual differences in suceptibility to persuasion. In *IFIP Conference on Human-Computer Interaction. Springer, Berlin, Heidelberg.* (pp. 115–118).

Kaye, J. (2011). Self-reported password sharing strategies. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems – CHI 2011*, 2619.

Leukfeldt, E.R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555.

Leukfeldt, E.R. (Ed.). (2017). *Research Agenda the Human Factor in Cybercrime and Cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E.R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology*, 57(3), 704–722.

Leukfeldt, E.R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263–280.

Leukfeldt, Eric Rutger, Notté, R. J., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders*, 15(1), 60–77.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79–100.

Lusthaus, J. (2018). Honour Among (Cyber)thieves? *European Journal of Sociology*, 59(2), 191–223.

Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1).

Michie, S., Stralen, M. M. Van, & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions, *42*(6).

Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The Generalizability of Survey Experiments. *Journal of Experimental Political Science*, *2*(2), 109–138.

Mutz, D. C. (2011). *Population-based survey experiments*. Princeton: Princeton University Press.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection Motivation Theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour* (pp. 81–127). Open University Press.

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology*, *8*(4), 1–25.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*.

Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behaviour relationship. *British Journal of Social Psychology*, *47*(4), 647–666.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd Generation E-Commerce : Privacy Preferences versus actual Behavior. *ACM Conference on Electronic Commerce*, 1–10.

Symantec. (2018). *Security Center White Papers*. Retrieved from https://www.symantec.com/security-center/white-papers

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 – 5th International Conference on Availability, Reliability, and Security*, 196–203.

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of Bluetooth security. *Information Management and Computer Security*, *20*(5), 364–381.

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559.

Van Wilsem, J. (2013). „Bought it, but never got it" assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816.

Appendix

R = Umgekehrt formulierte Frage-Items

Fragen
Passwort-Verwaltung
Ich teile meine persönlichen Passwörter mit anderen (R)
Ich verwende einfache, kurze Passwörter, z. B. mit nur 1 Zahl oder einem Großbuchstaben (R)
Ich verwende dasselbe Passwort für verschiedene Anwendungen, zum Beispiel für soziale Medien, Online-Banking und Webshops (R)
Sichern von wichtigen Dateien
Ich erstelle Sicherheitskopien von wichtigen Dateien
Ich speichere persönliche Informationen verschlüsselt, so dass andere sie nicht ohne weiteres lesen können
Installation von Updates
Ich installiere Betriebssystem-Updates auf meinen Geräten, sobald ein neues Update verfügbar ist
Ich installiere Updates für die von mir verwendeten Anwendungen oder Software, sobald ein neues Update verfügbar ist
Ich aktualisiere meine Sicherheitssoftware, sobald ein neues Update verfügbar ist

Fragen
Verwendung von Sicherheitssoftware
Auf meinen Geräten ist eine Sicherheitssoftware installiert, die nach Viren und anderer schädlicher Software sucht
Ich verwende Browsererweiterungen,[79] die mir helfen, sicher zu surfen, z. B. Software zum Blockieren von Werbung oder Pop-ups
Online-Wachsamkeit
Ich lade Software, Filme, Spiele oder Musik aus illegalen Quellen herunter (R)
Ich nutze öffentliches Wi-Fi (z. B. in Hotels, Restaurants, Bars oder öffentlichen Verkehrsmitteln) ohne VPN-Verbindung[80] (R)
Ich überprüfe die Datenschutzeinstellungen meiner Geräte, Apps oder sozialen Medien
Online-Weitergabe von persönlichen Informationen
Ich gebe persönliche Informationen wie meine Wohnadresse, E-Mail-Adresse oder Telefonnummer über soziale Medien weiter (R)
Ich bin wählerisch bei der Annahme von Verbindungsanfragen in sozialen Medien von anderen
Umgang mit Anhängen und Hyperlinks in E-Mails
Ich lösche E-Mails, denen ich nicht traue, sofort
Wenn ich Zweifel an der Echtheit einer E-Mail habe, kontaktiere ich den Absender, um zu fragen, ob eine E-Mail tatsächlich an mich gesendet wurde
Ich öffne Anhänge in E-Mails, auch wenn die E-Mail von einem unbekannten Absender stammt (R)

79 Für einen Überblick siehe z.B. Leukfeldt, Research.

80 Crossler et al.; Debatin et al.