

Ultrativ wissenschaftlich geprüft.

Heads up: Ein riesen, riesen Lob und Dank an Ultrativ. Er hat Quellen unter seinem Video angegeben, die dieses Video erst möglich machten, und auf die Frage, ob ich sein Video im Stream und jetzt hier verwenden darf, direkt zugestimmt. Dafür schonmal vorab ein riesen Dankeschön, das ist ein sehr gutes Zeichen, dass es ihm um Information und Wissensvermittlung geht.

In diesem Sinne - lasst uns starten:

Ultrativ hat vor nun 3 Wochen ein Video mit dem Titel

📺 **Virenschutz: Das digitale Schlangenöl** hochgeladen. Wir wollen uns einmal anschauen, auf welches Fundament dieses Video gebaut ist:

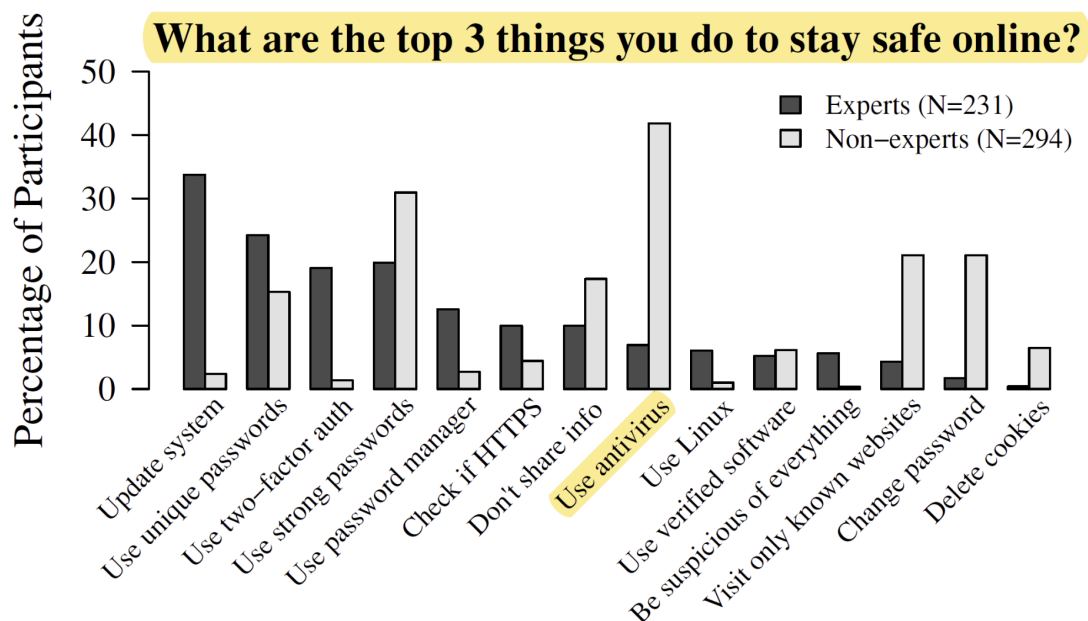
“Das Installieren von Antivirenprogrammen DIE Sicherheitsmaßnahme schlechthin.

- laut Laien

Unter Sicherheitsexperten wird diese Maßnahme aber nur von 7% der befragten überhaupt erwähnt.”

(*Virenschutz: Das Digitale Schlangenöl*, 2022)

Ultrativ redet von dieser Grafik, beziehungsweise der darunter liegenden Befragung.



(“...No One Can Hack My Mind”: Comparing Expert and Non-Expert Security Practices, 2015)

Doch - er lässt er dabei ein paar wichtige Details aus. An dieser Stelle sei schon mal ein wichtige Sache gesagt, die ich auch im Stream (*Uncut: Ultrativ Wissenschaftlich Geprüft*, 2022) hervorgehoben habe: Ich denke nicht, dass es Ultrativs Intention war, hier Umstände zu verschleiern oder falsche Ansichten zu verbreiten. Ich möchte nochmal hervorheben, dass er alle Quellen inklusive dieser verlinkt hat und auch diesem Video zugestimmt hat. In

diesem Kontext möchte ich Hanlons Rasiermesser aufbringen, wobei ich hier ein Wort in Kontext setzen möchte:

Schreibe nicht der Böswilligkeit zu, was durch Dummheit hinreichend erklärbar ist.

- Hanlons Rasiermesser

(*Hanlon's Razor* – *Wikipedia*, n.d.)

Ich sage nicht, dass Ultralativ “dumm” ist, sondern, dass er hier etwas übersehen hat - man sollte es also eher “Unwissenheit” nennen, und das ist, wie wir ja schon etabliert haben - nur menschlich.

Also - was lässt er denn nun aus?

Beginnen wir mit dem einfachsten: Der Überschrift.

Nur 7% der Experten erwähnen überhaupt Antivirenprogramme - Unter IHREN Top 3 Dingen, die SIE persönlich tun, um im Internet sicher zu sein. Diese Information beschreibt eine andere, als das, was von Ultralativ dargestellt wird - dass nur 7% diese Sicherheitsmaßnahme überhaupt erwähnen. Es könnte sein, dass die Sicherheitsexperten sie alle an vierter Stelle genannt haben, und diese information würde nicht in der Grafik auftauchen. Wir erfahren in der Studie von 4 “Bereichen” der Sicherheit:

4.1 Install Software Updates

4.2 Use Antivirus Software

4.3 Account Security

4.4 Mindfulness

(Ion et al., 2015)

und die Top 3 der Experten sind schlichtweg anders gewichtet, weil Experten sich mehr Gedanken um Software Updates (“Update System”) sowie Account Security (“Use unique passwords” und “Use two-factor authentication”) machen. Doch all dies sind wiederum Vermutungen meinerseits, die nicht minder fehleranfällig sind als Ultralativs ursprüngliche Aussage. Also schauen wir weiter in die Fakten:

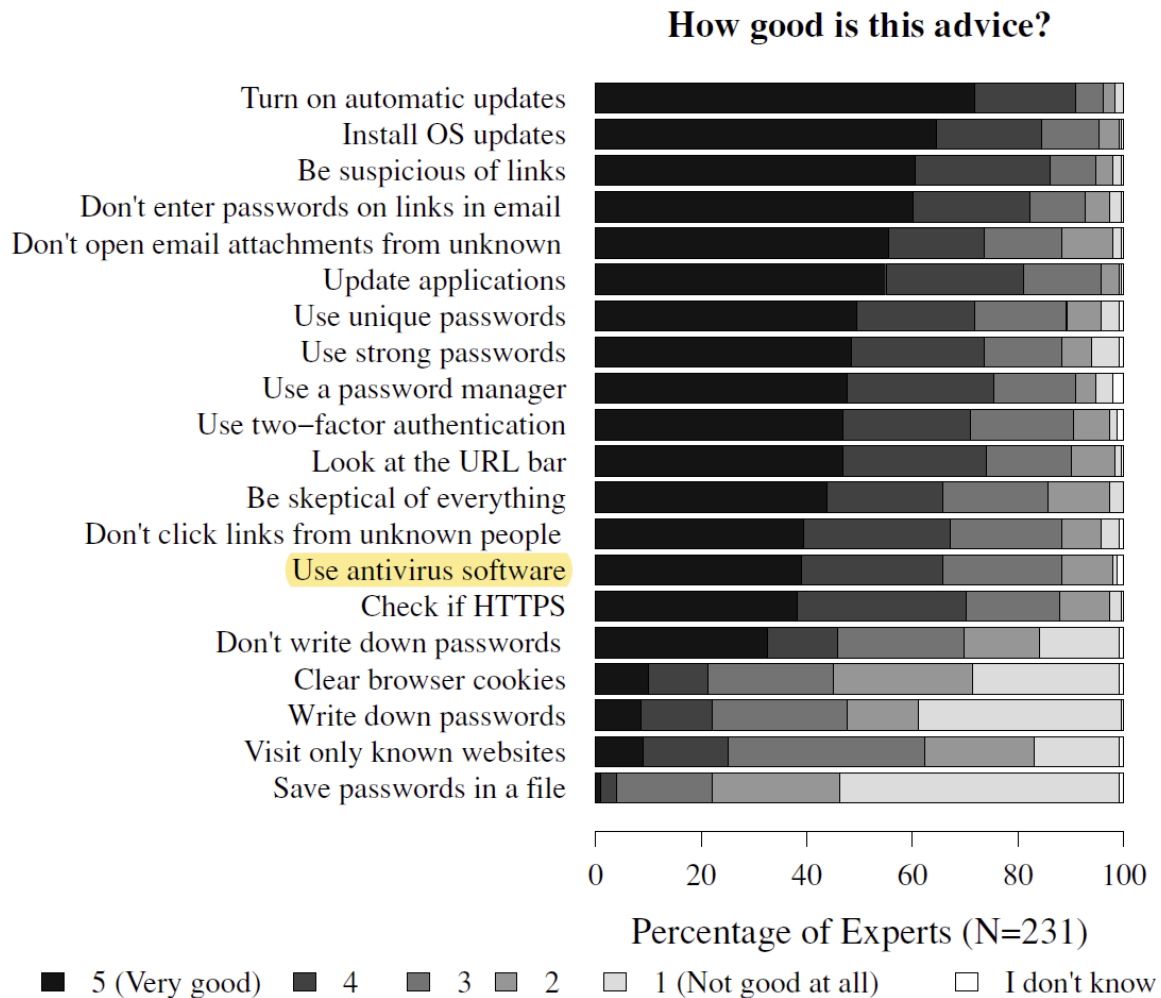


Figure 3: Advice considered “good” (i.e., both in terms of effective and realistic) by experts.

(“...No One Can Hack My Mind”: Comparing Expert and Non-Expert Security Practices, 2015)

Etwa 39% der Experten finden den Tipp “benutzt Antivirus software” sehr gut.

Etwa 65% der Experten finden diesen Tipp mindestens gut, etwa 85% zumindest nicht negativ.

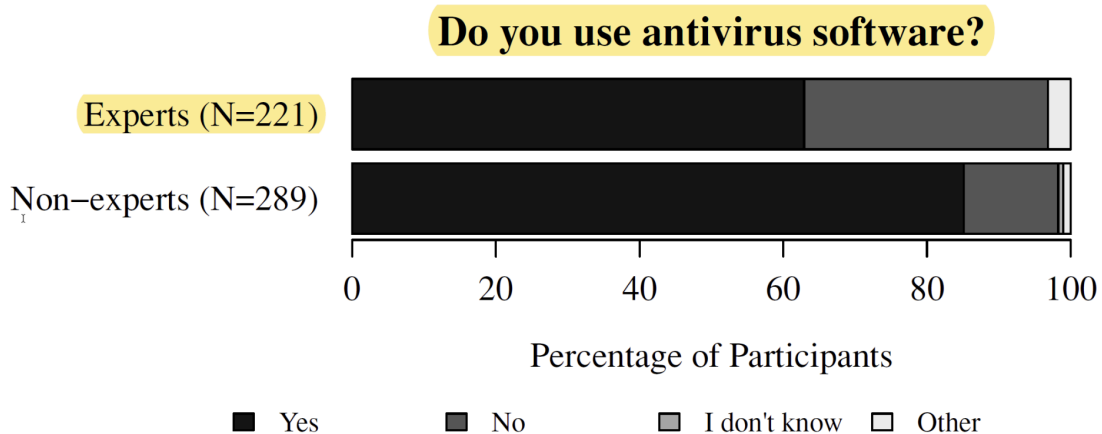


Figure 6: More non-experts reported to use antivirus software on their personal computer than experts.

(*"...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices*, 2015)

63% der Experten benutzen Antivirenprogramme.

Ebenso der Absatz:

"Während die Experten die Benutzerfreundlichkeit von Antiviren-Software anerkennen, warnen einige auch davor, dass Antivirus keine kugelsichere Sicherheitslösung ist. E47 war zum Beispiel der Meinung, dass "Antiviren-Software einfach zu benutzen ist, aber weniger effektiv als die Installation von Updates". Ähnlich meinte E116, dass ein Antivirus "gut darin ist, alltägliche/gewöhnliche Malware zu erkennen. Aber nichts, was etwas anspruchsvoller ist". E27 gab außerdem zu bedenken, dass ein Antivirenprogramm "auch aktuell gehalten werden muss, was oft nicht der Fall ist."

(*"...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices*, 2015)

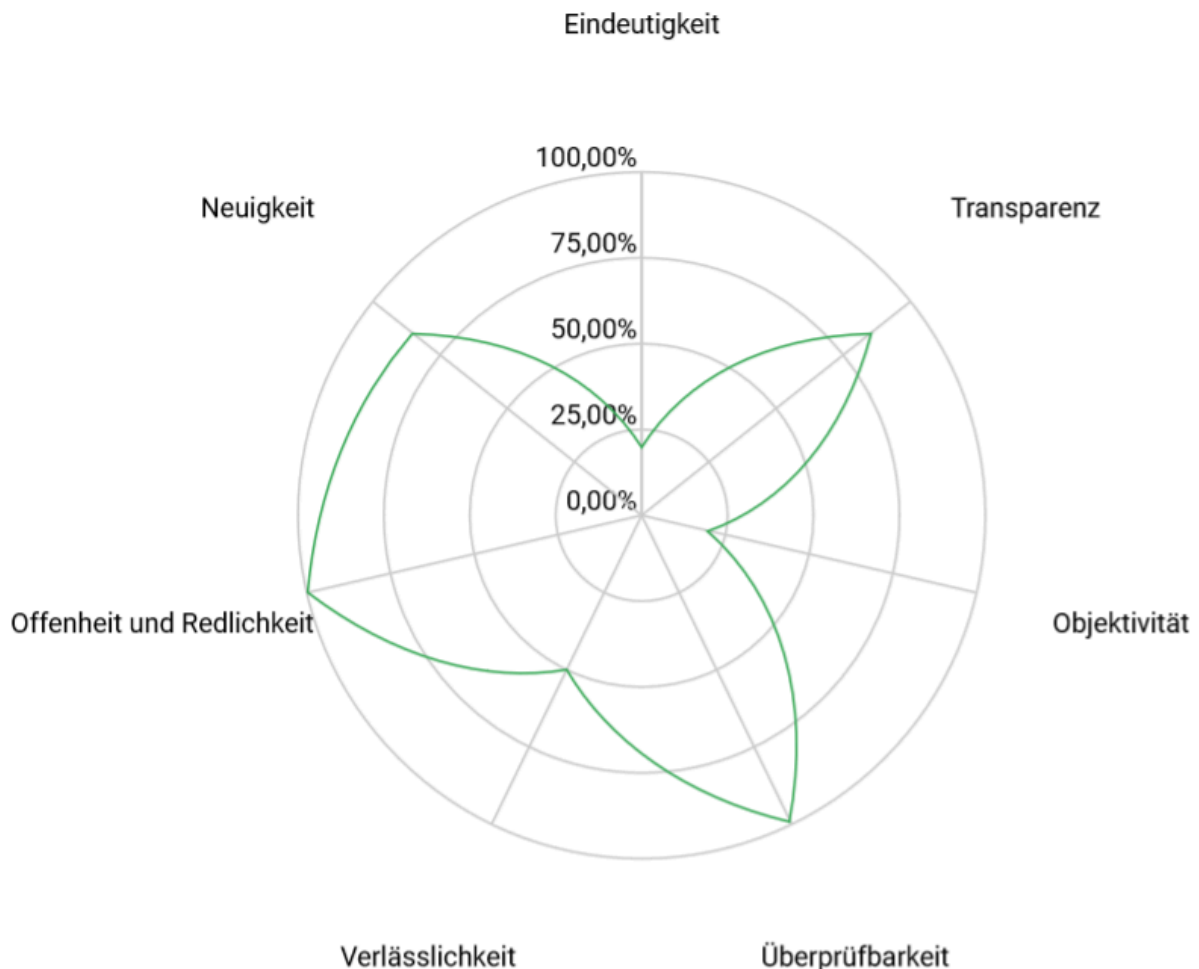
Übersetzt mit www.DeepL.com/Translator (kostenlose Version)

Im Stream gehe ich ausführlicher darauf ein, was diese Fakten implizieren, was die Folgen davon sind. Kurzum: Die gesamte Argumentationskette des Schlangenöl-Videos basiert darauf, dass Experten Antivirensoftware nicht empfehlen, dass sie eine größere Bedrohung für den Nutzer darstellen, als sie Nutzen bringen. Basierend auf diesem Paper, dass als Begründung für diese These angegeben wird, ist das exakte Gegenteil der Fall.

Damit wird nicht das ganze Video devalidiert. Ultrativ hat sehr gute Arbeit geleistet, hat Quellen angegeben, anhand derer man prüfen konnte. Er nennt auch weitere gute Punkte (benutzen sie Linux), die sich mit den Aussagen des Papers decken, und auch die Idee des Antivirenprogramms als Keil ist clever, ist sicherlich wichtig und möglicherweise richtig - wenn auch nicht ohne weiteres prüfbar, da hierfür die Quellen fehlen.

Verbleiben wir also bei folgendem Fazit:

Wenn die Aussage, auf der das Ultralativ-Video basiert, richtig wäre - dann wäre es ein vorzügliches Video, welches gut illustriert, gut fundiert und gut kommuniziert ist. Und auch in dem Umstand, dass dieser eine Fakt missinterpretiert wurde, ist zwar das Video und sein Fazit vorerst nicht gültig, nicht "Konsens", nicht supported durch die größere Evidenz, nicht "wahr", wie der Laie gern sagen würde - doch die Gelegenheit, diesen Fakt aufzudecken, die Gelegenheit, das Thema Internet Security zu thematisieren und mehr darüber zu lernen, wie man Fakten wissenschaftlich zusammenträgt.



Ultralativ hat es auf 65,57% BorgNetzWerk zertifizierte Punkte beim wissenschaftlichen Arbeiten gebracht. Man muss ihm definitiv Zugute halten, dass er in Punkten Offenheit und Redlichkeit sowie Überprüfbarkeit Spitzenarbeit geleistet hat. Wenn er an der Eindeutigkeit seiner Aussagen arbeitet sowie die Quellen entweder weiter streut oder zumindest ausführlicher liest - dann werden Videos wie diese obsolet und wir alle können uns mehr und mehr auf das verlassen, was Ultralativ schon seit Jahren so gut zusammenfasst.

In diesem Sinne vielen Dank nochmal an Ultralativ, dass er dieses Video möglich gemacht hat, ich hoffe, dass ich in diesem Video keine Gräben gezogen, sondern Brücken bauen konnte - und freue mich auf die Zukunft, die durch Videos wie diese ermöglicht wird.

In diesem Sinne:

Stay Safe

and Stay Critical

Noch kurz auf ein letztes Wort:

Am 15.03. hat das BSI eine Warnung herausgegeben, die ich euch anbei verlinkt habe. (*BSI Warnt Vor Dem Einsatz Von Kaspersky-Virenschutzprodukten, 2022*) Wenn wir auch mit diesem Video etabliert haben, dass Antivirenprogramme zumindest allgemein hilfreich sind, sollten die Bedenken des BSI unter aktuellen Umständen nicht vernachlässigt werden. Im Endeffekt sieht da die Rechnung etwa so aus:

$$\frac{\text{Gefahr durch Viren}}{\text{Virenschutz (ohne Kaspersky)}}$$

vs.

$$\frac{\text{Gefahr durch Viren}}{\text{Virenschutz (von Kaspersky)}} + \text{Gefahr, dass Kaspersky instrumentalisiert wird}$$

Wir wissen gerade nicht, wie groß diese Gefahr ist - und ich möchte mich da auch nicht zu äußern. Ich möchte nur hervorheben, dass das BSI diese Gefahr für groß genug befunden hat, die Warnung herauszugeben.

Ich kann euch also auch nicht mehr empfehlen als das, was das BMI schon im FAQ sagt: (*FAQ - Kaspersky, 2022*)

Schaut in die Fachpresse, was es an Alternativen gibt, und überlegt euch dann, ob ihr euer Kaspersky deinstallieren wollt. Und Falls ja - dann stellt sicher, dass VORHER ein anderer Virenschutz aktiviert ist - sei es Windows eigener Defender oder eine Alternative. Und dann möglichst reibungslos in den neuen Virenschutz.

Jetzt aber genug davon.

In diesen Zeiten nochmal doppelt und dreifach:

Stay safe
and stay critical.

References

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten. (2022, March 15). BSI.

Retrieved March 19, 2022, from

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html?nn=520690

DeepL Translate. (n.d.). DeepL Translate: The world's most accurate translator. Retrieved

March 19, 2022, from <https://www.deepl.com/translator>

FAQ - Kaspersky. (2022, March 15). BSI. Retrieved March 19, 2022, from

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/FAQ-Kaspersky/faq_node.html;jsessionid=7BD73DE5A7570B65E61C286F73832489.internet482

Hanlon's Razor – Wikipedia. (n.d.). Wikipedia. Retrieved March 19, 2022, from

https://de.wikipedia.org/wiki/Hanlon%E2%80%99s_Razor

Ion, I., Reeder, R., & Consolvo, S. (2015). “...*No one Can Hack My Mind*”: *Comparing Expert and Non-Expert Security Practices*. USENIX. Retrieved March 19, 2022, from

<https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>

“...*no one can hack my mind*”: *Comparing Expert and Non-Expert Security Practices*. (2015,

July 24). USENIX. Retrieved March 20, 2022, from

<https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf>

Virenschutz: Das digitale Schlangenöl. (2022, March 6). YouTube. Retrieved March 19,

2022, from <https://www.youtube.com/watch?v=ZxzvHXT0NXw>

Warnungen nach §7 BSIG. (n.d.). BSI. Retrieved March 19, 2022, from

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html

—BorgNetzwerk—

Uncut: Ultrativ wissenschaftlich geprüft. (2022, March 13). YouTube. Retrieved March 19, 2022, from <https://www.youtube.com/watch?v=t8Hr4gUfqLk>