Hinweise für den Gebrauch von Computern im Studium: E-Mail-Sicherheit

Prof. Dr. Robert Zydenbos
Institut für Indologie und Tibetologie, LMU
(Stand: 1. Februar 2020)

Die hier angebotenen Überlegungen und Anregungen sind dazu gemeint, den studentischen und dozentischen Alltag zu erleichtern und mögliche Schwierigkeiten, die bei der Verwendung von Computern im Studium entstehen können, zu vermeiden. Die hier geäußerten Meinungen sind die persönlichen Meinungen des Autors, aufgrund seiner eigenen Erfahrungen, aber andere Personen können sehr wohl begründete abweichende Meinungen und Präferenzen haben.

Textstellen in blauer Farbe sind so genannte **URLs,** d.h. durch Klicken darauf wird man zu anderen Stellen in diesem Text oder im Internet (natürlich nur bei bestehender Internetverbindung) mithilfe eines Webbrowsers zu Webseiten mit weiteren Informationen weitergeleitet.

Einleitende Bemerkungen

Im vorliegenden Text wird **E-Mail-Sicherheit** besprochen. Über weitere Information zum E-Mail-Verkehr lesen Sie bitte http://lmu.zydenbos.net/emailverkehr.pdf, und über Textverarbeitungsprogramme und digitale Textformate bitte http://lmu.zydenbos.net/textverarbeitung.pdf. Computerressourcen für Studierende an der LMU und Überlegungen bei der Wahl eines neuen Computers werden unter http://lmu.zydenbos.net/computerwahl.pdf besprochen.

Sicherheit im E-Mail-Verkehr

Im universitären Betrieb kann man auf E-Mail praktisch nicht mehr verzichten, u.a. für den Informationsfluss von Dozenten zu Studierenden. Deshalb ist es wichtig, dass alle Studierenden gut wissen, wie man mit E-Mail umgeht, und auch, was die alltäglichen, von den meisten Menschen übersehenen Risiken sind.

Themen:
(a) Die Wahl einer E-Mail-Adresse / eines E-Mail-Anbieters
(b) Die E-Mail-Dienste – ‚kostenlos' oder lieber doch nicht?

(a) Die Wahl einer E-Mail-Adresse / eines E-Mail-Anbieters

Es gibt ein riesiges Angebot an E-Mail-Postfächern von Seiten der verschiedenen E-Mail-Dienstanbieter (meistens anglifizierend-neudeutsch ‚Provider' genannt), in Deutschland sowie im Ausland. Die Wahl des Providers ist nicht unwichtig.

Wo der Dienstanbieter ist. Diese Frage ist nicht unwichtig, denn sie hängt mit Fragen des Datenschutzes und der Privatsphäre zusammen. Von Land zu Land gibt es unterschiedliche gesetzliche Regelungen in Bezug auf Sicherheit und den Schutz der Privatsphäre. In den USA, zum Beispiel, gibt es praktisch keinen solchen Schutz, wo es um E-Mail und andere Formen der elektronischen Kommunikation geht. – Seit den Enthüllungen von Edward Snowden wissen wir auch, dass die amerikanische Regierung freien Zugang zu den Servern von den großen Anbietern Yahoo, Microsoft, Google, Facebook und Apple hat. Der Geheimdienst NSA und die britischen Kollegen von GCHQ versuchen sogar alle elektronische Kommunikationen der gesamten Welt abzufangen und zu speichern.

Wenn Sie einen Provider wie Google Mail (Gmail), Yahoo, Outlook (das frühere Hotmail) oder iCloud wählen, dann heißt dies, dass Sie all Ihre Korrespondenz der amerikanischen Regierung zur Verfügung stellen. Nicht nur das, was Sie schreiben: auch alle von anderen an Sie verschickte Korrespondenz verschenken Sie der amerikanischen Regierung. Man kann, wie ein braves Schaf, dies zulassen, oder, wenn dieser Gedanken einen anekelt, kann man sich wehren und macht es den Spionen wenigstens ein bisschen schwieriger (wenn nicht unmöglich) und verwendet E-Mail mittels eines anderen Anbieters.

Lassen Sie sich übrigens nicht beirren durch den Landeszusatz „.de“ am Ende von Adressen von E-Mail und Internet-Webseiten: Dies muss nicht unbedingt heißen, dass Sie mit einem in Deutschland basierten Dienst (mit deutschem Datenschutz) zu tun haben. So unterliegen alle amerikanischen Firmen in Sachen Datenschutz dem amerikanischen Gesetz (was praktisch heißt: auch wenn Sie eine E-Mail-Adresse mit yahoo.de, hotmail.de, googlemail.de verwenden, ist in der elektronischen Korrespondenz Ihre Privatsphäre gesetzlich ungeschützt. Es ist, als ob Sie alles auf offenen Postkarten schreiben. Dies gilt natürlich auch für alles, was Sie von anderen in einem solchen Postfach empfangen. Deshalb verlangt die LMU, dass alle offizielle Korrespondenz zwischen Dozenten und Studenten über LMU-Adressen läuft – s. auch unten).

Die Wichtigkeit der Privatsphäre. Sie können meinen, dass Sie nichts zu verbergen haben. Vergessen Sie aber nicht: Irrtümlich, oder aus Leichtsinn, könnte man der Öffentlichkeit über sich selbst Informationen freigeben, die Jahre später von skrupellosen Personen und Instanzen gegen einen verwendet werden können. Das Internet *vergisst nichts*. Sie wissen heute nicht, wie irgendwann in der Zukunft irgendetwas in Cyberspace Findbares gegen Sie verwendet werden kann.

(b) Die E-Mail-Dienste – ‚kostenlos‘ oder lieber doch nicht?

Die LMU bietet Studierenden eine ‚Campus‘-Adresse an (im Format max.mustermann@campus.lmu.de): Dies ist aber ein sog. Alias, über die E-Mail an ein echtes Postfach (von den Studierenden selbst bei einem der vielen Anbieter zu wählen) weitergeleitet wird. Über diese virtuelle Adresse, die Sie während des gesamten Studiums behalten, kommuniziert die Universität mit Ihnen; Sie können aber, je nach Bedarf, im Hintergrund Ihre ‚echte‘ Adresse (also bei dem E-Mail-Anbieter, wohin die Post weitergeleitet wird) immer ändern. So bleiben Sie für die Universität erreichbar, auch wenn Sie Ihre echte Adresse ändern.

Die LMU verlangt von allen Dozenten und Studierenden, dass alle offizielle Korrespondenz über diese @campus.lmu.de-Adressen läuft. Dies hat zu tun mit der deutschen Daten-

schutzgesetzgebung. Falls Sie ein Postfach bei z.B. einem bedenklichen amerikanischen Email-Anbieter haben (s. oben), d.h. Sie lassen Ihre Korrespondenz an einen Dienst weiterleiten, der Ihre Privatsphäre nicht respektiert, **dann ist das Ihre Verantwortung(slosigkeit),** nicht die der LMU.

Jedenfalls brauchen Sie also ein echtes elektronisches Postfach bei einem Dienstanbieter (‚Provider'). Heutzutage hat fast jeder das. Über die Wahl eines E-Mail-Dienstanbieters soll zuerst etwas ganz Prinzipielles festgestellt werden: ‚Anscheinend Kostenloses' ist in der Regel **bloß das** – *anscheinend* kostenlos. Wenn irgendeine Firma etwas im Internet macht, dann sind damit Kosten verbunden, und die Firma muss irgendwie diese Kosten zurückgewinnen und auch noch Gewinn machen, um rendabel zu bleiben. Wenn Sie kein Geld für Ihren E-Mail-Verkehr ausgeben, dann zahlen Sie mit etwas Anderem, nämlich mit Daten über Sie selbst.

Wenn sie für einen E-Mail-Dienst bezahlen, liefert dieser in der Regel auch zusätzliche Vorteile, die Ihnen nützlich sein können, wie z.B. Online-Speicherplatz für Dateien, mehr Speicherplatz für E-Mail, das Fehlen von irritierender Werbung, oder erhöhten Schutz der Privatsphäre.

Im Folgenden stehen einige Überlegungen zur Wahl eines Anbieters. Man kann hiermit einverstanden sein oder nicht (und Sie als erwachsener Mensch haben natürlich das Recht, diese Überlegungen nicht zu beachten), aber wenigstens sollte man als Bürger im Informationszeitalter hierüber Kenntnis genommen haben.

Wer nicht einsieht, was und wie viel beim Datenschutz auf dem Spiel steht, sollte unbedingt lesen, was die britische Zeitung *The Guardian* hierüber sagt[1]. Über die Bedeutung für die Demokratie sollten Sie die **kurze Rede** hören, die der Journalist Glenn Greenwald, der die Enthüllungen Edward Snowdens ermöglichte, **in der Großen Aula unserer Universität** hielt, als er am 2.12.2014 den Geschwister-Scholl-Preis erhielt[2]. ***Sie sollten so viel wie möglich Herr / Herrin über Ihre eigenen persönlichen Daten sein, denn man weiß nie, wie Informationen über Sie gebraucht / missbraucht werden.***[3]

Einige Politiker und ‚Sicherheitsexperten' im In- und Ausland (und auch Führungskräfte bei Google und Facebook) argumentieren, dass dies alles uns doch egal sein sollte, wenn wir anständige Menschen sind und sowieso nichts zu verbergen haben. – Solche Leute sollten aber, wenn sie ihre eigenen Argumente wirklich ernst nehmen, sofort auf das Briefgeheimnis verzichten und ab sofort *alles* nur noch auf offenen Briefkarten schreiben (aber das machen sie nicht). Auch sollten sie im Sommer nackt herumlaufen – denn das geht doch, wenn man sowieso nichts zu verbergen hat?)[4].

Die so genannten kostenlosen Dienste. Die meisten Studierenden benutzen Gratis-Dienste, hauptsächlich aus finanziellen Überlegungen (diese ‚kostenlosen' Dienste haben oft aber sehr ernst zu nehmende Nachteile – s. unten).

Bitte achten Sie auf den von Ihrem Dienstanbieter angebotenen Speicherplatz! (Siehe

[1] http://www.theguardian.com/us-news/the-nsa-files Man lese über die Wichtigkeit der Online-Privatsphäre auch https://www.whonix.org/wiki/The_World_Wide_Web_And_Your_Privacy, https://www.eff.org/, https://duckduckgo.com/?q=online+privacy+importance und https://blog.protonmail.ch/privacy-under-attack/

[2] https://www.youtube.com/watch?v=nNGGYYF1jdY

[3] Siehe auch "You Think You Have Nothing to Hide? Think Again" – https://tutanota.com/blog/posts/nothing-to-hide

[4] Besonders empfehlenswert zu sehen, wenn Sie zwei Minuten Zeit haben, ist das humoristische „Eine wichtige Information der Vereinigten Geheimdienste" (https://www.youtube.com/watch?v=nNs99sdE7Hg oder http://www.better-no-letter.org/overlay.html) von der österreichischen Post – klicken Sie hier aber auch bitte weiter zu den anderen, informativen, weniger humoristischen Seiten.

auch die wichtige unten stehende Warnung über eventuellen Speicherplatzmangel.) Bei durchschnittlichem Gebrauch sollte 1 Gigabyte an Speicherplatz für E-Mail für längere Zeit ausreichen.

Einige Beispiele von kostenlosen Angeboten[5] sind:

(a) Die großen amerikanischen Dienste (Googlemail / Gmail, Outlook / Hotmail, Apple iCloud, Yahoo): s. unten, warum man sich von diesen fern halten sollte.

(b) Web.de (https://web.de): ***nur 12 Megabyte*** (*dies führt oft zu Problemen,* weil ein so kleines Postfach schnell voll wird! Dann kommt Post für Sie einfach nicht mehr an), es sei denn, man lässt sich auf besondere Bedingungen von Web.de ein. – In der Praxis benutzt unter den Studierenden kaum jemand diese Möglichkeit, weil sie zu umständlich ist, und deshalb kann ich das kostenlose Angebot von Web.de für die ernsthafte Verwendung als Kommunikationsmittel im Studium leider ***nicht empfehlen.*** Es ist wiederholt passiert, dass ich eine Studentin / einen Studenten mit einer Web.de-Adresse nicht erreichen konnte und ein Rundschreiben von mir als unbestellbar zurückkam.
Bereiten Sie sich auch auf große Ladungen unerwünschter Werbung vor, die Web.de Ihnen schicken wird. Passen Sie auch davor auf, auf vermeintliche Geschenkaktionen (lies: Abo-Fallen) wie die dreimonatige ‚Club'-Mitgliedschaft zu klicken[6].

(c) GMX (https://www.gmx.net): **1 Gigabyte.** Bereiten Sie sich auf große Ladungen unerwünschter Werbung vor, die GMX Ihnen schicken wird.

(d) T-Online (https://freemail.t-online.de) bietet **1 Gigabyte** und ist einer der älteren Anbieter in Deutschland. Lange Zeit war er ziemlich langsam und anfällig für große Mengen an unerwünschter Werbung (sog. ‚Spam', wogegen T-Online keine gute Abwehr hatte), weswegen er nicht zu den besseren Anbietern gehörte. In letzter Zeit hat der Dienst sich anscheinend verbessert. Es gibt aber eine merkwürdige **Schwachstelle:** Falls man den Webmailer verwendet, sollte man aber darauf **achten,** beim Ausloggen auch **den Webbrowser zu schließen:** Ihre Anmeldungsdaten bleiben hartnäckig im Browser hängen (!) und können ggf. Ihr Postfach für andere zugänglich machen.

(e) Das niederländische **Disroot** (https://disroot.org/en/services/email) stammt typischerweise aus der Amsterdamer alternativen Szene, ist vehement freiheitsliebend, bietet kostenlos schon sehr viel an **(2 Gigabyte Speicherplatz für E-Mail, 4 Gigabyte für Dateien in einer virtuellen Festplatte)**, falls aber das Angebotene nicht ausreicht, kann man zusätzlichen Speicherplatz, Aliasse u.a. dazukaufen. Wie bei Mailbox.org und Mailo (s. unten) ist die Möglichkeit der Verschlüsselung von E-Mail mithilfe von PGP eingebaut.

(f) Laposte.net (https://www.laposte.net/accueil) ist ein Angebot der französischen Post: **5 Gigabyte** (inklusive Kalender; separat wird ‚Digiposte', ein kostenloser Online-Speicher mit ebenfalls 5 Gigabyte angeboten).

(g) Outlook / Hotmail (https://login.live.com), Google (https://www.gmail.com): **15 Gigabyte** Speicherplatz für E-Mail

[5] Diese kurze Liste ist sehr unvollständig und gibt nur die Namen einiger der bekannteren Anbieter. Der Autor dieser Zeilen will nicht unbedingt diesen oder jenen Anbieter befürworten, gibt dem Leser aber zu überlegen, dass im Lichte der neueren Enthüllungen über die aktivitäten amerikanischer Geheimdienste (und auch der Geheimdienste einiger verbündeter Länder, allen voran Großbritannien) der Schutz der Privatsphäre bei den großen Gratis-Diensten von Microsoft (Outlook / Hotmail), Google (Googlemail / Gmail), Yahoo und Apple (iCloud) eine *äußerst bedenkliche Sache* ist.

[6] https://de.wikipedia.org/wiki/Web.de#Kritik (Stand: 23.01.2018).

(h) Yahoo (https://de.mail.yahoo.com): **1 Terabyte** Speicherplatz für E-Mail

(i) Yandex (https://mail.yandex.com), Mail.ru (https://e.mail.ru/login?lang=en_US): **unbegrenzt viel Speicherplatz für E-Mail.**

Man achte darauf, dass im Leben nur die Sonne gratis aufgeht – und dass alles Andere etwas kostet. Es gibt bei den Gratis-Diensten meistens irgendeinen Haken:

- Die deutschen Provider Web.de, GMX u.a. nerven mit Werbung für Sachen, wofür ein vernünftiger Mensch sich nicht interessieren sollte, sowohl in sog. ‚Newsletters' wie im Browserfenster (u.a. dating services, Seitensprungforen u.dgl.). Vor allem Web.de kann mit Werbung für sich selbst oder für Dritte sehr aufdringlich sein. Der zurückhaltendste und eleganteste dieser kostenlosen deutschen Dienste ist wohl Mail.de, der laut einer im Juli 2014 veröffentlichten Untersuchung auch der sicherste der fünf größten deutschen Gratis-Anbieter ist[7].

- **Noch um einiges schlimmer** ist es bewiesenermaßen bei den großen amerikanischen Providern: Diese sammeln Daten über Sie und verkaufen die gesammelten Daten. In gewissem Sinne machen diese Dienste Sie also zu deren Kaufware. Google ist schon lange als der große ‚Datenkrake' bekannt, der alles Mögliche über Sie herausfindet und diese Informationen käuflich verwertet[8]. Microsoft (die Firma hinter Outlook / Hotmail) hat bekannt gemacht, ebenfalls Benutzerdaten kommerziell benutzen zu werden[9]. Sowieso behalten Microsoft, Google, Yahoo and Apple sich das Recht vor, die Post ihrer Benützer zu lesen[10].

  Auch in anderen Hinsichten **nehmen diese Gratis-Anbieter den Datenschutz und die persönliche Sicherheit ihrer Benutzer nicht ernst.** Der übelste dieser Anbieter scheint Yahoo zu sein: Berichten zufolge hat dieser Dienstleister aus kommerziellen Überlegungen private Korrespondenz von chinesischen Nutzern an die Volksrepublik China freigegeben, die zu Verhaftung und Folter geführt haben[11]. Yahoo sieht oder sah in der Zusammenarbeit mit der Justiz offenbar eine so interessante Einkommensquelle, dass es eine Preisliste für Informationen über Yahoo-Benutzer gibt oder jedenfalls gab[12]. Auch scheint Yahoo anfällig für Hacker-Angriffe zu sein[13] und bekommt man dort große

[7] https://mail.de/blog/2014-09-mailde-ist-testsieger-im-vergleich-deutscher-e-mail-dienste/

[8] Zu den Praktiken von Google s. http://de.wikipedia.org/wiki/Kritik_an_Google_Inc. (Stand: 10.12.2015). Auch "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google": http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/ (vom 4.2.2010).

[9] http://www.zeit.de/digital/datenschutz/2012-10/microsoft-nutzungsbedingungen-profile/komplettansicht

[10] http://www.theguardian.com/technology/2014/mar/21/yahoo-google-and-apple-claim-right-to-read-user-emails

[11] Aus solchen Überlegungen forderte 2006 die britische Journalistengewerkschaft NUJ ihre 40.000 Mitglieder zu einem Boykott von Yahoo auf (man lese auch den Bericht von der BBC, "Yahoo 'helped jail China writer'", http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm). Laut Berichten hat Yahoo auch freizügig Informationen über deutsche Benutzer dem amerikanischen Geheimdienst NSA übergeben. Auch die technische Sicherheit scheint zweifelhaft zu sein: es passiert immer wieder, dass es Hackern gelingt, bei Yahoo einzubrechen und persönliche Daten zu rauben (s. http://de.wikipedia.org/wiki/Yahoo#Kritik (Stand: 29.3.2016)).

[12] https://www.eff.org/takedowns/yahoo-tries-hide-snoop-service-price-list (Stand: 3.2.2016.) Als Cryptome (https://cryptome.org/) auf dem Internet diesbezügliche Dokumente veröffentlichte, drohte Yahoo vergeblich mit juristischen Schritten, um die Sacche unter den Teppice zu kehren.

[13] Erst im September 2016 gestand die Firma, dass schon 2014 von Hackern die Daten von 500 Millionen Benutzern gestohlen wurden: http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html und http://www.bbc.com/news/world-us-canada-37447016 (Stand: 19.10.2016). Dabei blieb es aber nicht: im

Mengen an unerwünschter Werbung. Und wenn man auch noch weiß, dass Yahoo zum effizienteren Ausspionieren durch amerikanische Geheimdienste ein spezielles Programm zu deren Günsten auf seinen Servern eingebaut hat[14], dann fragt man sich, wie ein sich selbst respektierender Mensch überhaupt noch eine Yahoo-Adresse benutzen kann.
Außerdem: Alles, was bei diesen amerikanischen Anbietern verschickt und empfangen wird, landet auch bei den amerikanischen Geheimdiensten, die auch gerne die so gewonnenen Informationen mit ihren Kollegen anderswo in der Welt austauschen. (Oder finden Sie es gar nicht so schlimm, ständig überwacht zu werden, und helfen Sie der Entwicklung eines elektronischen Polizeistaates nach chinesischem Modell gerne weiter voran?) – Durch die Enthüllungen von Edward Snowden ist bekannt geworden, dass die Geheimdienste freien Zugang zu den Servern von Google (Gmail), Microsoft (d.h. Hotmail / Outlook), Yahoo, Apple (iCloud), Facebook u.a. haben[15].

- Nicht nur Yahoo, auch Google Mail (Gmail) ist offenbar anfällig für Hacker-Angriffe. 2016 hat Wikileaks gestohlene Nachrichten vom ehemaligen Stabchef des Weißen Hauses und Leiter des Wahlkampfes für Hillary Clinton, John Podesta, veröffentlicht[16], und auch erschienen gestohlene Nachrichten vom ehemaligen amerikanischen Verteidigungsminister Colin Powell[17]. Beide benutzten Gmail.

- Solche ‚Haken' sind vom russisch-niederländischen Privatunternehmen Yandex[18], dass auch ein Büro in der Mitte Berlins unterhält, nicht bekannt. Yandex hat von allen großen Gratis-Anbietern das mit Abstand klugste und schönste Web-Interface (grafische Benutzeroberfläche)[19], mit mehreren sehr intelligenten, nützlichen Funktionen. So kann man z.B. anstatt eine E-Mail sofort zu verschicken, den Server damit beauftragen, dass die E-Mail zu einer späteren Zeit verschickt wird; oder man kann um eine Erinnerung bitten, falls die eigene E-Mail nicht innerhalb von einigen Tagen beantwortet worden ist. Man bekommt unbegrenzt viel Speicherplatz für E-Mail und bei der Anmeldung auch sofort 7 Gigabyte an Online-Speicherplatz für Dateien (so genanntes ‚cloud storage'). Am Rande erwähnt: Die Suchmaschine http://www.yandex.com ist vergleichbar gut wie Google, älter, und vielleicht sogar besser.
Hier kann man sich fragen: Wenn man unbedingt ein kostenloses E-Mail-Postfach mit unendlich viel Speicherplatz will, darf es dann irgendwie mit Russland verbunden sein? Denken wir kurz hierüber nach. Interessiert sich jemand in Russland für Ihre persönlichen Daten? (Amerikanische Spitzenpolitiker sind für russische Hacker doch viel interessanter.) Man würde dort wohl weniger mit Ihren persönlichen Daten anfangen können als amerikanische, britische und andere westliche Instanzen, die die eigenen Bürger

---

Dezember 2016 gestand die Firma, dass im Jahre 2013 Einbrecher Zugangsdaten zu einer Milliarde Benutzerkonten gestohlen hatten: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0 (Stand: 10.05.2017).

14 http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT

15 Zu den Praktiken von Google s. http://de.wikipedia.org/wiki/Kritik_an_Google_Inc. (Stand: 10.12.2015). Auch "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google": http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/ (vom 4.2.2010).

16 https://www.wikileaks.org/podesta-emails/

17 https://theintercept.com/2016/09/13/colin-powell-emails/

18 https://mail.yandex.com; siehe auch https://de.wikipedia.org/wiki/Yandex

19 "Yandex.Mail Review: The Good and Bad": https://www.lifewire.com/yandex-mail-review-1170798

bespitzeln und mit denen wir viel mehr zu tun haben[20]. Die Russen werden bestimmt kein Abkommen zum Datenaustausch mit den verschiedenen Überwachungsinstanzen im Westen haben! Also ist Ihre Privatsphäre hier besser geschützt.

- Lassen Sie sich auch nicht von den größten deutschen E-Mail-Anbietern mit ihrer „E-Mail made in Germany"-Werbung betören: Dies ist bloß ein Werbetrick[21] ohne viel technische Bedeutung. Man verspricht hier eine erhöhte Sicherheit, als seien die hier vorgenommenen Maßnahmen etwas Besonderes[22].

Man kann sich aber auch ernsthaft überlegen, ein sehr kleines bisschen Geld für einen ethisch unbedenklichen E-Mail-Dienst auszugeben, der es mit der Privatsphäre der Benutzer ernst meint.

Fast gratis, und besonders gut: nur 1€ im Monat, d.h. *weniger als 4 Cent pro Tag.* Für ein modernes und so wichtiges Kommunikationsmittel kann auch ein Student sich das leisten:

- **Posteo,** ein kleiner Anbieter, der in der Presse mehrfach als Vorreiter beim Schützen der Privatsphäre seiner Kunden gelobt worden ist[23], und dessen Hauptmitarbeiter in Greenpeace tätig waren, ein sehr schlichtes, menschliches Mittel zum Datenschutz: Man kann keine persönlichen Informationen der Benutzer weitergeben, wenn diese gar nicht gesammelt worden sind! Es werden bei der Anmeldung keine persönlichen Daten gefordert. Anonymes Bezahlen ist möglich, unter Erwähnung einer Nummer, die mit dem elektronischen Postfach verbunden ist. Auch die Daten von Bank- oder PayPal-Überweisungen werden von Posteo nicht aufbewahrt. Man bekommt 2 Gigabyte Speicherplatz für E-Mail.
- **Mailbox.org** (ein Ableger von JPBerlin, Junge Presse Berlin, also ein Provider mit journalistischem Hintergrund) betont die avancierten technischen Mittel, die für Schutz der Privatsphäre eingesetzt werden. Mit Mailbox ist es äußerst leicht (noch leichter als bei Posteo), verschlüsselte E-Mail zu verschicken mithilfe des internationalen Verschlüsselstandards PGP (das hier eingebaut ist). Man kann sogar verschlüsselte E-Mail an Empfänger schicken, die selber kein PGP verwenden, wenn man im Voraus ein Passwort vereinbart hat. Man bekokmmt 2 Gigabyte Speicherplatz für E-Mail.
- **Mailo** (https://www.mailo.com; früher hieß es **Net-C**, https://www.netc.com) in Frankreich hat ein umfangreiches Angebot. Dauerhaft **gratis** kriegt man 1 Gigabyte Speicherplatz für E-Mail, 10 frei wählbare Aliasse, eine virtuelle Festplatte von 500 Megabyte, und noch mehr Schönes (siehe https://www.net-c.com/netc/de/funktionalitaten.php). Die Verwendung von PGP ist hier vergleichbar leicht wie bei Mailbox.org. Dieser Gratis-

[20] Sie dürfen diesen Vorschlag ironisch oder nicht auffassen, ganz wie Sie wollen.

[21] http://de.wikipedia.org/wiki/E-Mail_made_in_Germany#Kritik

[22] Siehe «Bullshit made in Germany: Chaos Computer Club warnt vor Mogelpackung „E-Mail made in Germany"» http://ccc.de/de/updates/2013/bullshit-made-in-germany und «„E-Mail Made in Germany": Das Sommermärchen von der sicheren E-Mail» http://ccc.de/de/updates/2013/sommermaerchen. Zwei der Initiativnehmer scheinen sich seit August 2015 sowieso von diesem billigen Werbungsprojekt verabschiedet zu haben: https://mail.de/blog/2015-08-mailde-verschluesselung-dane-und-dnssec-setzt-sich-durch!-e-mail-made-in-germany-vor-dem-aus/

[23] Posteo scheut sich auch nicht, intimidierende Polizisten zu verklagen: Man lese „Postbotin gegen Schnüffler", *Cicero* (August 2014), S. 32-33. Siehe auch den Artikel in der britischen Zeitung *The Guardian,* "Protect your email the German way", http://www.theguardian.com/technology/2014/aug/24/posteo-protect-email-the-german-way-patrik-lohr

Dienst ist eigentlich gedacht als Werbung für den eigenen bezahlten (‚Premium-') Dienst. Wenn man monatlich ein Euro zahlt, kriegt man **20 Gigabyte Speicherplatz für E-Mail,** eine virtuelle Festplatte von 5 GB, bis zu 100 Aliasse und mehrere andere Vorteile.

Bei sowohl Posteo als Mailbox.org kann man für einige Zeit kostenlos den Dienst probieren, bevor man bezahlt, und bei Mailo / Net-C und Disroot kann man mit nur geringer Einschränkung den Gratis-Dienst benutzen[24]. Den monatlichen Beitrag von einem Euro für Posteo oder Mailbox.org kann der Benutzer sogar anonym bezahlen, wenn man es so will: mit Bargeld in einem Briefumschlag.

***WICHTIG – WICHTIG – WICHTIG:* Bitte sorgen Sie dafür, dass immer einiges an Platz in Ihrem E-Mail-Speicher frei bleibt.** *Löschen Sie regelmäßig alles, was Sie nicht brauchen.* Es ist besonders ärgerlich, und für Sie einfach sehr nachteilig, wenn Sie wegen eines vollen Postfaches keine Post von der LMU (auch von mir und anderen Dozenten) mehr empfangen können. **In der Regel, bei durchschnittlicher Verwendung, sollte ein E-Mail-Benutzerkonto mit 1 bis 2 GB an Speicherplatz für längere Zeit ausreichen.**

zurück zum Homepage

[24] Weniger kostengünstige aber sehr gute Dienste sind z.B. Runbox (https://runbox.com) in Norwegen und StartMail (https://www.startmail.com) in den Niederlanden, die sehr auf Privacy setzen. Ebenfalls sehr interessant ist ein in der Schweiz beheimatetes Projekt, das StartMail in einigen Hinsichten ähnlich ist: ProtonMail (https://protonmail.ch), von einigen Wissenschaftlern vom CERN und MIT. Neuen Benutzern bietet man 500 MB Speicherplatz gratis an. Ähnlich ist auch das deutsche Tutanota (mit 1 GB gratis, https://tutanota.com/). Protonmail und Tutanota sind in beschränktem Umfang gratis benutzbar; sie bieten auch Premium-Dienste an.
Interessant bei Mailbox.org, ProtonMail, Tutanota und SmartMail ist auch die eingebaute Möglichkeit, mittels PGP (Pretty Good Privacy), dem Standard für Email-Verschlüsselung, zu schreiben an Personen, die auf ihrem Computer PGP nicht installiert haben (hierzu muss man mit der anderen Person ein Passwort vereinbart haben).