Spickzettel: Wie kann ich meine Privatsphäre im Netz schützen?

Ein paar grobe und unvollständige Anregungen für den Anfang.
Auch, wenn nur einige der Hinweise beachtet werden – es hilft!

Computer-Betriebssystem – Falls möglich ein freies Linux-Betriebssystem benutzen (am einfachsten ist Ubuntu). So etwas ist immer sicherer als jedes Windows- oder Apple-OS-Betriebssystem (stellt für sich alleine aber noch keinerlei Gewähr dar!) Bei der Installation möglichst die „Alternate"-Version verwenden, mit der die Verschlüsselung der Computer-Festplatte auf einfache Art und Weise in einem Rutsch erledigt wird. - http://ubuntuusers.de/

Internet-Browser – Den OpenSource-Browser Mozilla Firefox verwenden statt Internet-Explorer oder GoogleChrome! - https://www.mozilla.org/de/firefox/new/

Browser-Einstellungen – Unter Extras/Einstellungen/Datenschutz entweder auf permanent privaten Modus umschalten oder aber so, dass keine Chroniken gespeichert werden und Cookies nach jedem Schließen des Firefox gelöscht werden (und dementsprechend ab und zu mal den Firefox schließen und wieder neustarten).

Firefox-Browser-AddOns – Empfehlenswert sind folgende zusätzlichen AddOns: AdBlock-Plus, BetterPrivacy, Flashblock, Ghostery, HTTPS-everywhere, NoScript, Stealther, Cookie Monster

E-Mail – keine E-Mails von „Kostenlos-Anbietern" verwenden. Umsonst ist das nicht, ihr bezahlt mit euren Daten und Informationen über euer Wesen, euer Verhalten, eure Persönlichkeit. Nicht nur Googlemail erlaubt sich das Durchsuchen eurer Mails nach interessanten Stichworten und Inhalten! Vertrauenswürdige E-Mail-Anbieter, die sich über eine Spende in der Größe eurer Wahl (am besten: weniger, aber dafür als Dauerauftragspende!) können sein: https://so36.net/ - https://riseup.net/ - http://nadir.org/

E-Mail-Verwaltung – Nicht nur einfacher, sondern auch sicherer und übersichtlicher ist die Nutzung des OpenSource Programms Thunderbird (ein so genannter „E-Mail-Client"), mit dem ihr auch mehrere E-Mail-Adressen verwalten könnt. - https://www.mozilla.org/de/thunderbird/

E-Mails verschlüsseln – Mit Thunderbird lässt sich auch die E-Mail-Verschlüsselung einfach und anwenderfreundlich durchführen. Mit dem AddOn namens „Enigmail" könnt ihr somit dafür sorgen, dass niemand anderes außer der Empfänger in der Lage ist, den Einhalt eurer E-Mails zu lesen. Oft wird diese Verschlüsselung auch als „PGP" oder „GnuPG" bezeichnet. Wichtiger Hinweis: Nicht verschlüsselt wird die Betreffzeile!

Anonym surfen – Dafür gibt es mehrere Möglichkeiten. Kostenlos und nicht nur deswegen empfehlenswert ist das so genannte „Tor-Netzwerk". Dort gibt es ein Komplett-Paket, in dem ein bereits vorinstallierter Firefox-Browser die Nutzung dieses Services sehr einfach macht. Wichtige Hinweise: Die Verwendung von Tor macht das Internet etwas langsamer und durch die Übertragung von Computer- und Browser-Einstellungs-Daten ist eine 100%ige Anonymisierung nicht oder nur schwer möglich. Aber die Verwendung von Tor ist ein sehr großer Schritt in diese Richtung. - https://www.torproject.org/projects/torbrowser.html.en

Daten verschlüsseln – Dateien und ganze oder Teile von Computern bzw. ihrer Festplatten können hochgradig sicher verschlüsselt werden. Ein gutes Programm dafür ist Truecrypt. - http://www.truecrypt.org/downloads

Sichere Passwords – Möglichst niemals gleiche Passwörter für mehrere Zwecke einsetzen. Das Bekanntwerden an einer Stelle kann sonst zu größten Problemen führen. Ausreichend lange Passwörter mit Zeichen, Zahlen und möglichst ohne Wörter, die in Lexikas zu finden sind. Eselsbrücken bauen. Beispiel „Das ist mein Passwort für das blöde Google-Netzwerk." wird zu „D1mPw>d:(G00gle-Nw."

Sicherungskopien anlegen – Die für einen persönlich wichtigsten Daten möglichst regelmäßig sichern (auf externen Laufwerken oder – platzsparender – auf Speicherkarten) und an anderen Stellen sicher verwahren.

Kostenlose und offene Software benutzen – Firefox und Thunderbird (s.o.), LibreOffice (früher: OpenOffice) statt Word, Exel und PowerPoint. Gimp und Inkscape zur Grafikverarbeitung. http://de.libreoffice.org/ - http://www.gimp.org/ - http://www.inkscape.org/

Datenschutzfreundliche Suchmaschinen benutzen – Anstelle von Google z.B. Ixquick. Auch die deutsche Wikipedia eignet sich hervorragend zur Suche. https://www.ixquick.com/deu/ - https://de.wikipedia.org/

Metadaten in Dokumenten beachten – Fotos, Videos, Textdokumente, PDF-Dokumente, E-Mails – alle enthalten so genannte „Meta-Daten" oder andere nicht sichtbare Informationen, die darüber Auskunft geben können, wann, von wem, an welchem Ort, mit welchem Gerät Fotos aufgenommen, Texte usw. geschrieben worden sind. Gleiches gilt für Ausdrucke von Druckern und Kopierern.

Verzicht oder Beschränkung bei (a)sozialen Netzwerken – Facebook, Google & Co. leben von der Sammlung und Verwertung eurer persönlichen Daten und machen damit Geld und Profit. Verzichtet darauf oder macht euch intensiv bewusst, ob und wie ihr damit umgehen möchtet. Zum Anhören: http://devianzen.de/20110401-bba-laudatio-rena-tangens-facebook.mp3 - http://devianzen.de/20120204-DigitalerTsunami-RenaTangens.mp3

Umgang mit Mobiltelefonen – Smartphones sind derzeit (noch?) völlig unkontrollierbar – die Wahrung der Privatsphäre und die Benutzung von Smartphones stehen einander im Widerspruch. Ältere Handys sind dagegen tendentiell „sicherer". Stille SMS zur Lokalisierung von Mobilfunkgeräten und Überwachung durch IMSI-Catcher sind nur mittels komplexer Hardware erkennbar. Handys können auch nach dem Ausschalten weiter aktiv sein und eventuell als Mikrofon-Wanze fungieren. Da hilft nur: Akku raus!

Ein paar weitere Informationen: https://wiki.vorratsdatenspeicherung.de/Sichere_Kommunikation - https://www.taz.de/!86966/ - https://www.vorratsdatenspeicherung.de/content/view/494/79/lang,de/

Herausgeber dieses Blattes:
Arbeitskreis Vorratsdatenspeicherung, Ortsgruppe Hannover
https://wiki.vorratsdatenspeicherung.de/Hannover
Stand: 03/2012

AK VORRAT hannover