1.Check if you have an account that has been compromised in a data breach

https://haveibeenpwned.com/

2.Vergleich verschiedenen VPN

https://vpn-anbieter-vergleich-test.de/vyprvpn/

3.Sicherheit von VPN-Tools unter Kritik – was stimmt daran?

https://www.digitalwelt.org/ratgeber/anonym-surfen/vpn-sicherheit

4: MELANI (Melde- und Analysestelle Informationssicherung)

https://www.melani.admin.ch/melani/de/home.html

5. Das Märchen vom anonymen Surfen

https://www.kuketz-blog.de/kommentar-der-mythos-vom-anonymen-vpn-zugang/

6. Hands off my data! 15 default privacy settings you should change right now

https://mail.google.com/mail/u/0/?hl=de#inbox/WhctKJTrVKznKNsxWbGxMmvLZbBrVJcrMBcfXNVGHDJRNlWxFsfkXGLQqmzRqccpJqsWCFb

7. Password Check wie sicher ist mein Password (nie mit echtem Password testen)

https://checkdeinpasswort.de/

8. Wie erstelle ich ein sicheres Password

https://www.datenschutz.org/sicheres-passwort/

9. Checklisten und Tipps vom Deutschen Bundesamt für Sicherheit in der Informatik

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html

10. PC Sicherheit Goldene Regeln (PC magazin)

https://www.pc-magazin.de/ratgeber/pc-sicherheit-goldene-regeln-tipps-3196621.html

11: Name und Email Check Tool

https://www.checktool.ch/

12.Datenschutz im Internet: Tipps

https://www.computerbetrug.de/anonym-surfen/datenschutz-im-internet

Schutz vor Phishing

Phishing beruht in erster Linie auf Täuschung. Daher ist der beste Schutz vor dieser Art der Internetkriminalität gesundes Misstrauen.

Folgende Tipps sollten Sie beherzigen, um nicht zum Phishing-Opfer zu werden:

Misstrauen und Rückfrage: Kein seriöses Unternehmen – weder Sparkasse, noch Volksbank, Raiffeisenbank, oder Ebay – wird Sie per Mail auffordern, zu einer bestimmten Internetseite zu gehen und dort Ihre persönlichen Daten einzugeben oder zu aktualisieren.

Sollten Sie eine solche Mail bekommen, können Sie also in der Regel von einem Phishing-Versuch ausgehen. Sollte Sie trotzdem unsicher sein, fragen Sie direkt bei der Bank oder der Firma nach.

Eine solche Nachfrage sollte immer per Telefon oder Fax erfolgen.

Sofern Sie lieber per Mail anfragen möchten, verwenden Sie die Ihnen bekannte Mailadresse des Unternehmens, niemals eine solche, die in der verdächtigen Mail genannt ist.

Die meisten Mailprogramme bieten Ihnen die Auswahl, ob Sie Mails im html-Format erhalten möchten oder im reinen Textformat. Entscheiden Sie sich für das Textformat. Mails mögen dann nicht mehr so farbig sein; irreführende Links – und andere Gefahren – gehören dann aber der Vergangenheit an. Wenn Sie Emails nur noch im reinen Textformat erhalten, sind die meisten Phishing-Attacken harmlos.

Seitenbesuch: Besuchen Sie Webseiten immer über das Lesezeichen in Ihrem Browser, oder geben Sie die Adresse (URL) manuell in die Adressleiste des Browsers ein.

Folgen Sie niemals den Links, die Ihnen in dubiosen Mails angezeigt werden.

Ignorieren: Reagieren Sie niemals auf Emails, in denen Sie zur Eingabe oder Aktualisierung persönlicher Daten aufgefordert werden.

Information: Wenn Sie eine verdächtige Mail – gleich welcher Art – erhalten, überprüfen Sie in den gängigen Suchmaschinen, was es damit auf sich hat.

Geben Sie hierbei passende Stichworte ein, etwa den Namen des vermeintlichen Absenders und den Begriff „Mail“, „Phishing“, oder auch „Betrug“.

Die hohe Zahl der Informations- und Verbraucherschutzseiten im Internet macht es wahrscheinlich, dass aktuelle Phishing-Attacken sehr schnell bekannt werden und entsprechende Warnungen veröffentlicht sind.

Technischer Schutz: Verwenden Sie auf Ihrem Computer immer aktuelle Antiviren-Programme und halten Sie Ihren Rechner stets auf dem aktuellsten Stand.

VPN nur ein Mythos ?

Aufgrund von Schlagzeilen von Datenausspähungen, und angeblicher Beobachtung von Regierungen und Organisationen, ist das Thema Anonymes Surfen aktuell wie nie zuvor. Auch die Datenschutz-Grundverordnung (DSVGO) hat in den letzten Wochen für viel Diskussionsstoff gesorgt. In diesem Zusammenhang werden nun auch viele Medien erneut auf das Thema VPN aufmerksam. An der einen Stelle heisst es, man solle VPN nutzen, um sich zu schützen. Neuerdings gibt es jedoch Artikel, die genau das Gegenteil behaupten, VPN sei nur ein Mythos. Doch was ist wirklich daran?

Sicherheit von VPN-Tools

Vom Grundsatz zu behaupten, VPN-Tools seien nicht sicher und würden keinen ausreichenden Schutz leisten ist nicht korrekt. Genauso falsch ist es zu behaupten, VPNs würden 100%igen Schutz gegen alle möglichen Ausspähungen bieten.Die meisten Artikel im Web über VPNs von Personen verfasst worden sind, die keine VPN-Experten sind, geschweige denn Kompetenzen im Bereich der Informatik aufweisen. Diese Artikel sollten mit Vorsicht genossen werden. Empfohlene und zuversichtliche Quellen sind beispielsweise Magazine wie die c't (heise Verlag), oder Hinweise vom Chaos Computer Club. Beide Quellen haben sich bislang positiv zu VPNs geäussert.

Unseriöse VPN-Anbieter

Zunächst ist festzuhalten, dass es eine Menge an VPN-Anbietern gibt. Darunter gibt es dubiose Anbieter, die am Trend reiten und unzureichend ausgereifte VPN-Software anbieten. Es gibt auch Anbieter, die sich als VPN-Tools tarnen, doch es handelt sich dabei um Viren und Trojaner – hier ist besondere Vorsicht geboten: vor allem sollte man die Finger von angepriesenen kostenlose VPN-Tools lassen.

Welche Daten sammeln VPN-Anbieter?

Da VPN-Anbieter Geld für ihren VPN-Service verlangen, speichern sie Zahlungsdaten des Nutzers, wie beispielsweise die Paypal-Email, Kreditkartennummern oder Bankdaten. Die VPN-Server dagegen sind anonym. Das heisst, im Falle einer Zurückverfolgung wüsste eine Behörde oder Organisation lediglich, dass man VPN-Dienste in Anspruch nimmt. Nicht nachverfolgbar ist dagegen der Datenverkehr, d. h. die übertragenen Daten. Insofern ist die Anonymität im Datenfluss gesichert.

Die Schwachstellen beim Anonymen Surfen mit VPN

Die Schwachstelle bietet der heimische Computer. Organisationen und Behörden können aufgrund einer VPN-Nutzung die Daten zwar nicht mitverfolgen. Aber bei einer Hausdurchsuchung liegen die Daten trotzdem auf dem eigenen PC. Allerdings stellt sich die Erbringung einer rechtlichen Hausdurchsuchung als schwierig heraus, wenn der Nutzer sich mit

VPN-Software tarnt. Wohl gemerkt: Bei einer VPN-Verbindung ist nicht nur die IP verschleiert, sondern auch der gesamte Datenverkehr findet verschlüsselt statt und ist somit für Aussenstehende nicht lesbar. Das heisst, lediglich eine Vermutung einer illegalen Handlung reicht für eine Hausdurchsuchung zumindest in den meisten europäischen Ländern nicht aus.

Wovor schützt VPN nicht?

Die grundsätzliche Frage ist daher, schützt VPN vor kriminellen Handlungen? Wie bereits erläutert, gelingt es den Behörden nicht den VPN-Datenverkehr auszulesen und als Beweismittel zu nutzen, unabhängig von der Höhe der kriminellen Tat. Vor allem im kleinkriminellen Bereich verlassen sich Nutzer auf die Sicherheit, die VPN bietet, vernachlässigen jedoch dabei andere Fakten und Mittel, die Ermittler zur Verfügung haben, um Täter dingfest zu machen.

Wovor schützt VPN?

Wie bereits erläutert, wenn es nur um den Schutz des Datenverkehrs und der Verschleierung der eigenen IP geht, bieten die seriösen Anbieter von VPNs in jedem Fall Schutz. Somit können Behörden und auch Organisationen nicht nachvollziehen, welcher Datenfluss stattfindet. Letztlich muss auch die Frage gestellt werden, in wie fern überhaupt amtliche Behörden Interesse oder rechtliche Handhabe haben, den Datenverkehr ohne richterliche Genehmigung abzuhören.

Wann schützt VPN?

Letztlich erfüllt VPN zwei wichtige Aufgaben. Es schützt den Datenverkehr und verschleiert die Herkunft des Nutzers. Vor allem private Organisationen haben in diesem Fall keine Chance nachzuverfolgen, wer oder was etwas übertragt. Die bislang in Hollywood-Filmen propagierten Methoden anonyme IPs durch Trangulationsmethoden zu verfolgen sowie VPN-Verschlüsselungen wie AES in Echtzeit zu entschlüsseln, sind bislang in der realen Welt nicht bestätigt worden. Das schliesst nicht aus, dass tatsächlich solche Methoden seitens Regierungsorganisationen existieren – allerdings gibt es in der Realität bis heute keinen Beweis oder bekannten Fall dazu.

Erstellung sicherer Passwörter: Gross Kleinschreibung, Zahlen, Sonderzeichen und mindestens 8- 12 Zeichen und für jeden Dienst ein eigenes Password wer soll sich das alles merken können?

1: Nicht Password sondern Pass- Satz oder Redewendung

Passwörter, zu denen ein Bezug hergestellt werden kann, lassen sich leichter merken als eine beliebige Buchstaben-Zahlenkombination. So kann beispielsweise ein Satz oder eine Redewendung verwendet werden (wobei bekannte Redewendungen eher ungeeignet sind). Trotzdem wird beispielhaft folgende Redewendung verwendet: ***Rosen sind rot, Veilchen sind blau!***
Durch die Verwendung der Anfangsbuchstaben sowie Sonderzeichen der Redewendung lässt sich folgendes Passwort erstellen: ***Rsr,Vsb!***
Das ist leicht zu merken, schwer zu erraten und die Wahrscheinlichkeit gering, dass weitere Personen die selbe Idee haben. Trotzdem, die Redewendung ist bekannt, weshalb es empfehlenswert ist, einen individuellen Satz zu verwenden.

2: Verschiedene Passwörter

Ja das nervt, ist aber unumgänglich. Es müssen zwingend verschiedene Passwörter für unterschiedliche Dienste wie E-Mail, Online-Banking, Facebook & Co verwendet werden. Sollte ein Dienst durch einen Hackerangriff fallen, sind alle anderen weiterhin sicher. Wie kann ein sicheres Passwort erstellt werden, dass eine Eselsbrücke zum verwendeten Dienst herstellt?

Wieder am Beispiel von Rosen sind rot, Veilchen sind blau! soll gezeigt werden, wie leicht sich eine gute Eselsbrücke für ein sicheres Passwort erstellen lässt. Dazu wird der Satz entsprechend angepasst: ***Rosen sind rot, Facebook ist blau!***
Das ergibt das Passwort: ***Rsr,Fib!***
Das Passwort hat jetzt 8 Zeichen, das genügt für die meisten Dienste. Es soll noch sicherer werden? Wie wäre es mit ***Rosen sind rot, Facebook ist blau und weiss!*** wodurch sich das Passwort ***Rsr,Fibuw!*** ergibt. Sicher? Auf jeden Fall! Zudem leicht zu merken und individuell passend für den jeweiligen Dienst.
Sollte das Passwort ***Rsr,Fibuw!*** einem Angreifer in die Hände fallen, ist es so gut wie ausgeschlossen, dass beispielsweise das Xing-Passwort ***Rsr,Xigug!*** (Rosen sind rot, Xing ist grün und grau!) erraten werden kann.

3: Zahlen hinzufügen

Für extra Pfeffer (Sicherheit) können Zahlen dem Passwort hinzugefügt werden. Beispielsweise können die Teilsätze mit Zahlen beginnen: ***1 Rosen sind rot, 2 Facebook ist blau!***
Das Passwort ***1Rsr,2Fib!*** kann nur mit viel Glück erraten werden. Selbst wenn dem Angreifer bekannt sein sollte, dass der Satz Rosen sind rot, Veilchen sind blau verwendet wird, die eingebaute Eselsbrücke durch die Individualisierung auf den verwendeten Dienst machen in diesem Fall das Passwort sicherer als die reine Redewendung. Verwendete Sonderzeichen und Zahlen erhöhen die Sicherheit zusätzlich.

4: Passwörter trgelmässig ändern

Das tut weh und kostet Zeit, erhöht jedoch die Sicherheit und fördert die grauen Zellen. Passwörter sollten wenigstens **jährlich** geändert werden, zwingend jedoch, sobald der verwendete Online-Dienst durch einen Hackerangriff in den Nachrichten auftaucht. Dabei müssen nicht die Passwörter bei allen Diensten auf einmal geändert werden.

5: Passwörter werden nicht geteilt!

So einfach ist das. Ist es euer Dienst, ist es euer Passwort! Muss ein Passwort an eine dritte Person weitergegeben werden, dann mündlich und nicht per SMS, E-Mail oder WhatsApp. Passwörter werden auch nicht aufgeschrieben, insbesondere nicht in eine Datei mit dem Namen *Passwörter* die im Ordner *Privat* liegt!!

Tipp

Bietet der Online-Dienst eine Zwei-Faktor-Authentifizierung an, sollte diese aktiviert werden. Dabei erfolgt der Login des Benutzers über zwei, voneinander unabhängige, Komponenten. Beispielsweise Browser und Bestätigungscode auf dem Smartphone. Das erhöht die Sicherheit extrem, kostet aber Bequemlichkeit bei jedem Login (insbesondere, wenn der Benutzer nach jeder Session automatisch ausgeloggt wird).

Was taugen Passwort-Manager?

Schwer zu sagen! Hier sollte vorher analysiert werden, wie die Passwörter übertragen werden sowie wie und wo die Passwörter gespeichert werden. Hat der Anbieter Zugriff auf die Passwörter im Klartext? Kann der Anbieter möglicherweise per Gerichtsbeschluss zur Herausgabe der Passwörter verpflichtet werden? Was passiert, wenn der Dienst gehackt wird?