Passwort-Guide

„Sicher ist, dass nichts sicher ist. Selbst das nicht.“
Joachim Ringelnatz

Autor	Karsten Schröder, Bad Malente	Datum	05.07.2017
Quelle	https://www.kscreen.info/passwort-guide.php	Version	1.0.2
Lizenz	Kostenfrei nutzbar. Die kostenfreie Weitergabe dieses Passwort-Guide in *unveränderter* Form ist ausdrücklich erlaubt. Kostenfreier Download, Verkauf oder sonstige kommerzielle Nutzung - auch auszugsweise - ist nicht gestattet.		

Auch wenn es keine absolute Sicherheit gibt, so kann und sollte jeder seine eigenen digitalen Daten so gut es geht, schützen.

Mindestens mit einem GUTEN Passwort.

Inhalt

Einleitung

In unserer digitalen Welt nimmt die Anzahl an persönlichen Zugängen zu den verschiedenen Diensten ständig zu. Der Zugang zum Online-Shop, dem Bankkonto, dem E-Mail-Account, dem sozialen Netzwerk - all diese Zugangsdaten muss man parat haben.

Leider sind die Gefahren, Opfer eines Datendiebstahls zu werden alltäglich und nehmen weiter zu.

Mit diesem Passwort-Guide möchte ich Ihnen helfen, weder ein leichtsinniges, noch ein zu kompliziertes Verhalten mit Ihren digitalen Zugangsdaten zu entwickeln. Vor allem möchte ich Ihr Sicherheitsbewusstsein stärken. Denn wenn erstmal Ihre Zugangsdaten in fremden Händen sind, können die daraus resultierenden Schäden enorm sein.

Zwei mögliche durchaus realistische Beispiele:

- Online-Shop: Sollte ein Fremder mit IHREN Zugangsdaten sich in einem Shop einloggen, kann er sämtliche von Ihnen hinterlegten Daten ändern. So wäre denkbar, dass er die von Ihnen hinterlegten Zahlungsmethoden und Daten (z.B. Kreditkartennummer) belässt, jedoch die Lieferadresse und E-Mail Adresse ändert. Auf diese Weise könnte er in Ihrem Namen Waren bestellen. Geliefert würden diese jedoch an eine andere Adresse. Auf Ihrer Kreditkarten-Abrechnung würden Sie dann eine Buchung sehen, die sie nicht zuordnen können. Der finanzielle Schaden wäre vorhanden. Nach dem Schreck ist eine Anzeige bei der Polizei aufzugeben, müssten Sie sich mit Ihrer Bank zeitnah um eine Rückbuchung bemühen und Ihre Kreditkarte sperren lassen. Dies kann sehr nervenaufreibend sein und im negativsten Fall erhalten Sie Ihr Geld nicht zurück.

- Soziales Netzwerk: Facebook, tumblr, twitter, Pinterest, XING, linkedin, ello, ... Egal, bei welchem Netzwerk Sie einen Account nutzen, Sie verfolgen damit private und/oder berufliche Kommunikation. Sollte ein Fremder Zugriff auf Ihr Konto erlangen, kann er sämtliche Inhalte ändern und weitere hinzufügen. Von falschen Aussagen zu Ihrer Person über das Veröffentlichen unangemessener Fotos oder Videos bis hin zu Beleidigungen Ihrer Kontakte kann ein falscher Eindruck entstehen, der schwierig oder gar nicht mehr richtig zu stellen wäre.

Diese Beispiele zeigen, wie aus der Bequemlichkeit, ein leicht knackbares Passwort zu verwenden, äußerst unschöne Situationen entstehen können.

Login, Passwort, Kennwort - was ist was?

Egal, bei welchem Webdienst man sich einloggen möchte, fast immer besteht das entsprechende Formular aus zwei Eingabefeldern. Das erste möchte mit Ihrem Benutzernamen und das zweite mit Ihrem Passwort gefüttert werden. Da - je nach Website und Einsatzzweck - unterschiedliche Begriffe verwendet werden, gebe ich Ihnen hier eine Begriffserklärung.

- **Benutzername**
  Das erste Feld wird ggf. mit einem der folgenden Begriffe benannt:
  - Benutzer ID (häufig eine Zeichenfolge aus Buchstaben und / oder Ziffern)
  - Login oder Loginname
  - Kundennummer (typisch bei Online-Shops)
  - Account, Kennung, Anmeldename
  - E-Mail Adresse (sollten Sie mehrere E-Mail-Adressen besitzen, muss hier die Adresse eingegeben werden, mit der Sie sich auf der entsprechenden Seite registriert haben.)
  - Kontonummer (Online Banking)

- **Passwort**
  Das zweite Feld ist für die eigentliche sicherheitsrelevante Eingabe gedacht und wird ggf. auch wie folgt benannt:
  - Kennwort, Schlüsselwort, Codewort
  - Passphrase, Losung, Losungswort
  - PIN (häufig nur eine 4-8 - stellige Ziffernfolge, daher nur bedingt als Passwort zu bewerten.)

Zum besseren Verständnis nutze ich in diesem Guide ausschliesslich die Begriffe „*Benutzername*“ und „*Passwort*“.

Passwort generieren

Ein Online-Shop, das Konto zu einem sozialen Netzwerk, der Zugang zu einem Cloud- Dienst,... Wo auch immer man sich anmelden (registrieren) möchte, ohne persönliche Zugangsdaten geht nichts.

Man sitzt also vor dem Formular, in dem man ein selbst erstelltes Passwort eingeben soll. Nicht selten tippt man dann ein Wort ein, welches man sich gut merken kann. Ob es dann der Name des Hundes, das Geburtsdatum der Ehefrau oder die Stadt, in der man aufgewachsen ist - ein Passwort im eigentlichem Sinn ist es nicht. Auch mehr oder weniger sinnvoll erscheinende Kombinationen aus Zahlen und Wörtern erhöhen die Sicherheit eines Passwortes kaum.

Einige Webseiten erstellen selbst ein - in der Regel relativ sicheres - Passwort, welches man nach der Registrierung per E-Mail zugeschickt bekommt. Dieses kann - und sollte - man schnellstmöglich selbst ändern. Ein Fehler wäre es, wenn man dann wieder den Namen des Hundes als Passwort verwendet.

Folgende Beispiele sind als Passwort **ungeeignet**:

- leicht zu tippende Zeichenketten oder Kombinationen dieser (qwertz, 123, abc, yxcv, asdfg, etc.)
- Bestimmte Zeichen durch ähnliche ersetzen (Beispiel: statt einem „e“ eine „3“ Oder statt einem „o“ eine „0“ (Null) - „Sup3rPassw0rt“)
- Namen (egal, ob eigener oder der von Freunden, Bekannten, Prominenten, Haustieren, Firmen, etc.)
- Zitate, Songtexte, Gedichte, TV-Sendungen, Filmen, etc.
- Datumsangaben (Geburtstage, Feiertage, Jahrestage, Ferien, Geschichtsdaten, etc.)
- Ortsangaben (Städte, Länder, Regionen, Flüsse, etc.)
- Normale Begriffe oder Wörter (insbesondere, wenn diese in Wörterbüchern zu finden sind)
- Begriffe einer fremden Sprache, da auch diese mit hoher Wahrscheinlichkeit in Wörterbüchern zu finden sind.

- Verfremdete Schreibweisen (rückwärts, Bindestriche zwischen Buchstaben, etc.)

Solche Varianten (oder Kombinationen dieser) führen ggf. dazu, dass andere Menschen Ihr Passwort nicht erraten können. Doch spezielle Software, die „Muster“ in den Passwörtern erkennt, kann unter Umständen in sehr kurzer Zeit Ihr Passwort entschlüsseln.

Um sicher zu stellen, dass weder Computer noch Menschen, die eigenen Passwörter knacken oder erraten, sollte ein Passwort so kryptisch wie möglich sein.

Der Grund:
IHRE Passwörter sind auf dem jeweiligen Server des Webseiten-Betreibers gespeichert. Leider kommt es immer mal wieder vor, dass Nutzerdaten von Kriminellen entwendet (gehackt) werden. Wer im Besitz IHRER Daten wäre, könnte in der Regel zwar nur verschlüsselte Informationen sehen, doch umso aufwändiger es ist, diese Verschlüsselungen zu umgehen, desto unwahrscheinlicher ist es, das Unbefugte mit IHREN Zugangsdaten unberechtigten Zugriff auf Ihren Account bekommen.

Kriminelle nutzen spezielle Crack-Software, um Passwörter zu ergaunern. Diese Software erkennt „Muster“, in dem sie Wörterbücher, Datumsangaben, etc. mit Ihrem Passwort vergleicht. Bei einer Übereinstimmung wäre Ihr Passwort geknackt. Der zeitliche Aufwand, den ein Passwort-Knacker für unterschiedlich sichere Passwörter benötigt, zeigt beispielhaft die folgende Tabelle:

Passwort	**Zeit*, die eine Software zum Knacken benötigt**
8-stellig (nur Ziffern)	weniger als eine Minute
8-stellig (nur kleine Buchstaben)	ca. 1 Tag, 5 Stunden, 32 Mnuten
8-stellig (Kleinbuchstaben und Ziffern)	ca. 16 Tage, 10 Stunden, 32 Minuten
8-stellig (Kleinbuchstaben, Ziffern und Sonderzeichen)	ca. 2 Jahre, 115 Tage, 16 Stunden, 29 Minuten
16-stellig (Kleinbuchstaben und Ziffern)	ca. 58 Jahre, 120 Tage, 18 Stunden

*Die Zeitangaben (berechnet und entnommen von: http://calc.opensecurityresearch.com/) sind theoretisch berechnete Werte. Eine Hack-Software würde per „HMAC MD5“ verschlüsselte Passwörter nach der „Brute-Force-

Methode“ in etwa die oben genannte Zeit benötigen, um ein Passwort zu knacken. Die notwendige Zeit hängt sehr stark von der verwendeten Hard- und Software sowie der Komplexität des Passwortes ab. Fakt ist, dass bessere Software und neuere, bzw. zukünftige Hardware **schnellere Entschlüsselungen** ermöglichen werden. Ferner sind deutlich schnellere Entschlüsselungen bei schwächer verschlüsselten Passwörtern als mit „HMAC MD5“ möglich.

Die Tabelle dürfte eindeutig zeigen, wie wichtig es ist, ein sicheres Passwort zu verwenden. Hieraus resultieren die folgenden Eigenschaften, die ein RICHTIGES Passwort aufweisen sollte:

- **Länge**: Je mehr Zeichen, desto besser. Mindestens 10 Zeichen sollte ein Passwort aufweisen. Es spricht nichts gegen 30 oder mehr Zeichen.
- **Zeichenauswahl**: Ein Passwort sollte aus verschiedenen Zeichen bestehen. Neben kleinen und großen **Buchstaben** sollten **Ziffern**, **Satzzeichen** und **Sonderzeichen** verwendet werden.
- Ein Passwort sollte nicht lesbar/auszusprechen sein. Wollte man ein Passwort vorlesen, sollte man jedes Zeichen einzeln nennen müssen. (Beispiel: kleines h, Plus-Zeichen, kleines y, grosses Y, 4, Semikolon, grosses O, Minus-Zeichen, usw.)

Mit meinem **Passwort Generator*** können Sie online Passwörter erstellen lassen:

https://www.kscreen.info/passwort-generator.php

Dieser berücksichtigt alle relevanten und hier genannten Eigenschaften zur Erzeugung sicherer Passwörter.

*Der Passwort Generator ist auf meine Initiative von brünger.media (https://www.bruenger-media.de) aus Kiel programmiert worden. Ich bedanke mich für die freundliche Zusammenarbeit.

- Beispiel für ein gutes Passwort (Dieses bitte **NICHT** verwenden!):
  `h+yY4;O-4xf/n.}gR;E8rPq91-Vv?Y"70jy9kv`

Passwörter ändern

Ihre Passwörter sind auf allen Webseiten, bei denen Sie sich angemeldet haben, gesichert. Wie bereits weiter oben erwähnt, kommt es von Zeit zu Zeit vor, das Server gehackt werden. So gelangen persönliche Daten in fremde Hände oder werden gar veröffentlicht.

Aus diesem Grund ist es sehr zu empfehlen, regelmäßig seine Passwörter durch neuere zu ersetzen. Loggen Sie sich am Besten auf jeder Website, bei der Sie einen Zugang haben, hin und wieder ein und ändern Ihr Passwort. Dies sollten Sie mind. alle 6 Monate machen.

Darüber hinaus ist es sinnvoll nachzuschauen, ob alle Einstellungen noch aktuell sind und keine ungewollten Informationen vorhanden sind. Falsche oder veraltete Informationen können Sie so aktualisieren.

Sollten Sie bei einem solchen „Rundgang“ feststellen, dass Sie einen bestimmten Dienst gar nicht mehr benötigen, so können Sie ggf. den entsprechenden Account komplett löschen. Daten, die nicht vorhanden sind, können auch nicht missbraucht werden.

Passwörter merken / verwalten

Je sicherer (kryptischer) ein Passwort ist, desto schwieriger ist es, sich dieses zu merken. Es wird dann noch mal schwieriger, wenn man mehrere unterschiedliche Passwörter nutzt. So stellt sich die Frage, wie man den Überblick behält. Grundsätzlich kann man zwischen analogen und digitalen Lösungen unterscheiden:

Analoge Lösungen

- Passwörter auf Papier schreiben (Passwort-Liste):
  Diese Lösung hat den klaren Vorteil, dass Ihre Passwörter nicht digital von Ihrem Computer gestohlen werden können. Jedoch ist es wenig praxisfreundlich, kryptische Passwörter manuell beim Login abzutippen. Die Liste mit den Passwörtern sollte an einem geheimen Ort (zum Beispiel in einem Safe) aufbewahrt werden. Ferner sollten die Zettel mit den Passwörtern nicht unmittelbar als Passwort-Liste erkennbar sein.

- Merken:
  Wenn Sie sich zutrauen, Ihre (diversen) Passwörter im Kopf zu merken, ist dies zweifelsfrei die beste Methode und auch ein gutes Gedächtnis-Training. Vermeiden Sie jedoch, (knackbare) Muster in ihren Passwörtern zu verwenden. So sollte man beispielsweise *nicht identische Zeichenfolgen* mit einem dem Dienst zugehörigen Anhang benutzen. (Beispiel: IcliDi2014-fbook für Facebook und IcliDi2014-twit für Twitter und IcliDi2014-glge für den Google-Account.)

Digitale Lösungen

Der Vorteil der digitalen Lösung ist, das man das zu nutzende Passwort sofort am Rechner parat hat und dieses per *kopieren und einfügen* sofort nutzen kann. Egal, für welche digitale Variante man sich entscheiden mag: Die Daten sollten gut verschlüsselt gesichert werden und NUR mit einem (!) „Master-Passwort“ ausschließlich von Ihnen aufgerufen werden können. Dieses Master-Passwort sollte niemals auch als Passwort für eine Website genutzt werden.

- Passwörter in eine (Text-) Datei schreiben:
  Diese Form ist durchaus möglich. Man sollte jedoch darauf achten, dass die Datei nicht von Fremden eingesehen werden kann. Daher sollte die Datei verschlüsselt gesichert sein und wiederum mit einem (Master-) Passwort geöffnet werden können. Eine solche Textdatei sollte NICHT mit Word oder einer anderen weit verbreiteten Textverarbeitung erstellt werden, sondern mit einem einfachen Textprogramm als *.txt oder *.rtf - Datei gesichert sein. Ferner ist es ratsam, eine solche Datei auf einem externen Datenträger (z.B. USB-Stick) zu sichern, der ebenfalls verschlüsselt und über ein Passwort gesichert ist.
  Beispiel-Inhalte einer Tabelle mit Zugangsdaten:

Anbieter	Anmelde-Datum	Benutzername	Passwort	E-Mail-Adresse
Shop xy	16.03.2017	HansMeier	8:iFT9/Vfks&PeL“2CeU-hB1Dy5K	hansmeier@domain.de
Soz. Netzwerk	30.12.2016	HMeier	$vTH1p4J(S,b4XGFcJS%bLx9A2	hmeier@domain2.de
App-Store	19.04.2017	Hmeier589	m?,f7n4ydpi)Gb&WBzXa:6UAjc5+	hansmeier@domain.de

  Eine solche Tabelle kann nach eigenen Vorstellungen mit weiteren Informationen wie zum Beispiel Informationen zur Sicherheitsfrage, hinterlegter Telefonnummer oder Notizen erweitert werden.

- Passwortverwaltung im Browser: Diese Möglichkeit hat den Vorteil, dass Ihre Zugangsdaten unmittelbar beim Login vorliegen. Der Nachteil ist jedoch, dass sie nur im Browser gesichert sind und ggf. unsichere Synchronisationen mit anderen Geräten eine Sicherheitslücke darstellen können. Ferner bestehen in der Regel begrenzte Möglichkeiten der Verwaltung. So ist das manuelle Anpassen oder kopieren der Daten eingeschränkt oder nicht möglich.
- Passwörter mit einem Passwort-Manager verwalten:
  Es gibt eine Reihe von Programmen, mit denen man seine Passwörter (inkl. weiteren Informationen zu seinen Zugangsdaten) bequem verwalten und pflegen kann. Diese Programme speichern Ihre Zugangsdaten verschlüsselt auf Ihrem Computer. Über ein Master-Passwort gelangt man an alle in dem Programm gesicherten Zugangsdaten

  Auf den folgenden Webseiten erhalten Sie Informationen zu einer Auswahl geeigneter Programme*:
  - mSecure: https://www.msecure.com (kostenpflichtig)
  - onePassword: https://1password.com (kostenpflichtig)
  - dashlane: https://www.dashlane.com/passwordmanager (kostenfrei)
  - iPIN: https://www.ipin.ibilities.com/de/ (kostenpflichtig)
  - Keeper: https://keepersecurity.com/ (kostenpflichtig)
  - KeePass: http://keepass.info/ (OpenSource / kostenfrei)
  - LastPass: https://lastpass.com/ (Kostenfrei / kostenpflichtige Version verfügbar)

*Ich übernehme keine Verantwortung für die Inhalte der verlinkten Webseiten. Der Besuch sowie das Herunterladen / die Nutzung der Software geschieht auf eigenes Risiko. Die Kosten-Angaben sind den jeweiligen Webseiten im Januar 2017 entnommen. Diese können sich ggf. geändert haben.

Ungeeignete Lösungen zur Passwort-Verwaltung:

- Zettel mit Passwort an den Computer-Monitor kleben.
- Zettel mit Passwörtern auf dem Schreibtisch offen sichtbar liegen lassen.
- Einfache Textdatei (Notiz-App, SMS, oder ähnlich) unverschlüsselt auf einem Smartphone, Tablett oder Zweitrechner sichern.

10 Tipps für die Praxis

1. Behalten Sie den Überblick Ihrer Accounts. Führen Sie hierfür eine Liste oder nutzen Sie einen Passwort - Manager.
2. Benutzen Sie ausschließlich sichere Passwörter (mind. 10 Zeichen inkl. Sonderzeichen, Satzzeichen, große und kleine Buchstaben sowie Ziffern)!
3. Benutzen Sie pro Konto ein eigenes / anderes Passwort (Also bei eBay ein anderes als bei Amazon und beim Online-Banking wieder ein anderes.)
4. Ändern Sie regelmäßig (mind. alle 6 Monate) bei allen Konten Ihr Passwort.
5. Nachdem Sie keine weiteren Aktionen in Ihrem Account vornehmen möchten, loggen Sie sich aus. Schliessen Sie nicht nur den Browser oder den Tab.
6. Behalten Sie Ihre Passwörter für sich - niemand (!) sollte sie kennen.
7. Bewahren Sie alle Ihre Passwörter an einem nur für Sie zugänglichem Ort auf oder merken Sie sich ihre Passwörter. Alternativ nutzen Sie eine digitale Passwort-Verwaltungssoftware. Vermeiden Sie es, Passwörter - egal in welcher Form - in einem Cloud-Account online zu sichern.
8. Sollte ein Fall bekannt werden, in dem Zugangsdaten von Nutzern eines Anbieters gestohlen wurden, ändern sie schnellstmöglich ihr Passwort bei dem entsprechendem Anbieter.
9. Sofern es angeboten wird, nutzen Sie die 2-Faktor Authentifizierung (lesen Sie hierzu bitte den entsprechenden Abschnitt in diesem Dokument).
10. Wenn Sie sicher sind, dass Sie einen Webdienst (zum Beispiel einen Online-Shop) nicht mehr nutzen möchten, löschen Sie komplett und unwiederbringlich Ihren Account.

Passwort vergessen?

Eigentlich bietet jede Webseite die Möglichkeit an, Ihnen zu helfen, wenn Sie Ihr Passwort vergessen haben sollten. Die Funktion „Passwort vergessen“ anklicken und man erhält eine E-Mail mit Informationen, was man tun soll. In den meisten Fällen wird man gebeten, einen Link anzuklicken und dann über ein Formular ein neues Passwort einzurichten. Nachdem dies erfolgt ist, kann man sich mit dem neuen Passwort einloggen.

Etwas anders sieht es aus, wenn direkt in der E-Mail das Passwort genannt wird. Da es als sehr unsicher gilt, Passwörter per E-Mail zu übertragen, sollte man diesen Moment nutzen, sein Passwort zu ändern.

Die Sicherheitsfrage

Auf einigen Webseiten werden Ihnen Sicherheitsfragen wie „Wie hiess ihre erste Lehrerin?“ oder „In welcher Stadt sind sie aufgewachsen?“ gestellt. Man sollte sich bewusst sein, dass sich die Antworten auf eine solche Frage ggf. leicht heraus finden lassen. Daher sollten Sie diese Fragen nicht korrekt beantworten. Jedoch sollten Sie sich die entsprechende (falsche) Antwort gut merken oder in Ihrer Passwort-Verwaltung vermerken.

Diese Fragen dienen der zusätzlichen Sicherheit, da sie von Ihnen beantwortet werden müssen, um z.B. Ihr Passwort zu ändern.

Das Telefon-Passwort

Dieses Passwort wird (zusätzlich zu den üblichen Zugangsdaten) benötigt, wenn man mit dem Betreiber einiger Webseiten telefonisch in Kontakt tritt. Der Mitarbeiter kann auf diese Weise sicher stellen, dass Sie die Person sind, für die sich ausgeben.

Beispielsweise wird ein Telefon-Passwort bei einigen Webhosting-Anbietern genutzt, wenn telefonisch vertragliche Änderungen durchgeführt werden sollen.

Noch sicherer: Passwort + 2-Faktor Authentifizierung

Seit einiger Zeit wird auf Webseiten eine weitere, zusätzliche Sicherheitsstufe eingebaut. Die 2-Faktor Authentifizierung erfordert zusätzlich zum Passwort eine weitere Information, die der Nutzer über ein weiteres Gerät (meistens über ein Handy) erhält. Weit verbreitet ist die Methode, dass Sie beim Login neben Ihrem Benutzernamen und Passwort eine PIN per SMS erhalten, die Sie eingeben müssen, um den Login-Vorgang abzuschliessen.

Eine weitere typische Anwendung der 2-Faktor Authentifizierung ist die „SMS-TAN" beim Online-Banking. Ohne die nur für kurze Zeit aktive TAN (Transaktionsnummer, meist 6-stellig) ist der erfolgreiche Abschluss z. B. einer Überweisung nicht möglich.

Auch wenn sie ein wenig umständlicher ist, stellt die 2-Faktor Authentifizierung eine deutlich höhere Sicherheitsstufe gegenüber einer reinen Passwort-Abfrage dar. Wenn Ihnen bei einem Webdienst die 2-Faktor Authentifizierung angeboten wird, sollten Sie diese auch in Anspruch nehmen.

Eigenschaften sicherer Webseiten

Auch wenn Sie keinen Einfluss auf die eingesetzten Technologien einer Website haben, an den folgenden Eigenschaften können Sie erkennen, wie bemüht der Webseiten-Betreiber ist, Ihre Daten zu schützen:

- Werfen Sie zuerst einen Blick in die Adresszeile: Ist dort ein grünes Schloss-Symbol zu sehen oder ist ein Teil der Adressangaben grün unterlegt? Wenn ja, benutzt die Website eine verschlüsselte Übertragung per SSL. Dies ist meistens auch zu Beginn der Adresse, welche mit https://.. zu erkennen. Eine unverschlüsselte Übertragung beginnt mit mit http://... (ohne „s").
- Sie werden bei der Passwort-Vergabe grafisch und / oder textlich über die Qualität Ihres Passwortes informiert.
- Es besteht eine Mindest-Zeichenlänge (z.B. 10 Zeichen) für Ihr Passwort.
- Es besteht *keine* Maximal-Zeichenlänge (z.B. 20 Zeichen).
- Sie werden aufgefordert, Ziffern, Sonderzeichen und grosse Buchstaben zu verwenden.

- Bei wiederholten Falschangaben beim Einloggen wird Ihnen der Zugriff für eine bestimmte Zeit oder dauerhaft verweigert.
- Sie erhalten Ihr Passwort nicht in einer E-Mail genannt, sondern in den E-Mails sind Links vorhanden, die Sie nutzen können, um Ihre Anmeldung zu bestätigen oder Ihr Passwort zu ändern.

Passwort-Diebstahl vermeiden

Die folgenden Tipps sind kein Garant für ein mögliches Ausspähen Ihres Passwortes (oder weiterer Daten), doch können sie dazu beitragen, die Gefahr gering zu halten. Die Tipps sollten auf jedem Gerät (stationärer Computer, Notebook, Smartphone und Tablett) beherzigt werden.

- Benutzen Sie ein gutes Benutzer-Passwort, um Ihren Computer (oder Smartphone) nutzen / entsperren zu können.
- Sichern Sie Ihr eigenes WLAN-Netz mit einem guten Passwort.
- Öffnen Sie E-Mail (oder Messanger) - Anhänge nur, wenn Sie sich sicher sind, dass sie diese erhalten sollen und/oder erwarten. Beim geringsten Verdacht auf dubiosen/zweifelhaften Inhalt, löschen Sie die Nachricht inkl. Anhang sofort. Datei-Anhänge mit den folgenden Endungen können gefährliche Inhalte enthalten: *.exe, *.zip, *.doc, *.docx, *.ppt, *.xls.
- Vorsicht bei Phishing - Mails: Klicken Sie nicht unüberlegt auf Links, die in E-Mails enthalten sind. Insbesondere wenn die Mail im mäßigen Deutsch geschrieben ist, sie aufgefordert werden, etwas zu verifizieren oder ähnlich oder Sie gar nicht Kunde des vermeintlichen Absenders sind.
- Sämtliche Programme und Apps, die Sie benutzen, sollten möglichst zeitnah aktualisiert werden, sobald Updates erscheinen. Hierzu gehören insbesondere:
  - das Betriebssystem (Windows, Mac OS, Linux, Android, IOS)
  - der Browser (Firefox, Google Chrome, Opera, Safari, Internet Explorer, Edge, Vivaldi, etc.)
  - das E-Mail-Programm (Thunderbird, Outlook, Apple Mail, etc.)
  - eingesetzte Messanger (Skype, ICQ, Whatsapp, Threema, Telegram, Signal, Line, SIMSme, etc.)
  - Office-Software (OpenOffice, MS Office, iWork, etc.)

  - Finanzprogramme (Buchhaltungssoftware, Online-Banking-Tools, Steuererklärungsprogramme, etc.)
- Plugins und Zusatzprogramme (z.B. Flash, Java, Acrobat-Reader, etc.) sollten stets aktuell sein oder - wenn nicht nötig - deinstalliert werden.
- Virenschutz-Software (inkl. Virendefinitionen) sollten stets auf dem neuesten Stand sein. Diese Schutzprogramme sollten so eingestellt sein, dass sie möglichst viele Schädlinge (Trojaner, Keylogger, Phishing-Mails, etc.) zeitnah erkennen.
- Fremde Datenträger (ext. Festplatten, USB-Sticks, Speicherchips, DVD's, etc.) sollten Sie vor Nutzung der enthaltenen Daten mit Ihrem Schutzprogramm auf mögliche Schadsoftware prüfen.
- Die im Computer installierte Firewall sollte stets eingeschaltet sein.
- Router Firmware: Das Gerät, welches Sie von Ihrem Provider für Ihren DSL- oder Kabel-Anschluss zur Verfügung gestellt bekamen, sollte die aktuelle Firmware nutzen.
- Geräte, die nicht typischerweise einen Computer darstellen, basieren auf Software, die ebenfalls in regelmäßigen Abständen ein Hersteller-Update erhalten. So sollten Sie Ihren Fernseher, Ihren Backofen oder Ihren Rasen-Roboter auch aktuell halten.
- Sofern möglich, vermeiden Sie die Nutzung Ihrer Zugangsdaten auf fremden Computern (Internet-Café, Hotel-Bar, Computer von Freunden oder Verwandten, etc.).
- Drahtlose Schnittstellen wie Bluetooth, NFC (Near Field Communication), WLAN, GPS oder Infrarot-Sensoren sollten bei mobilen Geräten wie z.B. Smartphones nur dann eingeschaltet sein, wenn diese benötigt werden. Tipp: Ausgeschaltete Funktionen können den Betrieb mit einer Akku-Ladung verlängern.
- Öffentliche WLAN-Netze können von Kriminellen missbraucht werden, um im Netzwerk befindliche Computer auszuspähen. Daher sollten öffentliche WLAN-Netze nur genutzt werden, wenn dies nötig erscheint.
- Räumen Sie von Zeit zu Zeit in den von Ihnen genutzten Cloud-Diensten auf und löschen nicht mehr benötigte Daten.

Internet der Dinge und weitere Geräte, die mit dem Netz kommunizieren

Neben den „normalen“ Computern wie Desktop’s, Notebooks, Tabletts und Smartphones können eine Vielzahl von weiteren Geräten im Internet online sein. Bei jedem Gerät ist dies nicht auf Anhieb erkennbar, doch sind Fernseher (Smart-TV), AV-Receiver, Radios, Fitness-Armbänder, Uhren, Sprach-Assistenzsysteme, Thermostaten, Garagentore, Backöfen, Kühlschränke einige Beispiele dafür, dass im Haushalt häufig unbemerkt Kommunikation über das Internet statt findet.

Diese Geräte sind meist über das eigene WLAN mit dem Internet verbunden und stellen daher eine zusätzliche Gefahr dar. Diese Geräte sollten ebenfalls hinsichtlich der Software (häufig als „Firmware“ betitelt) aktuell gehalten werden.

Passwort weitergeben?

Es gibt einige wenige Ausnahmen, bei der Sie Ihr Passwort einer anderen Person weitergeben können:

- Wenn Sie ein Dokument erstellt haben, welches nur bestimmte Personen öffnen dürfen sollen, können Sie dies bei der Speicherung (Beispiel: eine PDF-Datei) mit einem Passwort versehen. Dem Empfänger können Sie in einem solchen Fall das Passwort - zum Beispiel telefonisch - mitteilen.
- Im Firmen-Alltag kommt es hin und wider vor, dass mehrere Personen ein und denselben Account nutzen. In einem solchen Fall nutzen zwei (oder gar mehr) Personen identische Zugangsdaten. Dies kann in seltenen Fällen als akzeptabel gelten, doch sollte dies lediglich für einen begrenzten Zeitraum aktiv sein. Grundsätzlich sollte jeder Mitarbeiter einen eigenen Account (z.B. zum firmeninternen Intranet) besitzen.

Fazit

Es ist jedem zu empfehlen, die persönlichen Zugangsdaten - insbesondere das Passwort - wie einen Schlüssel zu verstehen und entsprechend zu nutzen. Auch wenn es niemals eine absolute Sicherheit geben wird, so sollte jeder im eigenen Interesse die in diesem Passwort-Guide genannten Empfehlungen aktiv nutzen.

Ich bedanke mich für Ihr Interesse an diesem Dokument und hoffe, Ihnen hilfreiche Informationen gegeben zu haben.

Impressum / Kontakt

Autor:	Karsten Schröder / KScreen Web Dienstleistungen
Webseite:	https://www.kscreen.de
Adresse:	Stenkamp 7, 23714 Bad Malente-Gremsmühlen, Deutschland
Kontakt:	E-Mail: passwort-guide@kscreen.de
	Tel. 04523 / 880 31 31
Online-Quelle:	https://www.kscreen.info/passwort-guide.php

Haftungsinformationen