Sicheres-Netz

Wir sorgen für mehr Sicherheit im Netz

Ratgeber

PASSWORTSCHUTZ

Zugriff richtig schützen!

Autor: Markus Breitenstein

Sicheres-Netz.com

E-Mail Dienste, Internetportale, Onlineshops und soziale Netzwerke haben oft eines gemein – sie lassen unsichere Passwörter zu. Und das, obwohl dieses Passwort in Verbindung mit einem Benutzernamen, oder einer E-Mail Adresse oftmals die einzige Hürde ist die ein Angreifer nehmen muss, um an persönliche Daten zu kommen.

Je einfacher und leichter das Passwort ist, desto leichter können Unbefugte sich Zugriff verschaffen und damit nicht nur persönliche und vertrauliche Informationen abgreifen, sondern darüber hinaus beispielsweise auch Bestellungen tätigen, aber auch anderen wirtschaftlichen Schaden verursachen. Trotz der in Medien berichteten mangelnden Passwortsicherheit sind Passwörter wie “Passwort”, “123456”, “12345678”, aber natürlich auch Passwörter in Form des Geburtsdatums, als auch dem eigenen Nachnamen Gang und Gäbe.

Um den Zugang zu E-Mail Diensten, Internet-Portalen, Onlineshops und sozialen Netzwerken gegen Kriminelle zu schützen, sollten Sie diesen Zugriff und damit natürlich auch das Passwort sicher gestalten. Unser Passwort-Generator unterstützt Sie dabei, schnell wirkungsvolle sichere Passwörter für E-Mail Dienste wie web.de FreeMail, GMX und GoogleMail, für Onlineshops und Marktplätze wie Amazon, eBay und Zalando, bis hin zu sozialen Netzwerken wie Facebook, Instagram, Pinterest, Snapchat und Twitter und anderer Anbieter zu generieren.

Darüber hinaus erhalten Sie wertvolle Tipps, worauf Sie bei der Vergabe von Passwörtern und Kennwörtern achten müssen.

8 Tipps zum sicheren Passwort

Wenngleich Sie möglicherweise das Passwort, welches über den Passwort-Generator erstellt wird, abschreckt, desto mehr Wirkung und Schutz bietet dies gegenüber Kriminellen. Doch auch Passwort-Generatoren, welche viele Portale bereits mit der Registrierung bieten, aber auch bei Passwort-Änderungen zum Einsatz kommen, entsprechen einer sehr hohen Passwortsicherheit. Dennoch werden diese meist viel zu selten in Anspruch genommen.

Tipp 1: keine leichten Passwörter verwenden

Es ist immer wieder erschreckend zu hören, aber auch zu sehen, mit welch einfachen Passwörtern Zugänge zu E-Mail-Diensten, Online-Banking, aber auch zu Online-Shops und sozialen Netzwerken abgesichert wird. Beliebt sind Vornamen, Nachnamen, beides in Kombination mit dem Geburtsjahr, aber auch einfach nur das Geburtsdatum. Das meist genutzte Passwort ist tatsächlich auch “Passwort”.

Die Verwendung solch leichter Passwörter kann man fast schon als grob fahrlässig bezeichnen. Das ist zu vergleichen mit einer Wohnung, deren Wohnungstür man offen stehen lässt, obwohl diese gut gegen Einbrüche gesichert wäre. In der Wohnung liegt dann noch ein dickes Geldbündel herum, obwohl ein nahezu diebstahlsicherer Safe vorhanden ist.

Tipp 2: Lange Passwörter verwenden

Je kürzer das Passwort, desto leichter kann dies durch Kriminelle geknackt werden. Auf vielen Portalen rät man zu Passwörtern mit mindestens 8 Zeichen.

Wir raten zu mindestens 12 Zeichen, verwenden jedoch selbst Passwörter ab 16 Zeichen. Natürlich stellt ein längeres Passwort auch eine gewisse Hürde dar. Schließlich muss man sich nun deutlich mehr Zeichen merken und auch deutlich mehr Zeichen regelmäßig eingeben.

Doch genau vor dieser Herausforderung stehen auch Kriminelle. Denn je länger das Passwort, desto mehr Kombinationen sind möglich und je mehr Kombinationen bedeutet gleichzeitig mehr Zeit.

Tipp 3: Passwortstärke durch Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen

Passwörter, die ausschließlich aus Buchstaben, oder Zahlen bestehen, können von Kriminellen sehr schnell geknackt werden. Deutlich schwieriger sind dagegen Passwörter, die eine Kombination aus Kleinbuchstaben (a-z), Großbuchstaben (A-Z) Zahlen (0-9) und Sonderzeichen ($,%,#,!,…) willkürlich angeordnet bestehen. Eine kleine Kostprobe gefällig?

1.) 1(1)Bs9R59MD&))%$
2.) äj%ü3yPÖgLp23VÜTa

Sie können unseren Passwortgenerator benutzen, oder zur Erstellung von Passwörtern einige Eselsbrücken nutzen, die wir nachfolgen vorstellen möchten. Keinesfalls sollten Sie jedoch die hier beispielhaft abgedruckten Passwörter verwenden.

Passwort: !b73g+v€mdEvWiI

(**!**)ch **b**in 19**73 g**eboren und (**+**) **v**erdiene Geld (**€**) **m**it **d**er **E**rstellung **v**on **W**ebsites **i**m **I**nternet.

Das Ich kennzeichne ich mit einem Ausrufezeichen, während ich dann jeweils den ersten Buchstaben des Satzes mit einigen Ausnahmen betrachte. Und ersetze ich durch das mathematische Pluszeichen (+) und Geld lässt sich mit dem Euro-, oder Dollarzeichen ersetzen.

Link: https://sicheres-netz.com/passwort-generator/

Tipp 4: keine identischen Passwörter verwenden

Tatsächlich ist die Verwendung identischer Passwörter nicht nur das größte Problem, sondern stellt auch die größte Herausforderung dar dies eben nicht zu tun. Denn in je mehr Portalen man angemeldet ist, desto mehr Passwörter benötigt man. Password-Safe Tools können hier Abhilfe schaffen, wobei diese evtl. auch eine Gefahr darstellen, denn alle Passwörter werden in einer Applikation gespeichert.

Tipp 5: Regelmäßiges Ändern von Passwörtern

Das regelmäßige Ändern von Passwörtern erhöht zusätzlich den Schutz der unterschiedlichen Konten im Netz. Das Ändern von Passwörtern solltest Du in Abhängigkeit zur Passwortlänge entweder nach 6 oder 12 Monaten erneut durchführen. Bei einer Passwortlänge ab 16 Zeichen ist eine jährliche Änderung ausreichend. Bei kürzeren Passwörtern empfehlen wir eine Passwortänderung nach 6 Monaten. Idealerweise tragen Sie sich einen Serientermin in ihren Kalender ein, damit Sie das Ändern ihrer Passwörter nicht vergessen.

Tipp 6: Passwörter kombinieren

Je länger das Passwort, desto besser. Doch irgendwie ist es gar nicht so einfach sich neue Passwörter schnell einzuprägen. Kombiniert man jedoch bisher verwendete Passwörter, ergeben sich einerseits viele neue Kombinationen, andererseits wird das neue Passwort deutlich länger und ist dadurch von Kriminellen schwieriger zu knacken. Allerdings sollte man nicht das Passwort "Passwort" mit "1234567890" kombinieren ;), denn Passwort1234567890 ist nun auch nicht gerade sicher.

Tipp 7: Passwörter nicht speichern

In der Tat gibt es bereits diverse Möglichkeiten seine Passwörter zu speichern. So wird man bereits über den Webbrowser gefragt, ob das Passwort gespeichert werden soll. Eigentlich eine ganz bequeme Sache, denn so muss man beim Anmelden nicht immer das Passwort händisch eintragen, sondern es wird automatisch eingesetzt. Doch genau das kann einem auch zum Verhängnis werden. Insbesondere dann, wenn sich Kriminelle mit Spyware Zugriff auf ihren heimischen Rechner verschaffen. Nun gibt es aber auch Software, sogenannte Password-Safe Tools, mittels welcher alle Passwörter in einem Programm geschützt sein sollen. Doch auch hier gibt es Schwachstellen. So gab es bereits in der Vergangenheit erfolgreiche Ausspähungen von Tools wie beispielsweise 1-Password.

Tipp 8: 2 Faktor-Authentisierung

Die 2 Faktor-Authentisierung, häufig auch 2-Faktor-Authentifizierung genannt, bieten heute bereits soziale Netzwerke, diverse E-Mail-Dienste, als auch Onlineshops. Über die mittelbare 2-Faktor-Authentisierung ist ein Zugriff nur mit bereits authentifizierten Geräten möglich. Geschieht ein Zugriff über ein neues Gerät, muss dies zunächst über ein bereits authentifiziertes Gerät aktiviert werden. Ein Beispiel: Sie kaufen sich ein neues Notebook und melden sich das erste Mal bei iTunes, oder Facebook an, erhalten Sie eine Nachricht an alle bereits authentifizierten Geräte. Erst wenn Sie selbst dies bestätigen, erhalten Sie Zugriff über dieses neue Gerät auf ihr Konto. Die 2-Faktor-Authentisierung ist daher ein sehr wirksamer Schutz vor Angriffen.

Auch wenn Sie jetzt denken, dass dies ganz schön viel Aufwand ist, ist dieser Aufwand gemessen an dem potentiellen Schaden weitaus geringer.