Conectix - Blumenstraße 2 - 03159 Döbern

Passwort Generator

Sichere Passwörter erstellen - ein Passwort Generator hilft

Ein sicheres Passwort ist eine Aufgabe, die wohl jedem schwer fällt. Denn es soll zum einen "sicher" sein und zum anderen gilt es sich dieses gut einprägen zu können. Mit einem Passwort Generator haben Sie die Möglichkeit, online zufällige und sichere Passwörter zu erstellen.

Ihre cleveren Passwort-Tricks schützen Sie nicht vor Hacker-Angriffen

Sicherheitslücken kommen heutzutage so oft vor, dass Sie es wahrscheinlich satt haben, davon zu hören und davon wie Sie Ihre Konten besser sicher können. Auch wenn Sie denken, Sie haben schon alles gehört, sind die heutigen Tools zum Knacken von Passwörtern weiter fortgeschritten und umgehen die cleveren Tricks, die viele von uns anwenden.

Lassen Sie sich von uns sagen: Passwörter sind einfacher zu knacken als je zuvor! Die Passwörter sind heute noch unsicherer, als noch vor wenigen Jahren, aufgrund der besseren Hardware und neuer Techniken, die von Passwort-Crackern verwendet werden. Ars Technica erklärt, dass kostengünstige Grafikprozessoren es Passwort-Cracking-Programmen ermöglichen, Milliarden von Passwortkombinationen in einer Sekunde auszuprobieren. Was einst Jahre gedauert hätte, kann nur Monate oder vielleicht Tage dauern.

Erschwerend kommt hinzu, dass Hacker viel mehr über unsere Passwörter wissen als früher. All die jüngsten Passwortlecks haben

Hackern geholfen, die Muster zu identifizieren, die wir beim Erstellen von Passwörtern verwenden, sodass Hacker jetzt Regeln und Algorithmen verwenden können, um Passwörter schneller zu knacken als durch einfache Common-Word-Attacken.

Nehmen Sie das Kennwort "Sup3rThinkers" - ein Kennwort, das aufgrund seiner Länge von 13 Zeichen und der Verwendung von Groß- und Kleinschreibung und einer Zahl die meisten Kennwortsicherheitstests besteht. Wie sicher ist mein Passwort? Schätzungen zufolge würde ein Desktop-Computer etwa eine Million Jahre brauchen, um dieses Passwort zu knacken, mit einer Schätzung von 4 Milliarden Berechnungen pro Sekunde. Ein Hacker würde nur ein paar Monate brauchen!

Erstellen Sie starke, einzigartige und unvorhersehbare Passwörter

1. Vermeiden Sie vorhersehbare Passwortformeln

Das größte Problem ist, dass wir alle unsere Passwörter auf die gleiche Weise auffüllen (teilweise, weil die meisten Unternehmen Ihre Passwortlänge begrenzen und bestimmte Arten von Zeichen benötigen). Wenn es erforderlich ist, eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Symbolen zu verwenden, tun die meisten von uns folgendes:

- Sie verwenden einen Namen, einen Ort oder ein allgemeines Wort als Kern, z. B. "Fido" (Frauen verwenden in der Regel persönliche Namen und Männer verwenden in der Regel Hobbys).
- Großschreibung des ersten Buchstabens: "Fido"
- Fügen Sie am Ende eine Zahl hinzu, höchstwahrscheinlich 1 oder 2: "Fido1"
- Fügen Sie am Ende eines der häufigsten Symbole (~,!, @, #, $,%,

&,?) Hinzu: "Fido1!"

Nicht nur, dass diese Muster für professionelle Passwort-Hacker offensichtlich sind, auch das Ersetzen von Zahlen durch Vokale ("F1d01!") oder das anhängen eines anderen Wortes ("G00dF1d01!") würde nicht viel helfen, da Hacker die Muster gegen uns verwenden.

Die Lösung: Tun Sie nicht das, was alle anderen tun. Vermeiden Sie die obigen Muster und beachten Sie die Grundlagen: Verwenden Sie in Ihrem Passwort kein einzelnes Wörterbuchwort, keinen Namen oder ein Datum. Verwenden Sie eine Mischung aus Zeichentypen (einschließlich Leerzeichen) und machen Sie Ihre Passwörter so lang wie möglich. Wenn Sie eine Vorlage für die Erstellung einprägsamer Kennwörter haben, ist diese nur dann sicher, wenn diese Regel von niemand anderem verwendet wird.

2. Verwenden Sie für jede Site ein eindeutiges Kennwort

Verwenden Sie für jede Seite ein anderes Passwort. Dies begrenzt den Schaden, der bei einer Sicherheitslücke verursacht werden kann.

Wenn Sie für alles dasselbe Passwort verwenden und jemand Ihr Facebook-Passwort in den Händen hält, hat er Ihr Passwort für jede Website, die Sie besuchen. Wenn Sie für jede Website ein anderes Passwort haben, besteht nur Zugriff auf Ihr Facebook-Konto, sodass zumindest alle Ihre anderen Konten geschützt sind.

3. Verwenden Sie zufällige Passwörter

Sie haben wahrscheinlich gehört, dass eine zufällige Phrase mit vier Wörtern sicherer und einprägsamer ist als komplizierte, aber kürzere Passwörter. Dies ist wahr, aber oft irrelevant, denn wie gesagt: Sie müssen für jedes Konto ein anderes Passwort verwenden. Wenn Sie

sich an 100 verschiedene Vierwort-Passwörter erinnern können, seien Sie unser Gast. Für die meisten von uns ist es jedoch unerheblich, wie

einfach es ist, sich Ihre Passwörter zu merken - es gibt einfach zu viele davon.

Die Verwendung einer Variation des gleichen Passworts für jede Seite ist ebenfalls keine gute Idee. Angenommen, Sie haben ein Passwort wie ro7CSfac2V3p1 für Facebook und Sie verwenden die Variante ro7CSlif2V3p1 für Google und so weiter für alle Ihre anderen Websites. Wenn ein Hacker Zugriff auf eines dieser Passwörter erhält, kann er die anderen leicht erraten, indem er "fac" durch die Buchstaben ersetzt, die möglicherweise mit anderen Sites übereinstimmen (oder herausfindet, was auch immer Ihr Algorithmus ist). Es ist schwieriger, aber keineswegs unmöglich, und es ist nicht sicher genug, um sich darauf zu verlassen. Wenn Sie sich daran erinnern können, kann es wahrscheinlich jemand anderes herausfinden.

Also: Die sicherste Option ist die Verwendung eines Passwortgenerators und -managers. Wenn Sie Ihre Konten schützen möchten, müssen Sie ein wirklich zufälliges, langes und komplexes Kennwort verwenden und für jedes Konto ein völlig anderes Kennwort verwenden.