

Thema: „1234567“ – Wo sind meine Daten geblieben?

Beitrag: 1:54 Minuten

Anmoderationsvorschlag: „Eins zwei drei vier fünf sechs sieben“, „eins zwei drei vier“, „eins zwei drei vier fünf sechs sieben acht neun“ – auch wenn sich das so anhört – NEIN, ich bin nicht verrückt geworden. Das sind Passwörter, die nicht nur unglaublich beliebt sind, sondern auch ungefähr genau so viel Schutz vor Online-Kriminellen bieten, als würde man gar keins verwenden. Tatsächlich haben wir – wie auch bei der Netzabdeckung – in Sachen Internet-Sicherheit noch ziemlichen Nachholbedarf. Wie's besser geht, verrät Ihnen jetzt zum Safer Internet Day (5. Februar) mein Kollege Oliver Heinze.

Sprecher: Damit ein Passwort sicher ist, sollte es vor allem eins sein: auf den ersten Blick unlogisch. Eine lange Zufallskombination aus Zahlen, Groß- und Kleinbuchstaben und auch Sonderzeichen eignet sich am besten, weiß Lena Heuermann von Google Deutschland.

O-Ton 1 (Lena Heuermann, 16 Sek.): „Das kann man sich immer ganz gut merken, wenn man eine Eselsbrücke baut und beispielsweise einen Satz sich merkt und die Anfangsbuchstaben da nur verwendet. Das wäre zum Beispiel ein sicheres Passwort. Das muss man natürlich auch regelmäßig ändern, damit es immer sicher bleibt, und ganz wichtig ist es, dass man für jedes Konto ein anderes Passwort hat.“

Sprecher: Genau dabei sind viele User allerdings zu nachlässig.

O-Ton 2 (Lena Heuermann, 23 Sek.): „Wir haben eine Umfrage zu dem Thema durchgeführt und jeder dritte Internetnutzer in Deutschland hat angegeben, ein und dasselbe Passwort für mehrere Konten oder sogar alle zu verwenden. Ich regle das so, dass ich einen Passwortmanager integriert habe. Beim Chrome Browser beispielsweise ist der direkt dabei. Und der kann dann für mich sichere Passwörter erstellen und aufbewahren und das kann ich auch synchronisieren. Also das heißt, ich kann dann nicht nur am Rechner auf diese Passwörter zurückgreifen, sondern natürlich dann auch auf dem Telefon.“

Sprecher: Noch sicherer wird ein Account, wenn für die Anmeldung zwei Schritte nötig sind.

O-Ton 3 (Lena Heuermann, 19 Sek.): „Das bedeutet, dass man zusätzlich zu Nutzernamen und Passwort eine weitere E-Mail-Adresse hinterlegt oder eine Telefonnummer, sodass ich beispielsweise einen Code per SMS zugestellt bekomme, den ich dann eingeben muss, um Zugriff auf mein Konto zu bekommen. Das heißt, jemand Fremdes, der auf mein Konto zugreifen möchte, braucht nicht nur mein Passwort, sondern auch diesen Code.“

Sprecher: Zusätzlich empfiehlt die Expertin einen regelmäßigen Check der Sicherheitseinstellungen.

O-Ton 4 (Lena Heuermann, 24 Sek.): „Das ist wichtig, dass man sieht: Habe ich Sicherheitslücken? Und kann ich diese schließen? Also, wir von Google beispielsweise haben den Google Sicherheitscheck, wo man Schritt für Schritt durch die wichtigsten Einstellungen durchgeführt wird und beispielsweise Optionen zur Kontowiederherstellung aufgezeigt bekommt. Diese Checks machen laut unserer Umfrage erschreckend Wenige – gerade mal ein knappes Viertel. Dabei ist das wirklich eine leichte Art und Weise, sein Konto sicher zu machen.“

Abmoderationsvorschlag: Sichere Passwörter und Passwortmanager, Zwei-Schritte-Authentifizierung und – nicht vergessen – Sicherheitscheck! Das sind die wichtigsten drei Tools, um die Konten im Netz sicherer zu machen. Alle Tipps und Infos dazu, und wie Sie sich sonst noch Betrüger, Hacker und Datendiebe vom Hals halten, finden Sie auch noch mal im Netz unter safety.google.

Thema: „1234567“ – Wo sind meine Daten geblieben?

Interview: 3:12 Minuten

Anmoderationsvorschlag: „Eins zwei drei vier fünf sechs sieben“, „eins zwei drei vier“, „eins zwei drei vier fünf sechs sieben acht neun“ – auch wenn sich das so anhört – NEIN, ich bin nicht verrückt geworden. Das sind Passwörter, die nicht nur unglaublich beliebt sind, sondern auch ungefähr genau so viel Schutz vor Online-Kriminellen bieten, als würde man gar keins verwenden. Tatsächlich haben wir – wie auch bei der Netzabdeckung – in Sachen Internet-Sicherheit noch ziemlichen Nachholbedarf. Wie's besser geht, verrät uns jetzt zum Safer Internet Day (5. Februar) Lena Heuermann von Google Deutschland. Hallo!

Begrüßung: „Hallo!“

1. *Frau Heuermann, simple Passwörter kann man sich leicht merken, sind aber eben auch leicht zu knacken. Wann gilt ein Passwort denn als sicher?*

O-Ton 1 (Lena Heuermann, 35 Sek.): „Also am wichtigsten ist es eigentlich, dass man keine normalen Wörter, keine Zahlen, die auf einen zurückzuführen sind, benutzt. Also das heißt: Zum Beispiel den Vor- und den Nachnamen und das Geburtsdatum wäre kein sicheres Passwort. Am besten ist es, wenn man eine Kombination wählt aus Zahlen, Groß- und Kleinbuchstaben und beispielsweise Sonderzeichen noch hinzufügt. Das kann man sich immer ganz gut merken, wenn man eine Eselsbrücke baut und beispielsweise einen Satz sich merkt und die Anfangsbuchstaben da nur verwendet. Das wäre zum Beispiel ein sicheres Passwort. Das muss man natürlich auch regelmäßig ändern, damit es immer sicher bleibt, und ganz wichtig ist es, dass man für jedes Konto ein anderes Passwort hat.“

2. *Aber genau da hört's ja bei den meisten auf: Wer kann sich denn so viele und dann auch noch schwierige Passwörter merken?*

O-Ton 2 (Lena Heuermann, 44 Sek.): „Ja, das ist in der Tat ein Problem, weil viele bequem und sorglos damit umgehen. Wir haben eine Umfrage zu dem Thema durchgeführt und jeder dritte Internetnutzer in Deutschland hat angegeben, ein und dasselbe Passwort für mehrere Konten oder sogar alle zu verwenden. Ich kenne das selbst: Also es vergeht kaum ein Tag, wo man nicht ein neues Konto eröffnet, sei es, um einen Flug zu buchen oder um online zu shoppen, braucht man immer wieder neue Passwörter und die kann man sich in der Tat nicht alle merken. Ich regle das so, dass ich einen Passwortmanager integriert habe. Beim Chrome Browser beispielsweise ist der direkt dabei. Und der kann dann für mich sichere Passwörter erstellen und aufbewahren und das kann ich auch synchronisieren. Also das heißt, ich kann dann nicht nur am Rechner auf diese Passwörter zurückgreifen, sondern natürlich dann auch auf dem Telefon.“

3. *Welche Möglichkeiten gibt es noch, das Online-Konto zu sichern?*

O-Ton 3 (Lena Heuermann, 34 Sek.): „Am besten kann man sein Konto schützen, indem man eine Anmeldung über zwei Schritte hinzufügt. Das bedeutet, dass man zusätzlich zu Nutzernamen und Passwort eine weitere E-Mail-Adresse hinterlegt oder eine Telefonnummer, sodass ich beispielsweise einen Code per SMS zugestellt bekomme, den ich dann eingeben muss, um Zugriff auf mein Konto zu bekommen. Das heißt, jemand Fremdes, der auf mein Konto zugreifen möchte, braucht nicht nur mein Passwort, sondern auch diesen Code. Das ist gängige Praxis beispielsweise im Online Banking. Da kennt man das mit dem TAN-Verfahren. Aber bei E-Mailkonten und sozialen Netzwerken ist das noch nicht der Fall, würde aber die Konten sehr viel sicherer machen.“

4. *Passwörter sind das eine. Wie kann man den Hackern das Leben außerdem noch schwerer machen?*

O-Ton 4 (Lena Heuermann, 30 Sek.): „Ganz wichtig ist, dass man immer wieder seine Sicherheitseinstellungen überprüft, egal für welches Konto. Das ist wichtig, dass man sieht: Habe ich Sicherheitslücken? Und kann ich diese schließen? Also, wir von Google beispielsweise haben den Google Sicherheitscheck, wo man Schritt für Schritt durch die wichtigsten Einstellungen durchgeführt wird und beispielsweise Optionen zur Kontowiederherstellung aufgezeigt bekommt. Diese Checks machen laut unserer Umfrage erschreckend Wenige – gerade mal ein knappes Viertel. Dabei ist das wirklich eine leichte Art und Weise, sein Konto sicher zu machen.“

5. *Nun gibt's ja auch viele, die das Internet zwar nutzen, sich mit den ganzen Einstellungen aber nicht wirklich auskennen und denken, dass das alles sowieso viel zu kompliziert ist...*

O-Ton 5 (Lena Heuermann, 32 Sek.): „Da haben Sie vollkommen recht. Das ist in der Tat ein großes Problem, dass viele Nutzer sagen: ‚Ich habe nicht wahnsinnig viel Ahnung von Technik und bevor ich irgendwas falsch mache, mache ich lieber gar nichts.‘ Deswegen versuchen wir, diesen Nutzern so einfache Tools wie möglich an die Hand zu geben. Im Prinzip muss man sich drei Dinge merken: Zum einen sichere Passwörter – da hilft der Passwortmanager. Zum anderen die Zwei-Schritte-Authentifizierung – das heißt, entweder eine weitere E-Mailadresse oder Telefonnummer hinterlegen und, ganz sicher, die Sicherheitseinstellungen immer mal wieder überprüfen und schauen, ob man da alles richtig eingestellt hat.“

Lena Heuermann von Google Deutschland über sicherere Passwörter und noch mehr Möglichkeiten, Cyber-Kriminellen das Leben schwer zu machen. Vielen Dank für das Gespräch!

Verabschiedung: „Ich danke Ihnen!“

Abmoderationsvorschlag: Sichere Passwörter und Passwortmanager, Zwei-Schritte-Authentifizierung und – nicht vergessen – Sicherheitscheck! Das sind die wichtigsten drei Tools, um die Konten im Netz sicherer zu machen. Alle Tipps und Infos dazu, und wie Sie sich sonst noch Betrüger, Hacker und Datendiebe vom Hals halten, finden Sie auch noch mal im Netz unter safety.google.