LastPass ••• | by LogMeIn

Psychologie der Passwörter: Ihr Online-Verhalten – sicher oder riskant?

Arbeiten, einkaufen, Sozialkontakte pflegen: Immer mehr Menschen tun dies ausschließlich online. Das ruft immer mehr Hacker mit kriminellen Absichten auf den Plan. Unsere bei 500 Personen in Deutschland durchgeführte Umfrage zum Online-Verhalten zeigt: Alle wissen, dass man sich vor Sicherheitsrisiken schützen soll, doch sie handeln nicht danach. Und Sie? Wie sicher oder riskant ist Ihr Online-Verhalten?

Sechs Verhaltensweisen, die uns zum Ziel von Hackern machen

1 Wir verwenden für alles dasselbe Passwort

Hat ein Hacker dieses Passwort geknackt, hat er überall freie Bahn.

94 % wissen, dass es riskant ist, dasselbe Passwort immer wieder oder in Varianten zu verwenden

50 % tun aber genau das!

2 Wir möchten alles unter Kontrolle haben

Ein Passwort für alles – das gibt uns ein Gefühl der Sicherheit. In Wirklichkeit jedoch ist das gefährlich. Gefragt nach dem Grund für die Wiederverwendung von Passwörtern sagen die Befragten:

42 % Ich habe Angst davor, meine Zugangsdaten zu vergessen

58 % Ich möchte alle meine Passwörter im Kopf haben

3 Wir merken uns Passwörter oder schreiben sie auf

Wer kann sich schon starke, einmalige Passwörter für seine ganzen Konten merken? Höchstens ein Superhirn! Verlassen Sie sich besser nicht auf Ihr Gedächtnis, wenn es um Online-Sicherheit geht.

55 % versuchen, sich Passwörter zu merken

Anscheinend mit nur mäßigem Erfolg:

12 % setzen ihre Passwörter mindestens einmal pro Monat zurück, weil sie sie vergessen haben

4 Bekannte Datenlecks sind uns egal

Wenn ein Anbieter, bei dem Sie ein Konto haben, gehackt wurde, sollten Sie Ihr Passwort ändern.

66 % haben in den letzten 12 Monaten keine Passwörter geändert – auch nicht nach Bekanntwerden eines Datenlecks.

5 Wir unterschätzen unser Risiko

Ich bin doch für Hacker kein lohnendes Ziel, oder? Doch! Eine einzige Kreditkartennummer bringt dem Hacker vielleicht nur 5 Euro im Dark Web[1], erbeutet er aber hunderttausende Daten auf einmal, dann läppert es sich.

51 % halten ihre Konten für nicht wertvoll genug, um gehackt zu werden

6 Wir sind berechenbar

Hacker kommen mühelos an persönliche Informationen über uns – ein Blick in unsere Social-Media-Accounts oder eine kurze Internetrecherche genügen.

15 % können das Passwort ihres Lebenspartners erraten

16 % verwenden Kosenamen und Ähnliches als Passwort

Gibt es auch etwas, das wir *gut* machen?

Wir verwenden Multifaktor-Authentifizierung!

45 % nutzen MFA für private Konten

Aber nur 21 % nutzen MFA für Konten bei der Arbeit

Wir vertrauen der Biometrie:

54 % vertrauen der Fingerabdrucks- oder Gesichtserkennung mehr als herkömmlichen Passwörtern

Was ist MFA?

Mit MFA führen Sie eine zusätzliche Sicherheitsebene ein. Von Benutzername und Passwort abgesehen verlangt MFA beim Login eine weitere Information – einen Einmalcode oder Ihren Fingerabdruck.

Wir schützen unser Online-Banking und E-Mail besser als andere Konten

66 % erstellen ein starkes Passwort für das Online-Banking und 51 % für E-Mail

59 % verwenden Multifaktor-Authentifizierung beim Online-Banking und 42 % bei E-Mail

LastPass ••• | by LogMeIn

Wir können noch viel mehr für unsere Online-Sicherheit tun. Doch was macht sicheres Verhalten aus? Wie können Sie Ihr digitales Leben besser schützen? In unserem E-Book „Psychologie der Passwörter" erfahren Sie es. www.lastpass.com

Quellen:
1. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

04.20.2020/PDF/LMI1249