

Datendiebstahl: Tipps gegen Betrug im Netz

- Leichtsinniger Mut zur Lücke: 61 Prozent der Menschen in Deutschland attestieren sich höchstens „befriedigende“ Kenntnisse und Fähigkeiten in Bezug auf die persönliche Datensicherheit im Internet. Über die Hälfte nutzt dasselbe Passwort für mehrere Accounts.
- CosmosDirekt gibt Tipps von der Passwörterstellung über das Verhalten im Internet-Betrugsfall bis zum passenden Versicherungsschutz.







Fotoquelle: CosmosDirekt/Adobe Stock

Saarbrücken – Wie schütze ich eigentlich meine persönlichen Daten? Was macht ein gutes Passwort aus und wie reagiere ich, wenn es entwendet wird? CosmosDirekt, der Direktversicherer der Generali in Deutschland, gibt Tipps und erklärt, wie man sich gegen Schäden durch Internetbetrug absichern kann.

Pressekontakt

Jörg Linder, Head of Media Relations, T +49 (0) 241 456 5664
Sabine Gemballa, Media Relations CosmosDirekt, T +49 (0) 681 966 7560

presse.de@generali.com

 CosmosDirekt
 @CosmosDirekt
 Generali Deutschland AG
 @GeneraliDE

www.cosmosdirekt.de
www.generali.de

Generali Deutschland AG
Adenauerring 7
D-81737 München

WORAUF MUSS ICH FÜR EIN SICHERES PASSWORT ACHTEN?

„Passwort-Diebstahl? Das wird mich schon nicht treffen!“ Aber was, wenn doch? Ist das Passwort zu einem Internet-Account geknackt, haben Online-Diebe leichtes Spiel und können unter Umständen auf Kosten des Opfers im Internet bestellen, Verträge schließen, Nachrichten verschicken oder Profile verändern. Zum eigenen Schutz sind daher starke Passwörter das A und O. Dass hier jedoch noch Wissenslücken bestehen, zeigt eine aktuelle forsa-Umfrage¹ im Auftrag von CosmosDirekt. So bewerten 61 Prozent Menschen in Deutschland ihre Kenntnisse und Fähigkeiten in Bezug auf die Sicherheit ihrer persönlichen Daten im Internet höchstens mit der Schulnote 3 – „befriedigend“. Über die Hälfte (56 Prozent) nutzt dasselbe Passwort für mehr als einen Account. Und 23 Prozent haben schon einmal das Geburtsdatum oder den Geburtsort als Bestandteil eines Passworts verwendet. Solche personenbezogenen Passwörter stellen ein ebenso hohes Sicherheitsrisiko dar wie einfache Zahlenfolgen oder Buchstabenkombinationen in alphabetischer Reihenfolge, da sie leichter zu entschlüsseln sind. Für ein sicheres Passwort helfen fünf Tipps:

1. Für jeden Account ein eigenes Passwort verwenden.
2. Je länger, desto sicherer das Passwort: Dabei hat man die Wahl zwischen kurzen und komplexen Passwörtern – mindestens acht bis zwölf Zeichen und mindestens vier verschiedenen Zeichenarten (z. B. C_D1!#23krB%) – oder langen und weniger komplexen Passwörtern – mindestens 25 Zeichen und zwei Zeichenarten (z. B. versicherung_sonne_familie_blau_sport).
3. Möglichst viele verschiedene Zeichen nutzen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).²
4. Eine Zwei-Faktor-Authentifizierung, also eine zusätzliche Bestätigung des Anmeldeversuchs, als Ergänzung zum Passwort einrichten. Wichtig ist, dass die Faktoren aus verschiedenen Kategorien stammen (z. B. über einen Biometrie-Faktor wie die Gesichtserkennung, einen Wissens-Faktor, wie die Bestätigung mithilfe eines PINs oder einen Besitz-Faktor wie einen TAN-Generator).³
5. Zugangsdaten in einem Passwortmanager sichern. Dabei handelt es sich um ein Programm, das die Passwörter und Benutzernamen verwaltet und die Zugangsdaten durch eine Verschlüsselung und ein komplexes Masterpasswort sichert. So muss man sich nur ein sehr starkes Passwort für dessen Zugang merken.⁴

WAS KANN ICH TUN, WENN ICH OPFER VON INTERNETKRIMINALITÄT WURDE?

Trotz sicherer Passwörter ist man vor Betrug im Internet nicht immer gefeit. Landen auf einmal Rechnungen und Mahnungen von Online-Shops im Briefkasten, obwohl man gar nichts bestellt hatte, ist man höchstwahrscheinlich Opfer eines Online-Betrügers. In diesem Fall ist schnelles Handeln wichtig:

1. Die eigene Bank schnellstmöglich informieren und betroffene Konten und Karten sperren lassen. Falls möglich, sollten unberechtigte Transaktionen umgehend zurückgebucht werden.
2. Strafanzeige bei der Polizei stellen.
3. Die zuständige Versicherung informieren.
4. Passwörter der betroffenen Accounts ändern und Smartphone, Laptop, Tablet und Co. auf installierte Schadsoftware prüfen.
5. Identitätsmissbrauch der Schufa und anderen Auskunfteien melden und auf Zahlungsaufforderungen reagieren: Damit es nicht zu einem unberechtigten Schufa-Eintrag aufgrund des Identitätsdiebstahls kommt, sollte der Vertragsschluss schriftlich bestritten werden und gegen Mahnbescheide innerhalb von 14 Tagen Widerspruch eingelegt werden.⁵

GESCHÜTZT, WENN'S DRAUF ANKOMMT

„Neben dem psychischen Stress durch einen Betrugsfall, kann dieser zusätzlich finanzielle Folgen nach sich ziehen“, weiß **Sandra Kniesigk, Versicherungsexpertin bei CosmosDirekt**, und rät: „Gegen finanzielle Schäden durch den Missbrauch der persönlichen Daten im Internet kann man sich absichern, beispielsweise mit einer Hausratversicherung. Denn viele Anbieter decken auch Schäden durch Missbrauch bei Online-Banking und - Shopping, Phishing oder Kredit- und Bankkarten ab. Im Zweifelsfall sollte für den besten Schutz der bestehende Versicherungsumfang geprüft und ggf. erweitert werden.“

¹ Repräsentative Befragung „Passwortschutz“ des Meinungsforschungsinstituts forsa im Auftrag von CosmosDirekt, dem Direktversicherer der Generali in Deutschland. Im April 2023 wurden in Deutschland 1.027 Bürgerinnen und Bürger ab 18 Jahren befragt. Die Fehlertoleranz der ermittelten Ergebnisse liegt bei +/- 3 Prozentpunkten.

² Quelle: Bundesamt für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

³ Quelle: Bundesamt für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

⁴ Quelle: Bundesamt für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html

⁵ Quelle: Verbraucherzentrale Hamburg e. V.:

<https://www.vzhh.de/themen/einkauf-reise-freizeit/online-shopping/identitaet-geklaut-das-sollten-sie-jetzt-tun>

COSMOSDIREKT

CosmosDirekt ist Deutschlands führender Online-Versicherer und der Direktversicherer der Generali in Deutschland. Mit einfachen und flexiblen Online-Angeboten und kompetenter persönlicher Beratung rund um die Uhr setzt das Unternehmen neue Maßstäbe in der Versicherungsbranche. Zum Angebot zählen private Absicherung, Vorsorge und Geldanlage. Rund 1,7 Millionen Kunden vertrauen auf CosmosDirekt.

GENERALI IN DEUTSCHLAND

Die Generali ist eine der führenden Erstversicherungsgruppen im deutschen Markt mit Beitragseinnahmen von rund 14,9 Mrd. € und mehr als 9 Mio. Kunden. Als Teil der internationalen Generali Group ist die Generali in Deutschland mit den Marken Generali, CosmosDirekt und Dialog in den Segmenten Leben, Kranken und Schaden/Unfall tätig. Ziel der Generali ist es, für ihre Kunden ein lebenslanger Partner zu sein, der dank eines hervorragenden Vertriebsnetzes im Exklusiv- und Direktvertrieb sowie im Maklerkanal innovative, individuelle Lösungen und Dienstleistungen anbietet. Generali Deutschland gehört zu der im Jahr 2022 neu geschaffenen Business Unit „Deutschland, Österreich und Schweiz“ (DACH). Mit rund 19,6 Mrd. € Beitragseinnahmen und 12,2 Mio. Kunden ist die neue Business Unit der Generali Group eine der führenden Erstversicherungsgruppen in Deutschland, Österreich und der Schweiz.

Die Sicherheit Ihrer persönlichen Daten ist uns sehr wichtig. Bitte teilen Sie uns mit, wenn Sie keine weiteren Informationen mehr von uns wünschen. Wir werden Ihre Daten dann aus unserem Verteiler löschen.