# Wenn das „digitale Ich“ entwendet wird: Jeder Dritte hat Erfahrungen mit Identitätsdiebstahl

**Berlin/Bonn/Hamburg/Stuttgart, 27. März 2024 – Mehr als ein Drittel der Menschen hierzulande hat bereits Erfahrungen mit dem Diebstahl von Online-Konten und der eigenen digitalen Identität gemacht. Dennoch agieren insbesondere junge Menschen im Internet noch immer sorglos. Und das, obwohl die Gefahr, Opfer eines digitalen Identitätsdiebstahls zu werden, nicht zuletzt durch Künstliche Intelligenz zunimmt. Dabei sind viele wirksame Schutzmaßnahmen vor der perfiden Betrugsmasche einfach umzusetzen. Die Initiative Sicher Handeln (ISH) klärt auf.**

Kriminelle, die im Namen und Erscheinungsbild anderer im Internet ihr Unwesen treiben: Was für viele eine Horrorvorstellung ist, haben mehr als ein Drittel der Menschen in Deutschland bereits erfahren müssen – entweder am eigenen Leib oder im Umfeld. Das hat eine repräsentative Umfrage des Meinungsforschungsinstituts YouGov im Auftrag der Initiative Sicher Handeln (ISH) ergeben. Demnach ist bereits jeder zehnte Befragte (11 %) Opfer von Identitätsdiebstahl im Netz geworden. Fast jeder Fünfte, der selbst bisher verschont geblieben ist, kennt aber einen (14 %) oder gar mehrere Menschen (5 %), die Opfer wurden. Fünf Prozent haben beides erlebt, sind also selbst Opfer geworden und kennen weitere Opfer.

Dass der Anteil der Betroffenen so groß ist, kommt nicht von ungefähr: Die Gefahr, Opfer eines digitalen Identitätsdiebstahls zu werden, nimmt zu. Das Hasso-Plattner-Institut (HPI) hat 2021 fast 185 Millionen kompromittierte Nutzerkonten gezählt. Allein im Januar dieses Jahres waren es bereits mehr als 46 Millionen. Auf das Jahr gerechnet könnte sich die Zahl der fingierten Profile im Vergleich zu 2021 damit fast verdreifachen. Auch, weil Künstliche Intelligenz diese Form der Cyberkriminalität nicht nur einfacher, sondern auch skalierbar macht: „Mittels KI könnten Kriminelle ihren Betrug noch einfacher und schneller automatisieren und so zahllose Taten gleichzeitig begehen. Ein enormer Effizienzgewinn“, sagt Harald Schmidt von der Stiftung Deutsches Forum für Kriminalprävention und Sprecher der Initiative Sicher Handeln.

## Streaming, Dating, Online-Handel: Kaufen auf fremde Kosten

Identitätsdiebstahl ist eine besonders perfide Betrugsmasche. Kriminelle nutzen dabei Daten wie den Namen, das Geburtsdatum, die Anschrift oder Kreditkarten- oder Kontonummern ihrer Opfer, um sich mithilfe dieser Daten Nutzerkonten bei Online-Diensten anzulegen und auf fremde Kosten einzukaufen oder Verträge abzuschließen. Die Opfer bekommen das meistens erst mit, wenn es zu spät ist und die Überweisungen auf dem Konto verbucht sind oder Rechnungen eintrudeln.

Es gibt zahlreiche Anwendungsfälle, um mit fremden Identitäten Geschäfte zu machen. Aktuell nimmt die Bedeutung von Identitätsdiebstahl, beispielsweise auf dem Wohnungsmarkt, zu. Kriminelle erstellen hierbei mithilfe gestohlener Nutzerdaten Wohnungsinserate. Sie gewinnen damit das Vertrauen von Wohnungssuchenden, die ihnen wiederum ihre Daten preisgeben oder Zahlungen leisten. Bisweilen nutzen Betrüger die gewonnenen Daten (bspw. Scans von Ausweisen) auch für andere Betrügereien und vielfach gehen sie dabei arbeitsteilig vor.

Geld spielt auch beim sogenannten Money Muling eine Rolle. Dabei bringen Kriminelle ergaunertes Geld über Konten argloser Internetnutzer wieder in Umlauf. Die Opfer, die zu Mittätern werden, glauben, im Dienste seriöser Unternehmen zu handeln – eine Form der Geldwäsche. Noch einen Schritt weiter geht der sogenannte Account Takeover: Dabei wird kein neues Konto angelegt, sondern ein vorhandenes übernommen. Hacker ergaunern dafür die Zugangsdaten und treiben im Namen ihrer Opfer ihr Unwesen, etwa durch Phishing.

**Generation sorglos: Jüngere sind weniger vorsichtig als Ältere**

Obwohl die Gefahr steigt, nehmen viele das Thema offensichtlich noch immer auf die leichte Schulter. Die aktuelle Umfrage der Initiative Sicher Handeln zeigt: Insbesondere die junge Generation tut sich als besonders sorglos hervor. So sagt jeder dritte 18- bis 24-Jährige, für mehrere Nutzerkonten im Netz dasselbe Passwort zu verwenden. Im Schnitt handelt gerade einmal jeder Fünfte (22 %) so. Zudem geben 16 Prozent der jungen Erwachsenen an, bereits eine Kopie ihres Personalausweises über das Internet mit einer fremden Person geteilt zu haben. Innerhalb der gesamten Stichprobe trifft das nur auf elf Prozent der Befragten zu.

Auch beim Thema Sicherheitsmaßnahmen gehen ältere Befragte deutlich gewissenhafter zu Werke als die jüngste Generation. So geben rund 70 Prozent der Über-55-Jährigen an, regelmäßig ihre Kontoauszüge zu prüfen. Von den 18- bis 24-Jährigen machen das gerade einmal vier von zehn (39 %). Auch im Umgang mit E-Mails gibt sich die älteste Gruppe (66 %) deutlich vorsichtiger als die jüngste (38 %). Aktuelle Sicherheitssoftware hat nicht einmal jeder vierte 18- bis 24-Jährige (24 %) installiert. Bei Über-55-Jährigen ist es knapp die Hälfte (47 %) – also gut doppelt so viele.

„Unsere Umfrage zeigt, dass viele Internetnutzer bereits Erfahrung mit dem Diebstahl digitaler Identitäten gemacht, aber offenbar wenig daraus gelernt haben. Anders lässt es sich nicht erklären, weshalb so viele Befragte noch immer ein und dasselbe Passwort für mehrere Accounts nutzen oder sorglos Kopien wichtiger Dokumente wie Zahlungskarten oder Personalausweise übers Internet an Fremde versenden“, so Harald Schmidt. „Für unsere Initiative leiten wir daraus den klaren Auftrag ab, weiter über die Risiken, die

durch Cyberkriminalität entstehen, aufzuklären und Tipps zu geben, wie man ihnen im Netz begegnen sollte.“

**Mit der SHS-Regel zu mehr Sicherheit im Netz**

Neben diesen gängigen Maßnahmen gibt es viele weitere Tipps, um sich vor Betrug im Netz zu schützen. Um sich Passwörter besser merken zu können, sind Passwortmanager eine gute und sichere Option. Eine von immer mehr Diensten angebotene Zwei-Faktor-Authentifizierung von Konten hebt zudem den Schutz beim Anmelden auf eine neue Stufe. Dabei wird neben dem Passwort auch ein Code verlangt, der an eine hinterlegte Mobilnummer oder Authentifizierungs-App geteilt wird. Erst mit Eingabe dieses Codes ist der Login erfolgreich. Auch ist es hilfreich, Profile in öffentlichen Netzwerken auf „privat“ zu stellen, sodass sie nur von Freunden oder Kontakten eingesehen werden können. Je weniger Informationen preisgegeben werden, desto geringer ist das Risiko, dass diese missbraucht werden.

Darüber hinaus empfiehlt die Initiative Sicher Handeln zum Schutz vor Internetkriminalität ihre SHS-Regel: Stoppen, Hinterfragen, Schützen. Stoppen heißt, bei Auffälligkeiten kurz innezuhalten und das Risiko der geforderten Aktion, etwa ein Klick auf einen Link, abzuwägen. Zudem sollten Nutzer das Verhalten des Gegenübers hinterfragen und nicht ohne weiteres hinnehmen, gerade wenn Zeitdruck suggeriert wird. Allgemein gilt zudem: Wenn etwas zu gut scheint, um wahr zu sein – ist es das sehr wahrscheinlich eben nicht! Und Schützen bezieht sich am Ende nicht nur auf den eigenen, sondern auch auf den Schutz anderer: Wenn eine Aktion verdächtig erscheint, soll sie dem Plattformbetreiber gemeldet werden. Außerdem sollten Menschen im Familien- und Bekanntenkreis über ihre Erfahrungen sprechen.

**Über die Initiative Sicher Handeln**

Sicher Handeln ist eine gemeinsame Initiative der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK), der Stiftung Deutsches Forum für Kriminalprävention (DFK), Deutschland sicher im Netz e. V. (DsiN), RISK IDENT und Kleinanzeigen, die 2023 ins Leben gerufen wurde. Mit dem Ziel, der wachsenden digitalen Kriminalität entgegenzuwirken, setzt sich die Initiative für mehr Aufklärung beim Thema Online-Betrug ein. Ziel ist die Vermittlung digitaler Basiskompetenzen – unter anderem mit der „SHS-Regel“ (Stoppen, Hinterfragen, Schützen). Weitere Informationen unter www.stark-gegen-betrug.de.

**Kontakt**

Pierre Du Bois, Head of Communications bei *Kleinanzeigen*

E-Mail: medien@kleinanzeigen.de