IDENTITÄTSDIEBSTAHL: CHECKLISTE FÜR DEN ERNSTFALL

Beim Identitätsdiebstahl geben sich Täterinnen und Täter als eine andere Person aus. Online verwenden sie dafür meist persönliche Daten ihres Opfers, etwa Name, Adresse, Zugangsdaten oder Kontoinformationen. Sie geben dann z. B. Bestellungen auf, schließen Verträge ab, übernehmen die Kontrolle über bestehende Benutzerkonten oder nehmen Kontakt zu Angehörigen ihres Opfers auf.

Identitätsdiebstahl bleibt häufig zunächst unbemerkt. Die Folgen können jedoch erheblich sein. Mitunter erfahren Opfer erst von ihrer Betroffenheit, wenn Täterinnen und Täter z. B. illegale Waren unter dem Namen ihres Opfers im Internet verkaufen und bei strafrechtlicher Verfolgung die Spur zum Opfer des Identitätsdiebstahls statt zu den eigentlichen Täterinnen und Tätern führt.

SO ERKENNEN SIE IDENTITÄTSDIEBSTAHL

Konto-Anmeldungen, Abbuchungen und Bestellungen, die Sie nicht selbst vorgenommen haben, sowie veränderte Profil-Einstellungen können darauf hindeuten, dass Täterinnen und Täter sich Zugang zu einem Ihrer Benutzerkonten verschafft haben. Werden Sie auch hellhörig, wenn Bekannte Nachrichten erhalten, die Sie nicht selbst verschickt haben, oder auf Social-Media-Profilen unter Ihrem Namen Inhalte veröffentlicht werden, die nicht von Ihnen stammen.

Gut zu wissen: In einigen Fällen übernehmen Täterinnen und Täter ein Benutzerkonto des Opfers – etwa eine E-Mail-Adresse. In anderen Fällen erstellen sie neue Benutzerkonten. Damit diese vertrauenswürdig erscheinen, nutzen Täterinnen und Täter u. a. frei verfügbare Bilder, etwa aus Social-Media-Posts, oder auch aus einem Datenleck stammende Inhalte, z. B. Ausweiskopien. Um an weitere Daten des Opfers zu gelangen, setzen sie auch Phishing-Mails oder Schadprogramme ein.

DAS SOLLTEN SIE TUN, WENN…

… Ihre Zugangsdaten unberechtigt von Täterinnen oder Tätern genutzt werden:

- ✓ Ändern Sie umgehend das Passwort des betroffenen Benutzerkontos.
- ✓ Ändern Sie auch Passwörter bei anderen Benutzerkonten, wenn Sie dort dasselbe Passwort verwendet haben oder die Profile miteinander verknüpft sind. Das ist etwa der Fall, wenn eine E-Mail-Adresse gehackt wurde, die auch in einem anderen Benutzerkonto hinterlegt ist.
- ✓ Überprüfen Sie die Profil-Einstellungen, z. B. hinterlegte E-Mail-Adressen, Telefonnummern oder verbundene Geräte. Mitunter ändern Täterinnen und Täter diese ab.
- ✓ Melden Sie sich bei allen aktiven Sitzungen ab und entfernen Sie unbekannte Zugriffe. Dies ist meist mit einem Klick in den Profil-Einstellungen möglich.
- ✓ Informieren Sie den Diensteanbieter, z. B. die Social-Media-Plattform, über den Vorfall.

HINWEIS

Werden bei einem Virenscan Schadprogramme festgestellt, müssen diese beseitigt werden, bevor Sie weitere Maßnahmen ergreifen. Dabei hilft Ihnen die Checkliste für den Ernstfall: Infektion mit Schadprogrammen.

HINWEIS

Sie können sich nicht mehr in Ihr Benutzerkonto einloggen? Möglicherweise haben Täterinnen und Täter bereits die Zugangsdaten geändert. Bitten Sie daher umgehend den Diensteanbieter um Unterstützung.

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

... in Ihrem Namen Bestellungen oder Verträge abgeschlossen wurden:

- ✓ Nehmen Sie Kontakt zum Anbieter, Verkäufer oder Shop auf und schildern Sie den Vorfall.
- ✓ Widersprechen Sie unberechtigten Forderungen und verlangen Sie eine Sperrung des Benutzerkontos oder eine Stornierung der Bestellung.
- ✓ Prüfen Sie Ihre Kontoauszüge und lassen Sie unberechtigte Abbuchungen umgehend klären.
- ✓ Informieren Sie auch Ihre Bank oder Ihren Zahlungsdienstleister über den Missbrauch.
- ✓ Sichern Sie alle Unterlagen, Bestellbestätigungen oder Mahnungen als Beweismaterial.

...Sie verdächtige Vorgänge beim Onlinebanking oder bei Zahlungsdienstleistern feststellen:

- ✓ Informieren Sie Ihre Bank oder den jeweiligen Zahlungsdienstleister. Lassen Sie Karten, Konten oder Zugänge sperren, wenn Anzeichen für Missbrauch vorliegen.
- ✓ Prüfen Sie Ihre letzten Transaktionen genau und melden Sie unberechtigte Buchungen.
- ✓ Ändern Sie die Zugangsdaten zu den (möglicherweise) betroffenen Benutzerkonten.
- ✓ Erstatten Sie Anzeige – insbesondere wenn ein finanzieller Schaden entstanden ist.

... jemand sich in E-Mails oder in einem Social-Media-Profil als Sie ausgibt:

- ✓ Melden Sie das betroffene Profil bei dem E-Mail-Anbieter oder dem Betreiber der Social-Media-Plattform und bitten Sie um Prüfung und Löschung.
- ✓ Ändern Sie die Zugangsdaten und kontrollieren Sie, ob Ihre Benutzerkonten ausreichend abgesichert sind – etwa mit einem starken Passwort und einer Zwei-Faktor-Authentisierung oder mit einer passwortlosen Alternative wie Passkeys.
- ✓ Informieren Sie Ihr Umfeld, damit dieses nicht auf mögliche Nachrichten oder Kontaktaufnahmen hereinfällt.
- ✓ Dokumentieren Sie den Vorfall durch Screenshots oder Links. Tipps für rechtssichere Screenshots finden Sie auf **www.polizei-beratung.de**.
- ✓ Wenn Ihnen persönlicher Schaden entstanden ist, wenden Sie sich an die Polizei, um Anzeige zu erstatten.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR IDENTITÄTSDIEBSTAHL

- › Nutzen Sie für jeden Dienst ein eigenes, starkes Passwort in Kombination mit der Zwei-Faktor-Authentisierung oder alternativ Passkeys als passwortlose Alternative. Wenn Sie viele Passwörter zu verwalten haben, kann ein Passwortmanager helfen.
- › Gehen Sie sparsam mit persönlichen Daten um. Das betrifft u. a. Veröffentlichungen auf Social-Media-Profilen oder auch Angaben in Onlineshops. Legen Sie in den Privatsphäre-Einstellungen Ihrer Benutzerkonten fest, wer Ihre Inhalte sehen kann. Verwenden Sie eine E-Mail-Adresse für wichtige Kommunikation und eine andere für z. B. Gewinnspiele, Newsletter und soziale Netzwerke. Manche E-Mail-Anbieter ermöglichen es auch, mehrere Adressen innerhalb eines E-Mail-Postfachs zu erstellen.
- › Öffnen Sie keine Links oder Anhänge aus unbekannten oder verdächtigen Nachrichten.
- › Prüfen Sie regelmäßig Ihre Kontoauszüge und die Einstellungen Ihrer Benutzerkonten.
- › Nutzen Sie einen VPN, falls Sie sehr sensible Vorgänge, etwa Onlinebanking, über ein öffentliches Netzwerk durchführen möchten.
- › Installieren Sie zeitnah zur Verfügung stehende Sicherheitsupdates.

Mehr Informationen rund um Cybersicherheit:
www.bsi.bund.de/VerbraucherInnen

Mehr Informationen für Opfer von Internetkriminalität:
www.polizei-beratung.de/cybercrime

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei