IDENTITÄTSDIEBSTAHL – WAS IST DAS UND WAS KANN ICH TUN?

- Kriminelle nutzen gestohlene Daten, um im Netz damit einzukaufen, Verträge auf Kosten ihrer Opfer zu schließen oder sie gegen Geld weiter zu verkaufen.
- Vorsicht: An persönliche Daten können Kriminelle nicht nur durch Ausnutzen von Sicherheitslücken auf Anbieter-Servern oder auf dem Smartphone kommen, sondern häufig auch, indem sie Menschen zur Herausgabe von Daten manipulieren (sog. Social-Engineering).
- Wer betroffen ist, sollte schnell handeln.

DAS SIND DIE FAKTEN:

- Bei einem Identitätsdiebstahl nutzt ein kriminell handelnder Dritter die Identität einer anderen Person missbräuchlich zu seinem persönlichen Vorteil. Hierzu bedienen sich Kriminelle meist einem Set an Daten der betroffenen Person wie Name, Anschrift, E-Mail-Adresse, Geburtsdatum, Kreditkarten- und Kontonummer oder Passwörter / Zugangsdaten zu Online-Accounts.
- Cyberkriminelle missbrauchen diese Daten, um Geschäfte im Internet auf Kosten der betroffenen Personen abzuschließen, z.B.:
  - Abschließen von Online-Verträgen für Abos (z.B. Mobilfunk, kostenpflichtiges Streaming, Online-Marktplatz, Online-Dating, Gaming).
  - Bestellen von Waren und kostenpflichtigen Dienstleistungen (z.B. Hörbücher, Software).
  - Überweisungen und Abbuchungen von fremden Konten.
  - Verkauf der entwendeten Daten auf Schwarzmärkten im Internet (sog. Darknet).
- Es gibt viele Wege, über die Kriminelle an Ihre Daten kommen können, u.a.:
  - Phishing / Smishing: Versuch, mit präparierten E-Mails oder SMS den Empfänger dazu zu bringen, auf Links oder Anhänge in einer Nachricht zu klicken, um Schadsoftware auf das Gerät zu bringen oder Daten wie Passwörter abzugreifen.
  - Datenleaks bei Unternehmen: Cyber-Kriminelle nutzen Sicherheitslücken bei Anbietern aus, um an Kundendaten zu kommen, die auf Servern gespeichert sind.
  - Fake-Profile auf sozialen Netzwerken: Kriminelle kapern oder duplizieren Social-Media-Accounts, um die Kontakte in der Freundesliste des gehackten oder duplizierten Profils anzuschreiben und sie dazu zu bringen, bspw. Geld zu überweisen oder Bezahlcodes zu verschicken.
  - Gestohlene Personalausweise oder Reisepässe: Diese werden auf dem Schwarzmarkt besonders teuer gehandelt.

Hier gelangen Sie zu einer Checkliste, wie Sie Phishing Mails erkennen können:

TiPP

DAS SOLLTEN SIE TUN, WENN SIE BETROFFEN SIND:

- **Bei einem Datenleak:**

✓ Ob Sie von einem Datenleak betroffen sind, können Sie beispielsweise hier prüfen: https://sec.hpi.de/ilc/search?lang=de

✓ Ändern Sie Passwörter betroffener Online-Accounts, insbesondere das Ihres E-Mail-Accounts.

✓ Überwachen Sie Ihre Konto-Aktivitäten und behalten Sie Ihr Bankkonto im Blick. Sollten Sie beispielsweise Abbuchungen bemerken, die Sie sich nicht erklären können, informieren Sie umgehend Ihre Bank und stellen Sie Strafanzeige.

✓ Vorsicht vor möglichen Phishing-Versuchen. Um an Ihr Passwort zu kommen, könnten Kriminelle mit den ergaunerten Daten versuchen, Sie gezielt mit vorgetäuschten E-Mails oder SMS dazu zu bringen, auf einen Link zu klicken, über den Sie sich bspw. in Ihren Account einloggen sollen.

✓ Informieren Sie Ihre Kontakte, falls beispielsweise einer Ihrer Social Media-Accounts gehackt wurde.

- **Bei Schadprogrammen auf dem Gerät:**

✓ Trennen Sie das Gerät vom Internet.

✓ NICHT auf Zahlungsaufforderungen eingehen.

✓ Ändern Sie Passwörter sämtlicher Accounts.

✓ Ziehen Sie ggf. einen IT-Experten hinzu.

- **Sie erhalten Rechnungen, Inkasso- oder Mahnbriefe:**

✓ Unberechtigte Forderungen abwehren (siehe Musterbrief). Gläubiger kontaktieren und Vertragsschluss bestreiten.

✓ Einträge bei Auskunfteien einsehen und etwaige Falscheinträge berichtigen/sperren lassen.

✓ Strafanzeige bei der Polizei stellen.

SO KÖNNEN SIE SICH VOR IDENTITÄTSDIEBSTAHL SCHÜTZEN:

- **Geizen Sie mit Ihren Daten!** Nutzen Sie verschiedene Pseudonyme und posten keine unnötigen privaten Informationen. Achten Sie darauf, dass Ihre Profile auf sozialen Medien nicht öffentlich einsehbar sind.

- **Schützen Sie Ihre Online-Accounts:**

✓ Achten Sie auf starke Passwörter. Verwenden Sie für jedes Nutzerkonto ein individuelles, starkes Passwort. Ausführliche Tipps für sichere Passwörter finden Sie auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik.

✓ Nutzen Sie – wenn möglich – eine Zwei-Faktor-Authentisierung.

- **Seien Sie skeptisch!**

✓ Betrüger kommen oft per Phishing zum Beispiel per E-Mail oder SMS an die Daten ihrer Opfer. Seien Sie vorsichtig, wenn sensible Daten wie Passwörter, PINs, Bankverbindung oder Kreditkartennummern abgefragt werden. Geben Sie Passwörter und PINs niemals an andere weiter.

✓ Klicken Sie nicht auf Links und Anhänge in E-Mails oder SMS, die Sie unaufgefordert erhalten.

✓ Bei Zweifeln an der Echtheit einer Nachricht: Über anderen Kontaktweg nachfragen, ob sie wirklich vom Empfänger stammt.

@

MUSTERBRIEFE

Auf unserer Webseite finden Sie einen Musterbrief, mit dem Sie sich bei Identitätsdiebstahl gegen Forderungen wehren können:

WEITERFÜHRENDE TIPPS BEI BETRUG

Weitere Tipps, was Sie tun können, wenn Kriminelle in Ihrem Namen einkaufen:

Verbraucherzentrale Nordrhein-Westfalen e.V., Mintropstr. 27, 40215 Düsseldorf, www.verbraucherzentrale.nrw
Stand: 08/2023