Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Identitätsdiebstahl im Internet

So können Sie sich vor einem Identitätsdiebstahl schützen!

Wenn Cyberkriminelle Ihre Identität im Internet missbrauchen, handelt es sich um einen Identitätsdiebstahl. Ein Identitätsdiebstahl kann in unterschiedlichen Ausprägungen vorkommen. Beispielsweise als Abschluss von kostenpflichtigen Abos oder Verbreitung von politischen Desinformationskampagnen in sozialen Netzwerken. Ein Identitätsdiebstahl ist dabei nicht nur im Internet möglich, sondern kann auch analog erfolgen z.B. beim Enkeltrick.

Was ist ein Identitätsdiebstahl?

Bei einem Identitätsdiebstahl im Internet verschaffen sich Cyberkriminelle Zugang zu fremden Accounts, um in deren Namen kriminelle Handlungen durchzuführen.[1] Zugangsdaten werden dabei häufig durch Täuschungsversuche oder Phishing-E-Mails erbeutet.

Für einen Identitätsdiebstahl ist es aber nicht zwingend notwendig, dass sich Cyberkriminelle Zugriff auf Ihre Accounts verschaffen. Ebenso können Cyberkriminelle beispielsweise in sozialen Netzwerken neue Accounts in fremdem (Ihrem) Namen erstellen und diese mit Ihren persönlichen Informationen und Bildern befüllen, die das Profil täuschend echt erscheinen lassen.[2]

Was sind typische Beispiele für einen Identitätsdiebstahl?

1. Cyberkriminelle kaufen auf Ihren Namen bei Online-Händlern ein und schließen kostenpflichtige Abos oder Verträge ab (z.B. Handyverträge, Online-Streaming-Dienst-Verträge).
2. Kriminelle erlangen Zugriff auf Ihr Bankkonto bzw. Online-Banking und buchen Geldbeträge ab.

3. Freunde oder Bekannte werden mit der gestohlenen Identität getäuscht, in dem sich die Angreifenden als Person in einer Notlage ausgeben und um Geld bitten.
4. Bei E-Mail-Konten und Accounts in sozialen Netzwerken werden Freunde und Bekannte auf Phishing-Links verwiesen oder infizierte Dateianhänge zugesandt.
5. Der Verkauf von illegalen Waren auf fremden Namen im Internet.

Welche Schäden können entstehen?

Kriminelle können durch einen Identitätsdiebstahl mitunter hohe personelle und finanzielle Schäden anrichten.

1. **Finanzielle Schäden:**
   Häufig sind finanzielle Motive Grund für Identitätsdiebstahl. Ob Einkauf in Online-Shops, Kreditkartenbetrug, Abbuchung von Geldbeträgen oder teuren Abos. Die Opfer sind von teils hohen finanziellen Schäden betroffen.
2. **Persönliche Schäden:**
   Auf sozialen Netzwerken und beim sog. Cyber-Mobbing werden die Opfer in der Öffentlichkeit bloßgestellt oder es werden Unwahrheiten verbreitet. Dadurch wird die Reputation der betroffenen Personen massiv beschädigt.

Was ist die richtige Reaktion?[3]

1. Ändern Sie unverzüglich die Passwörter Ihrer Online-Accounts.
2. Lassen Sie Ihre Bankkonten sperren, falls Sie von betrügerischen Abbuchungen betroffen sind.
3. Stellen Sie unverzüglich eine Strafanzeige bei der Polizei, um sich vor rechtlichen Konsequenzen zu schützen.
4. Widersprechen Sie Mahnbescheiden innerhalb einer 2-wöchigen Frist.
5. Melden Sie den Identitätsdiebstahl bei den Plattformbetreibern.
6. Melden Sie den Identitätsdiebstahl bei Auskunfteien (z.B. Schufa) und lassen Sie Ihre dortigen Einträge berichtigen.

Wie können Sie sich schützen?

1. **Starke Passwörter:**
   Schützen Sie Ihre Accounts und Profile mit starken Passwörtern und nutzen Sie zur Organisation Ihrer Passwörter einen Offline-Passwortmanager. Nutzen Sie für jeden Account ein individuelles starkes Passwort.

2. **Zwei-Faktor-Authentifizierung:**
   Aktivieren Sie, wenn möglich, die Zwei-Faktor-Authentifizierung, um sich in Ihre Accounts einzuloggen.
3. **Umgang mit persönlichen Informationen:**
   Gehen Sie vorsichtig mit persönlichen Informationen um und beachten Sie das Prinzip der Datensparsamkeit, insbesondere in sozialen Netzwerken.
4. **Geräteschutz:**
   Schützen Sie die Geräte, die Sie zum Zugriff auf Accounts nutzen durch Virenschutzprogramme, Updates und durch eine automatische Displaysperre.
5. **Phishing-E-Mails:**
   Prüfen Sie E-Mails immer auf Merkmale von Phishing und geben Sie im Zweifelsfall keine sensiblen Daten, wie z.B. Passwörter, auf sich öffnenden Seiten ein.
6. **Öffentliche WLAN-Netzwerke:**
   Seien Sie vorsichtig im Umgang mit öffentlichen WLAN-Netzwerken, da diese Ihre Daten meist unverschlüsselt und somit unsicher übertragen.
7. **Downloads:**
   Laden Sie Apps und Software nur vom Anbieter der Software oder in seriösen App-Stores herunter.

Quellen:

[1] https://www.cybersicherheit.nrw/de/identitaetsdiebstahl

[2] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html

[3] https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750

Weitere CSBW-Factsheets unter folgendem Link:
Wissen kompakt: Factsheets | Cybersicherheitsagentur

Oder QR-Code scannen:

www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 02.2025
Kontakt: schulungen@cybersicherheit.bwl.de