POLIZEI Hamburg

WIR INFORMIEREN

IDENTITÄTSMISSBRAUCH

Hamburg

Worum geht es?

Ihre Identität ist ein hohes Gut – und keiner von uns möchte, dass die eigene Identität von Fremden für unlautere Zwecke missbraucht wird.

Fremde Identitätsdaten sind zur Handelsware geworden und werden für alle möglichen Zwecke, vor allem zum Abschluss von Verträgen, missbraucht. Wo z.B. Händler Waren gegen Rechnung versenden, ist es für Betrüger ein Leichtes, unter einem fremden Namen* Dinge zu bestellen und diese bspw. an eine Paketstation liefern zu lassen.

* Da Online-Händler in der Regel vor einer Auslieferung von Waren die Bonität von Bestellern bei Wirtschaftsauskunfteien (z.B. der Schufa) überprüfen, sind die Betrüger auf die Daten von real existierenden Personen angewiesen.

Wo ist das Problem?

Fremde Identitäten werden zumeist zur Begehung von Straftaten, z.B. Betrügereien, missbraucht. Betrogene Online-Händler geben nicht bezahlte Rechnungen regelmäßig an **Inkasso-Services** weiter, die zu dem missbräuchlich genutzten Namen eine Anschrift– Ihre Anschrift – ermitteln. Und so sehen Sie sich erstmals dem Vorwurf ausgesetzt, Ihre Bestellung nicht gezahlt zu haben.

Inkasso-Ermittlungen gehen in der Regel auch mit einer Meldung an die besagten **Wirtschaftsauskunfteien** einher, wodurch Ihnen persönlich weitere Nachteile (reduzierte Kreditwürdigkeit) entstehen.

Wie kann ich mich schützen?

1. Beachten Sie das 1x1 der Online-Sicherheit!

Wie kann ich mich schützen?

2. Achten Sie auf Ihre Daten!

Gehen Sie in allen Lebensbereichen sparsam mit der Preisgabe Ihrer persönlichen Daten um.

ONLINE: Nutzen Sie Dienste (z.B. Soziale Netzwerke) unter einem Pseudonym oder mit verkürztem (Nach-)Namen, der keine unmittelbaren Rückschlüsse auf Ihre Person zulässt.

OFFLINE: Leeren Sie Ihren Briefkasten täglich und achten Sie darauf, welche Daten von Ihnen (z.B. auf Briefen) im Altpapiercontainer landen.

Zeigen Sie den Verlust von Ausweispapieren und Zahlungskarten umgehend an und lassen Sie Kartendaten unverzüglich sperren.

3. Achten Sie auf sichere Verbindungen!

Geben Sie vertrauliche Daten niemals ein, wenn Sie über einen öffentlichen Zugang (z.B. offene WLAN-Hotspots in Hotels oder im ÖPNV) mit dem Internet verbunden sind – auch das automatische Einloggen mit voreingetragenen Zugangsdaten ist hier riskant.

4. Achten Sie auf Risiken in Nachrichten!

Links in empfangenen Nachrichten können Sie auf Seiten führen, über die ein Schadcode auf Ihr Endgerät geladen wird – Dateianhänge können diesen Schadcode direkt mitbringen. Klicken Sie deshalb niemals vorschnell auf Links und öffnen Sie Dateianhänge nur, wenn Sie eine Zusendung erwarten.

5. Achten Sie auf Ihre Kontoauszüge!

Prüfen Sie regelmäßig Ihre Kontoauszüge und Kreditkartenabrechnungen auf unklare Abbuchungen und widersprechen Sie Buchungen, die nicht von Ihnen veranlasst wurden, umgehend.

DAS 1X1 DER ONLINE-SICHERHEIT

Quelle: BSI / eigene Bearbeitung

1. Nutzen Sie ein **Anti-Viren-** und ein **Anti-Spyware-Programm** und halten Sie diese durch automatische Updates aktuell!

2. Setzen Sie eine **Personal Firewall** ein! Sie schützt vor Angriffen aus dem Internet und verhindert bei einer Infektion des PCs, dass ausspionierte Daten an einen Angreifer gesendet werden können.

3. Sofern Sie nicht die automatisierten Update-Funktionen nutzen, **aktualisieren** Sie Ihr Betriebssystem, Ihren Browser und andere verwendete Software regelmäßig!

4. Gehen Sie nie mit Administrator-Rechten online, denn so können Schadprogramme auf alle Daten und Rechnerfunktionen zugreifen! Richten Sie für alle Nutzer **Benutzerkonten mit eingeschränkten Rechten** ein. So werden auch private Daten vor unbefugtem Zugriff geschützt.

5. Gehen Sie sorgfältig mit **Zugangsdaten** um! Halten Sie Benutzernamen und Kennwörter für E-Mail-, Shopping-, Banking- oder Bezahldienste unter Verschluss! Wählen Sie **sichere Passwörter** und wechseln Sie diese in regelmäßigen Abständen!

6. Seien Sie vorsichtig beim Öffnen von **E-Mail-Anhängen** – diese können Schadprogramme enthalten. Fragen Sie im Zweifel beim Absender nach, ob der Anhang tatsächlich von ihm stammt.

7. Seien Sie vorsichtig bei **Downloads** von Webseiten! Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist.

8. Seien Sie zurückhaltend mit der Veröffentlichung bzw. Weitergabe von **persönlichen Informationen**! Online-Betrüger nutzen zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, um Vertrauen zu erwecken.

9. Achten Sie bei Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN) auf eine **Verschlüsselung** Ihrer Kommunikation, damit Ihre Daten nicht von Dritten mitgelesen bzw. abgehört werden können.

10. Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit Schadsoftware, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig **Sicherungskopien** Ihrer Daten auf externen Datenträgern (CD/DVD, USB-Stick, externe Festplatte) erstellen.

Was tun, wenn es passiert ist?

1. Reagieren Sie schnell und richtig!

Bei einem Missbrauch Ihrer Identität sollten Sie umgehend aktiv werden.

- ✓ Setzen Sie sich **am besten persönlich** (telefonisch) mit Firmen in Verbindung, die Ihnen eine Rechnung/Mahnung zugestellt haben.
- ✓ Melden Sie einen Identitätsmissbrauch bei den großen **Wirtschaftsauskunfteien;** entsprechende Formulare unter: **schufa.de** und **crifbuergel.de**
- ✓ Widersprechen Sie in jedem Fall fristgerecht einem **gerichtlichen Mahnbescheid,** da eine Forderung gegen Sie ansonsten vollstreckbar wird.

WICHTIG: Seien Sie sehr vorsichtig bei angeblichen Rechnungen, die Ihnen per E-Mail zugestellt werden. Denn mit dem Betreff „Rechnung" o.ä. werden nicht selten Dateien verschickt, die auf Ihrem Endgerät Schadcodes ausführen.

2. Ändern Sie Ihre Passwörter!

Sollte der Verdacht bestehen, dass Fremde Zugang zu einem kritischen Konto (E-Mail, Online-Banking, Soziale Netzwerke, Online-Bezahldienst) erlangt haben, ändern Sie umgehend die betreffenden Zugangsdaten. Sollten Sie selbst keinen Zugang mehr zu Ihren Konten haben, versuchen Sie zunächst, diesen über die Funktion „Passwort vergessen" wieder zu erlangen. Informieren Sie im Zweifel den Betreiber des jeweiligen Dienstes.

WICHTIG: Verwenden Sie für alle Dienste **unterschiedliche und sichere** Passwörter und wechseln Sie diese regelmäßig; Tipps finden sich z.B. auf: **bsi-fuer-buerger.de**

3. Erstatten Sie Strafanzeige!

Wurde Ihre Identität missbräuchlich verwendet, erstatten Sie Strafanzeige. Dies können Sie über die Seite Ihrer Polizei auch online erledigen, in Hamburg unter: **https://www.polizei.hamburg/onlinewache/**

IMPRESSUM

Landeskriminalamt Hamburg
FSt 3 | Jugend, Prävention, Opferschutz

Bruno-Georges-Platz 1 | 22297 Hamburg
Tel.: 040 42 86 - 7 03 20
Fax: 040 42 86 - 7 03 09
kriminalpraevention@polizei.hamburg.de
https://www.polizei.hamburg

Frontbild: AdobeStock / Scusi / eigene Bearbeitung

Stand: Mai 2020