Haus des Stiftens
Engagiert für Engagierte

Quelle: Bundesamt für Sicherheit in der Informationstechnik

SO SCHÜTZEN SIE SICH VOR DIGITALEM IDENTITÄTSDIEBSTAHL UND GEHACKTEN ACCOUNTS

Cyberkriminelle verschaffen sich mitunter unbefugt Zugriff zu einem fremden Account: Etwa mithilfe von Phishing-Mails oder Datenlecks greifen sie Login-Daten ab. Anschließend können sie sich einloggen und den Account übernehmen. Über ein fremdes Onlineshopping-Konto verkaufen sie dann beispielsweise illegale Waren. Bei einer strafrechtlichen Verfolgung führt die Spur zunächst zum Besitzer oder der Besitzerin des gehackten Kontos. Die eigentlichen Täterinnen und Täter aber bleiben im Verborgenen.

Um sich im Internet als eine andere Person auszugeben, müssen Cyberkriminelle jedoch nicht zwingend ein fremdes Konto übernehmen. Eine andere Strategie ist, einen neuen Account in fremdem Namen zu erstellen. Zuvor sammeln sie Bilder und private Daten wie Geburtsdatum und Beruf. Damit befüllen sie zum Beispiel ein Social Media-Profil, das täuschend echt aussehen kann. Sie bitten dann etwa Familienmitglieder der betroffenen Person, ihnen in einer finanziellen Notlage auszuhelfen, oder nutzen deren Vertrauen aus, um an sensible Daten zu gelangen. Zugleich verschicken sie Links zu infizierten Webseiten.

Digitaler Identitätsdiebstahl hat also viele Gesichter. Die Gemeinsamkeit: Kriminelle geben sich im Internet als eine andere Person aus. Die Folgen können schwerwiegend sein – von finanziellen Schäden über Rufschädigung bis zu strafrechtlichen Konsequenzen. Damit es so weit nicht kommt, sollten Sie Cyberkriminellen möglichst viele Steine in den Weg legen.

Wie Sie Ihre digitale Identität und Ihre Accounts absichern

Wenn Sie einen neuen Account anlegen:

- Folgen Sie unseren Empfehlungen zu starken Passwörtern und nutzen Sie einen Passwort-Manager.
- Verwenden Sie für jeden Dienst ein eigenes Passwort. Sollte zum Beispiel Ihr Social Media-Konto gehackt werden, ist so etwa Ihr E-Mail-Konto nicht mitbetroffen.
- Aktivieren Sie die Zwei-Faktor-Authentisierung, wo möglich. Wird ein Passwort erraten, veröffentlicht oder anderweitig gehackt, erschweren Sie es so Cyberkriminellen, Zugriff zu ihren Accounts zu gewinnen.
- Geben Sie nur so viel wie unbedingt notwendig über sich preis – sowohl öffentlich als auch gegenüber dem Anbieter ihres E-Mail-Dienstes oder einer Social Media-Plattform.
- Nutzen Sie unterschiedliche Nutzernamen auf unterschiedlichen Plattformen. So erschweren Sie es Cyberkriminellen, ein Gesamtprofil über Sie zu erstellen.

Wenn Sie im Internet unterwegs sind:

- Verwenden Sie für Geräte wie Smartphones oder Tablets eine Displaysperre. Diese kann zum Beispiel auf biometrische Daten wie einen Fingerabdruck zurückgreifen. Lassen Sie sich zudem nicht bei der Eingabe von Passwörtern beobachten.
- Prüfen Sie E-Mails genau, bevor Sie auf Anhänge oder Links klicken. Mit Phishing-Mails versuchen Cyberkriminelle zum Beispiel, Passwörter abzugreifen. Auch sind E-Mail-Anhänge einer der häufigsten Wege, um Schadsoftware einzuschleusen.
- Dasselbe gilt für alle Links, die Ihnen im Internet begegnen: Hinter scheinbar lustigen oder skandalösen Inhalten verbergen sich oft präparierte Webseiten oder Malware.
- Seien Sie vorsichtig im Umgang mit öffentlichen WLAN-Netzwerken. Zu Risiken können die unverschlüsselte Übertragung von Daten und das Einschleusen von Schadsoftware gehören.
- Schützen Sie sich mit regelmäßigen Updates von Software und Betriebssystem. Diese schließen Sicherheitslücken oft, bevor Cyberkriminelle sie ausnutzen können.
- Verwenden Sie auf allen Geräten einen Virenscanner und aktivieren Sie die Firewall.
- Nutzen Sie unterschiedliche E-Mail-Adressen, eine etwa für Gewinnspiele, Newsletter und soziale Netzwerke, eine andere für wichtige Kommunikation mit engen Kontakten.
- Erzählen Sie online nichts über sich, das Sie nicht auch Fremden in der U-Bahn erzählen würden. Stellen Sie daher auch Ihre Social Media-Profile auf privat und prüfen Sie Freundschafts- oder Folgeanfragen gründlich.

Wenn Sie von digitalem Identitätsdiebstahl betroffen sind:

Im Ernstfall kann rasches Handeln schwere Folgen verhindern. Dafür bieten wir eine

- Anleitung für Betroffene von gehackten Accounts, insbesondere E-Mail-Konten,
- für Betroffene von Identitätsdiebstahl auf Social Media-Plattformen sowie
- für Betroffene von mit Schadsoftware infizierten Geräten.