Über Kanäle der sozialen Netzwerke bleiben Sie in Kontakt mit Familie und Freunden. Nützlich, aber auch riskant: Jeden Moment kann es im Netz zu Identitätsdiebstahl kommen, oder private bzw. dienstliche Informationen werden ausgespäht.

Private Informationen verbreiten sich

Oft werden die Privatsphäre-Einstellungen in sozialen Medien nicht konsequent genutzt, sodass private Aufnahmen und Daten, Telefonnummern oder E-Mail-Adressen auf fremden Webseiten landen oder betrügerisch missbraucht werden.

Das Phishing der Passwörter

Mit täuschend ähnlich gestalteten E-Mails und Webseiten seriöser Firmen bringen Betrüger arglose Nutzer dazu, auf Phishing-Links zu klicken und im nächsten Schritt persönliche Zugangsdaten zu verraten.

Identitätsdiebstahl und Abzocke

Kriminelle hacken die Accounts echter Nutzer und geben sich als diese aus. Zum Beispiel um Freunde des Opfers um Geld zu bitten.

Unsichere Spiele

Betrüger verschicken Nachrichten mit einem Link auf manipulierte Webseiten, um Schadsoftware zu verbreiten. Mit demselben Ziel werden auch Minispiele auch auf gewöhnlichen Plattformen angeboten. Diese Seiten erreicht man zwar über die großen sozialen Netzwerke, sie haben aber nicht immer hohe Sicherheitsstandards.

Mobbing

Öffentliche Belästigung und Beleidigung haben durch die sozialen Medien neue Dimensionen angenommen. Menschen werden geblockt, aus Gruppen entfernt, auf der eigenen Seite attackiert. Viele Angreifer verbergen dabei ihre Identität mit einem falschen Profil, um hemmungslos vorgehen zu können.

www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©Julien Eichinger (Titel), ©metamorworks (innen oben), ©sabelskaya (innen unten)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Sicherheit auf Facebook und Co.

Tipps und Tricks, wie man Identitätsdiebstahl, Betrug und Datenlecks verhindert

Informationssicherheit

Vor Identitätsdieben, Betrügern und Hatern kann man sich schützen. Es gibt gegen alle Angriffe auf die Datensicherheit Gegenmittel, die auch einem Nutzer ohne IT-Studium helfen: nicht sehr komplex, aber wirksam.

1. Unterschiedliche Zugangsdaten

Melden Sie ihre verschiedenen Accounts in sozialen Medien mit separaten Passwörtern und nach Möglichkeit auch mit verschiedenen E-Mail-Adressen an.

2. Doppelter Schutz

Verwenden Sie – wenn vom Anbieter vorgesehen – eine Zwei-Faktor-Authentifizierung zur Sicherheit Ihrer Accounts (Passwort plus persönliche Endgeräte). Bei Mobilgeräten achten Sie darauf, dass der Zugriffsschutz mit Sperrcode aktiviert ist.

3. Vorsicht bei Drittanbietern

Informieren Sie sich über die Vertrauenswürdigkeit von Apps, Add-ons oder Plug-ins, bevor Sie sich anmelden.

4. Identitätsdiebe auflaufen lassen

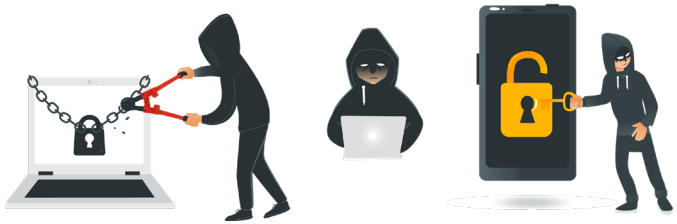
Wenn Sie zweifelhafte Anfragen über den Account eines Freundes erhalten, fragen Sie per Telefon oder persönlich nach, ob derjenige wirklich selbst geschrieben hat.

5. Schadsoftware aussperren

Seien Sie immer misstrauisch und klicken Sie nicht unüberlegt auf Links oder öffnen Dokumente, die Sie per E-Mail oder Nachricht erhalten.

6. Privatsphäre schützen

Lernen und verwenden Sie die Sicherheitseinstellungen Ihrer Netzwerke. Sie können z. B. festlegen, dass Suchmaschinen nicht auf Ihr Profil zugreifen können.



7. Wehren Sie sich

Melden Sie Cyberstalker und Hasskommentare dem Netzwerkbetreiber, damit deren Profile gelöscht werden. Auch eine Anzeige bei der Polizei ist ratsam.

8. Richtig „Schlussmachen“

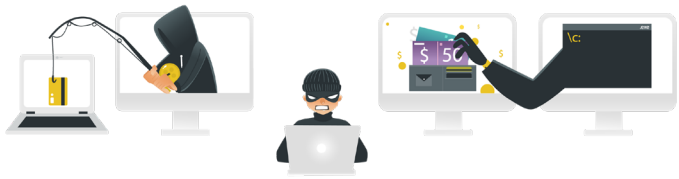
Löschen Sie jeden Account, den sie nicht mehr brauchen. Nutzen Sie das dafür angebotene Prozedere des Anbieters.

9. Wissen, worauf man sich einlässt:

Prüfen Sie, wie ein Netzwerkanbieter mit Daten umgeht. Auch wenn es mühsam ist: Erst die Datenschutzbestimmungen und AGB lesen, dann anmelden.

10. Nichts ist wirklich ohne Gegenleistung!

Scheinbar kostenlose Dienste finanzieren sich in der Regel über Werbung. Dabei geht es nicht nur darum, Ihnen Werbung anzuzeigen, sondern vor allem um die Ergründung von persönlichen Bedürfnissen und Vorlieben zur Bildung von Profilen. Diese Informationen werden in der Regel weiterverkauft.



Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:	Klaus Mebus
Dienststelle:	Bauhaus-Universität Weimar, SCC
Telefon:	03643 58 24 32
E-Mail:	security@uni-weimar.de