Fokus: Online-Banking

Grundlegende (Sicherheits-)Hinweise

90 Minuten MEDIEN

Ein Angebot der MEDIENANSTALT HESSEN

Grundlegende (Sicherheits-)Hinweise

Online-Banking nur mit **eigenem Gerät**
und in sicherer Umgebung

Beispiele für **unsichere** Situationen:

- fremde oder gemeinsam genutzte Computer
- öffentliches WLAN
- wenn andere über die Schulter schauen können

Grundlegende (Sicherheits-)Hinweise

Online-Banking nur über offizielle Wege

- die Banking-App der Bank oder
- die offizielle Internetseite der Bank

Grundlegende (Sicherheits-)Hinweise

Online-Banking nur über offizielle Wege

- die Banking-App der Bank oder
- die offizielle Internetseite der Bank

Tipps

- **Lesezeichen für die Bank-Internetseite setzen**
- **niemals Links aus E-Mails anklicken**
- **auf https / Schloss-Symbol in der Adresszeile im Browser achten**

Grundlegende (Sicherheits-)Hinweise

Software aktuell halten

Warum?
Updates schließen Sicherheitslücken

Was aktualisieren?

- Betriebssystem (des Smartphones/Tablets, bzw. des Computers – z. B. Windows)
- Browser
- Banking-App

Grundlegende (Sicherheits-)Hinweise

Software aktuell halten

Warum?
Updates schließen Sicherheitslücken

Was aktualisieren?

- Betriebssystem (des Smartphones/Tablets, bzw. des Computers – z. B. Windows)
- Browser
- Banking-App

Tipp: Automatische Updates aktivieren

Grundlegende (Sicherheits-)Hinweise

Anmeldung (Login)

Für das Online-Banking
braucht man

1. Benutzername /
   Anmeldename / Alias / ID

2. PIN oder Passwort

Grundlegende (Sicherheits-)Hinweise

Anmeldung (Login)

Für das Online-Banking braucht man

1. Benutzername / Anmeldename / Alias / ID

2. PIN oder Passwort

Das Passwort sollte
- **nur für Online-Banking verwendet werden**
- **nicht leicht zu erraten sein**

Grundlegende (Sicherheits-)Hinweise

Anmeldung (Login)

Für das Online-Banking braucht man

1. Benutzername / Anmeldename / Alias / ID

2. PIN oder Passwort

Das Passwort sollte
- **nur für Online-Banking verwendet werden**
- **nicht leicht zu erraten sein**

Nicht geeignet (Beispiele):

- **12345, 11111 o.ä.**
- **Geburtsdatum**
- **Postleitzahl**

Grundlegende (Sicherheits-)Hinweise

Freigabe von Bankgeschäften, z. B.:
bei Überweisungen, Änderungen und manchmal zusätzlich bei der Anmeldung

Freigabe erfolgt meist mit

TAN-App

- auf dem registrierten Smartphone
- geschützt durch Passwort oder Fingerabdruck/Gesichtserkennung
- teilweise durch Scannen eines QR-Codes am Computer-Bildschirm

oder TAN-Generator

- separates Gerät
- funktioniert zusammen mit der EC-Karte

Grundlegende (Sicherheits-)Hinweise

Freigabe von Bankgeschäften, z. B.:
bei Überweisungen, Änderungen und manchmal zusätzlich bei der Anmeldung

Freigabe erfolgt meist mit

TAN-App

- auf dem registrierten Smartphone
- geschützt durch Passwort oder Fingerabdruck/Gesichtserkennung
- teilweise durch Scannen eines QR-Codes am Computer-Bildschirm

oder TAN-Generator

- separates Gerät
- funktioniert zusammen mit der EC-Karte

Vor Freigabe immer erst prüfen: Betrag und Empfänger korrekt?

Grundlegende (Sicherheits-)Hinweise

Warum ist Online-Banking sicher?

Es braucht zwei Faktoren

1. Wissen – z. B. Passwort / PIN
2. Besitz oder Biometrie – z. B. Smartphone, EC-Karte oder Fingerabdruck

Grundlegende (Sicherheits-)Hinweise

Warum ist Online-Banking sicher?

Es braucht zwei Faktoren

1. Wissen – z. B. Passwort / PIN
2. Besitz oder Biometrie – z. B. Smartphone, EC-Karte oder Fingerabdruck

Für Kriminelle reicht es also nicht, nur das Passwort zu kennen. (Was Kriminelle sonst noch versuchen, sehen wir gleich.)

Fokus: Online-Banking

90 Minuten MEDIEN

Ein Angebot der MEDIENANSTALT HESSEN

In Kooperation mit

DIGITAL IM ALTER HESSEN

LANDESSTIFTUNG MITEINANDER IN HESSEN

Umgesetzt vom

BÜRO FÜR MEDIENBILDUNG