BSI - Online Banking - Zusatzinformationen

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/onlinebanking_node.html

Inhaltsverzeichnis

Zusatzinformationen

Verwandte Themen

Gerät einrichten

Machen Sie es Angreifern schwer und setzen Sie Sicherheitseinstellungen für Computer, Smartphone & Co.

Banking-Software

Statt Online-Banking mit dem Browser zu nutzen, können Sie auf dem PC auch eine extra Online-Banking-Software verwenden. Während Browser kostenlos im Internet heruntergeladen werden können, ist Online-Banking-Software in der Regel nicht kostenfrei. Diese Programme bieten aber im Gegenzug neben dem Online-Zugriff auf die Konten meist zusätzliche Funktionen zur Verwaltung mehrerer Konten und Depots, die den Überblick über die eigenen Finanzen erleichtern. Zudem können Sie mithilfe von Banking-Software Transaktionen mit den besonders sicheren Signaturverfahren durchführen.

Sicherheit im Online-Banking: Die PIN- TAN-Verfahren und andere Schutzmaßnahmen. Erfahren Sie, welche Sicherheitsverfahren es beim Online-Banking gibt.

Schutz für Smartphone und Co.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

Mittlerweile entsprechen die mobilen, internetfähigen Geräte kleinen Computern, auf denen gearbeitet, kommuniziert und vertrauliche Daten gespeichert werden. Dadurch gelten für sie mindestens die gleichen Sicherheitsanforderungen wie für stationäre Computer. Die Sicherheit spielt im Grunde sogar eine noch größere Rolle, denn die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden, birgt zusätzliches Gefahrenpotenzial.

Alle Benutzer von Smartphones und Tablets sollten daher folgende, kurze Sicherheitshinweise beachten.

Die dienstliche Nutzung von privaten Geräten ist nicht nur praktisch, sondern stellt zusätzliche Anforderungen an die sichere Verwendung der Geräte. Aus diesem Grund finden Sie am Ende dieser Seite unter anderem Links zu Überblickspapieren, die sich dieses Themas annehmen.

Sicherheitshinweise für mobile internetfähige Geräte:

- **Sorgen Sie für einen Basisschutz und führen Sie regelmäßig Sicherheitsupdates durch.** Vergewissern Sie sich, dass die vorhandenen Sicherheitseinstellungen Ihres Geräts eingeschaltet sind. Aktualisieren Sie Apps und Betriebssystem umgehend, sobald Aktualisierungen erhältlich sind. Viele Angriffe zielen auf bekannte Schwachstellen, die erst durch Updates der Hersteller geschlossen werden. Aktivieren Sie daher die automatische Update-Funktion, damit Sicherheitsupdates direkt nach dem Erscheinen eingespielt werden. Kontrollieren Sie aber auch hier, welche Erweiterungen der Berechtigungen mit dem Update verbunden sind.
- **Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die Zugriffsberechtigungen.**

Informieren Sie sich vor Installation einer App, wenn Ihnen der Anbieter nicht bekannt ist. Eine kurze Suche im Internet reicht meistens aus, um sich zu informieren. Entfernen Sie veraltete Anwendungen oder solche, die Sie nicht mehr nutzen. Denn jede zusätzliche App ist eine mögliche Sicherheitslücke.
Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind. Wichtig: Durch Updates können auch Änderung oder Erweiterung der Zugriffsberechtigungen erfolgen. Die daraus resultierenden Konsequenzen sind gegen den Mehrwert des Updates abzuwägen.
Vermeiden Sie "Sideloading" - also das Installieren von Apps aus einer anderen Quelle als dem offiziellen App-Stores - so weit wie möglich und überprüfen Sie die Quellen.

- **Nutzen Sie Sperrcodes und Passwörter.**
  Achten Sie darauf, dass die SIM/USIM-PIN und die Bildschirmsperre Ihres Telefons stets aktiviert sind. Auch sensible Anwendungen, wie Online-Banking oder App-Käufe, können mit einer PIN oder einem Passwort geschützt werden. Ersetzen Sie voreingestellte Codes durch eine eigene Kombination.
  Bequemer aber nicht ganz so sicher: Das Gerät lässt sich über das Betriebssystem mit einer Mustersperre entriegeln. Dabei ziehen Sie mit dem Finger eine bestimmte Spur über den Bildschirm. Das bietet zwar weniger Sicherheit, ist aber schneller ausführbar als das Eintippen einer Zahlenkombination. Ob PIN oder Muster: Sorgen Sie für einen Sichtschutz bei der Eingabe, damit niemand Ihre Kombination ausspähen kann. Bitte reinigen Sie auch regelmäßig Ihr Display, um Wischspuren zu beseitigen.
- **Aktivieren Sie Schnittstellen nur bei Bedarf und sichern Sie diese.**
  Deaktivieren Sie Drahtlosschnittstellen, wie WLAN, Bluetooth oder NFC, wenn Sie diese nicht benötigen. So ist Ihr Gerät weniger anfällig für Cyber-Angriffe.
  Der Aufenthaltsort von Mobilfunkgeräten kann von den Betreibern der Funknetzwerke und zum Teil auch von den App-Anbietern jederzeit ermittelt werden. Prinzipiell sollten Sie mit der Weitergabe Ihrer Ortsangaben sehr zurückhaltend sein - also etwa Lokalisierungsdienste meiden und keine Ortsangaben in Fotos speichern, die Sie ins Internet laden. Schalten Sie die GPS-Funktion aus. Dadurch wird die Positionsbestimmung zumindest ungenauer.
  Auch für USB gilt: Schließen Sie Ihr mobiles Gerät nur an vertrauenswürdige Rechner an, denn auch auf diesem Weg kann Malware übertragen werden. Gleiches gilt für die Stromzufuhr. Auch hier ist auf eine vertrauenswürdige USB-Verbindung zu achten.
- **Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.**
  In öffentlichen WLAN-Netzen im Café oder am Flughafen ist der Zugang meist unverschlüsselt. Hier ist erhöhte Vorsicht geboten. Nutzen Sie, sofern möglich, eine gesicherte Verbindung, die am Kürzel https in der Adresszeile erkennen. Anwendungen wie Online-Banking sollten Sie in offenen Netzwerken nicht ausführen. Falls es doch notwendig ist, empfiehlt sich der Aufbau einer sicheren Verbindung. Nutzen Sie dafür eine App, die ein Virtuelles Privates Netzwerk (VPN) aufbauen kann.
  Mit der Tethering-Funktion können andere Anwender Ihre Internetverbindung. Ihr Gerät wird so zu einem Hotspot. Nutzen Sie das WLAN-Sicherheitsprotokoll WPA2 und richten Sie für den Hotspot ein sicheres Passwort ein. Teilen Sie dieses Passwort nur vertrauenswürdigen Personen mit und beenden Sie die Hotspot-Funktion, wenn Sie sie nicht mehr benötigen.
- **Lassen Sie Ihr Gerät nicht aus den Augen.**
  Um das Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Ihr Smartphone niemals unbeobachtet lassen oder verleihen.
  Verlorene oder gestohlene Geräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. Hier reicht meist der Versand einer vorher definierten Nachricht mit dem richtigen Befehlscode an die eigene Nummer. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht oder nicht mehr aufzurufen. Doch Vorsicht: Derartige Befehle können ebenso von böswilligen Dritten genutzt werden. Achten Sie auch hier auf einen vertrauenswürdigen Anbieter.
  Nach erfolgter Sperrung sollten Sie die SIM-Karte bei Ihrem Anbieter sperren lassen. Bitte beachten Sie die richtige Reihenfolge: Ist die SIM-Karte deaktiviert, lässt sich auch kein Sperrcode mehr empfangen. Installieren Sie Sicherheitslösungen für Mobilgeräte (beispielsweise Ortung, Remote-Sperung, Verschlüsselung, AV-App), die Ihrem konkreten Bedarf entsprechen.
- **Surfen Sie mit gesundem Menschenverstand.**
  Bewahren Sie sich eine gesunde Skepsis, welcher Empfehlung beispielsweise für eine App Sie folgen wollen, was Sie von wo installieren, beziehungsweise worauf Sie alles klicken. Nicht alles hält letztlich, was es verspricht, und leere Versprechungen werden gerne genutzt, um Schadsoftware auf dem Gerät zu installieren.

- **Schützen Sie Ihre Daten.**
  Nutzen Sie die Funktionen zur Datenverschlüsselung, wenn vorhanden, oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware.
  Erstellen Sie regelmäßig Backups der Daten. Hier spielt neben der Aktualität der gesicherten Daten auch der Speicherort eine wichtige Rolle. Viele Backup-Programme nutzen Cloud-Speicher als automatisches Backupmedium. Es ist zu beachten, dass diese Cloudspeicher nicht unter der Kontrolle des Benutzers liegen. Wer - außer dem Benutzer - sonst noch auf die Daten zugreifen kann, ist nicht klar. Backups in der Cloud sollten grundsätzlich verschlüsselt werden. Außerdem gibt es oft keine Garantie für die Verfügbarkeit der Daten in der Cloud.
  Als weiterer Punkt bei Backups in der Cloud ist der Spezialfall eines Verschlüsselungstrojaners zu beachten. Diese Trojaner verschlüsseln die Daten des Benutzers und machen das Gerät damit unbrauchbar. Anschließend fordern sie den Benutzer zur Zahlung eines Lösegeldes auf, um die Daten wieder zu entschlüsseln. Da die Backupprogramme automatisch geänderte Daten in den Cloudspeicher sichern, werden auch die verschlüsselten Daten gesichert und damit die originalen Daten des Backups überschrieben! In diesem Fall nutzt ein Backup gar nichts mehr.
  Der sicherste Speicherort für ein Backup ist ein externer Datenträger, beispielweise auf einem externen Computer oder eine SD-Karte, die nach einem manuellen Backupprozess aus dem Gerät entfernt wird.
- **Prüfen Sie unbekannte Rufnummern vor Rückruf.**
  Rufen Sie unbekannte Rufnummern nicht zurück. Weitere und aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf unerwünschte Rufnummern zu Mehrwertdiensten von Ihrem Netzbetreiber sperren.
- **Verschlüsseln Sie vertrauliche Gespräche.**
  Mobiles Telefonieren ist nicht abhörsicher. Wenn Sie vermehrt schützenswerte oder gar geheime Informationen austauschen wollen, weichen Sie besser auf verschlüsselte Kommunikation aus. Beachten Sie auch Vorgaben Ihres Arbeitgebers bei der privaten Nutzung eines dienstlichen Gerätes oder der dienstlichen Nutzung eines privaten Gerätes.
- **Löschen Sie alle Speicher, bevor Sie das Gerät verkaufen oder entsorgen.**
  Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, dann sollten Sie bedenken, dass Datenspuren verbleiben können, wenn nicht vorher alle Datenspeicher sicher gelöscht wurden. Wie das bei Smartphones funktioniert, ist für viele Modelle und Betriebssysteme auf dem IT-Nachrichten- und Service-Portal Chip Online, für iPhone, iPad oder iPod touch auf der Internetseite von Apple beschrieben. Die SIM-Karte sollten Sie entfernen und – falls Sie diese nicht weiter verwenden wollen – vernichten.