

Sicherheit beim Onlinebanking

Durch Anschluss eines Computers ans Internet öffnet sich eine Welt der Informationen und Unterhaltung. Der Computer ist dabei jedoch auch anfällig gegenüber zahlreichen Onlinebedrohungen. So werden z. B. Viren einfacher von einem befallenen Computer auf einen anderen Computer übertragen. Die aus diesen Onlinebedrohungen resultierenden Gefahren für den Computer können durch eine Kombination aus bewährten Vorgehensweisen wie der Erstellung starker Passwörter, der Verschlüsselung von Daten und der Verwendung von Antivirensoftware verringert werden.

In der folgenden Tabelle werden die verschiedenen Maßnahmen beschrieben, die dem Sichern von Online- und Netzwerktransaktionen dienen.

Methode	Beschreibung	
Verwenden starker Passwörter	<p>Bei einem starken Passwort handelt es sich um ein komplexes Passwort, das nicht ohne weiteres erraten werden kann. Das Passwort sollte sich aus einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie einem <i>kaufmännischen</i> und einem <i>Nummernzeichen</i> zusammensetzen und keine vollständigen Wörter oder Namen enthalten.</p> <p>Ein sicheres Passwort bietet den besten Schutz vor Sicherheits- und Datenschutzbedrohungen. Sichere Passwörter müssen für folgende Vorgänge bzw. Daten erstellt werden:</p> <ul style="list-style-type: none"> • Lokaler Zugriff auf eigenständige Computer • Zugriff auf Netzwerke • Zugriff auf Websites, die vertrauliche Informationen wie persönliche oder finanzielle Details enthalten • Zugriff auf wertvolle Daten • Auf dem Computer gespeicherte persönliche Daten 	



<p>Schutz vor Hackern und Spyware</p>	<p>Beim Surfen im Internet sendet ein auf Ihrem Computer installiertes Softwareprogramm möglicherweise persönliche Informationen an einen Hacker in einem anderen Land. Solche Programme werden als Spyware bezeichnet. Sie werden im Allgemeinen ohne Wissen des Benutzers installiert und übertragen vertrauliche Daten vom Computer an den Hacker. In manchen Fällen installieren Unternehmen bewusst Spyware auf den von Mitarbeitern verwendeten Computern, um deren Computeraktivitäten nachzuverfolgen. Um eine heimliche Installation von Spyware zu verhindern, können auf dem Computer Softwareprogramme wie Microsoft Defender installiert werden. Zudem müssen zum Schutz vor Viren und Hackern Antivirensoftware und eine Firewall auf dem Computer installiert werden.</p>	
<p>Regelmäßiges Leeren des Verlaufs und des Cache</p>	<p>Die beim Surfen im Internet besuchten Websites und Webseiten werden im <i>Verlauf</i> des Browsers gespeichert. Beim Surfen im Internet wird eine Reihe von Dateien im temporären Speicher des Computers gespeichert. Dieser temporäre Speicher wird als <i>Cachespeicher</i> bezeichnet. Die im Cachespeicher gespeicherten Dateien zeichnen Informationen zu besuchten Webseiten auf. Einige dieser temporären Internetdateien beinhalten u.U. persönliche Informationen wie Benutzername und Passwort, auf die Hacker zugreifen können. Löschen Sie regelmäßig den Inhalt des Browserverlaufs und des Cachespeichers, um Hacker am Zugriff auf persönliche Informationen zu hindern.</p>	



<p>Regelmäßiges Löschen von Cookies</p>	<p>Beim Besuch einer Website stellen Sie möglicherweise fest, dass diese Ihren Namen anzeigt. Dies ist auf die Verwendung von Cookies zurück zu führen. Cookies sind kleine Dateien, die von zuvor besuchten Websites auf dem Computer erstellt werden, um Ihr bevorzugtes Verhalten im Internet zu erkennen und nach zu verfolgen. Ihr Zweck besteht darin, der Website ein auf den jeweiligen Benutzer zugeschnittenes Profil zu verleihen. Cookies können jedoch auch eine Bedrohung für den Datenschutz darstellen, da sie persönliche Informationen beinhalten. Die Cookies enthalten möglicherweise Ihre beim Onlineeinkauf angegebenen Kreditkartendaten. Aus diesem Grund empfiehlt sich das regelmäßige Löschen von Cookies zur Verhinderung des Missbrauchs persönlicher Informationen.</p>	
<p>Durchführen von Onlinetransaktionen auf sicheren Sites</p>	<p>Beim Onlineeinkauf müssen in der Regel vertrauliche Informationen wie Bankkontonummer oder Kreditkartendaten angegeben werden. Aus diesem Grund dürfen Onlinetransaktionen nur auf sicheren Websites durchgeführt werden. Eine Website ist sicher, wenn der Name das Präfix <i>https</i> trägt. Dieses Präfix gibt an, dass die Website das <i>Secure Sockets Layer (SSL)</i>-Protokoll verwendet. Bei SSL handelt es sich um ein Internetsicherheitsprotokoll, das sichere Datenkommunikation durch Verschlüsselung der übertragenen Informationen gewährleistet. Das SSL-Protokoll bestätigt, dass die Website authentisch ist und stellt sicher, dass die angegebenen Daten nicht missbraucht werden.</p> <p>Beim Betreten einer sicheren Website zeigen die meisten Webbrowser eine Meldung an, in der bestätigt wird, dass es sich um eine sichere Website handelt. Das gesperrte Vorhängeschlosssymbol unten rechts im Browserbildschirm ist ebenfalls ein Hinweis auf eine sichere Website. Vor einer Onlinetransaktion auf dieser Website kann zudem das Sicherheitszertifikat einer Website überprüft werden.</p>	