Sparkasse
Neu-Ulm – Illertissen

Aktueller Sicherheitshinweis

Sehr geehrte Kundin, sehr geehrter Kunde,

aufgrund anhaltender und neuer Sicherheitsbedrohungen im Internet möchten wir Ihnen weitere Informationen zu Ihrem persönlichen Schutz für das S-Internet Banking mitteilen:

Mit immer raffinierteren Angriffsversuchen bzw. durch Kombination bereits bekannter Angriffsmethoden werden derzeit Internetbenutzer ausspioniert oder sogar geschädigt. Diese Angriffe werden durch Installation von Schadprogrammen (sog. Trojanische Pferde) auf dem Kunden-PC verursacht. Bitte beachten Sie daher folgende, wichtige Sicherheitshinweise:

1. Einsatz eines Virenscanners mit aktuellsten Virendefinitionen (z.B. Norton AntiVirus oder AntiVir).
2. Einsatz einer aktuellen und sicher konfigurierten Personal Firewall (z.B. Norton Internet Security oder Zonelabs ZoneAlarm).
3. Einsatz der aktuellsten Betriebssystem- und Browserupdates bzw. ServicePacks.
4. Einsatz eines Datenschutzprogrammes gegen unerwünschte Spyware (z.B. das kostenlose Javasoft Ad-Aware).

Darüber hinaus sollten Sie folgende Regeln im Umgang mit Ihren persönlichen Daten beachten:

1. Speichern Sie niemals Zugangsdaten auf Ihrem Rechner ab.
2. Benutzen Sie kein Passwortverwaltungsprogramm zum Speichern Ihrer Passworte (z.B. Passwortmanager der Internet Browser).
3. Öffnen Sie niemals E-Mails und E-Mail Anhänge mit dubiosem Inhalt; auch bei bekannten E-Mail Absendern sollten Sie Anhänge nur mit höchster Vorsicht öffnen.
4. Kontrollieren Sie in regelmäßigen Abständen Ihre Konto- bzw. Kreditkartenumsätze und teilen ggf. aufgetretene Unregelmäßigkeiten unverzüglich Ihrer Sparkasse mit.

In jüngster Zeit mehren sich auch Hinweise, dass Betrüger versuchen, sicherheitsrelevante Informationen mit dem sogenannten "Phishing" (Passwort fischen) auszuspionieren. Die aktuellste Variante bedient sich dabei ganz herkömmlicher und traditioneller Techniken. Neben dem inzwischen bekannten "Phishing" per E-Mail werden Kunden nun auch angerufen. Unter verschiedenen Vorwänden, wie z. B. nötige Wartungsmaßnahmen und/oder Sicherheitsüberprüfungen, werden Zugangsdaten zum Online-/S-Internet Banking (PIN/TAN) über das Telefon erfragt.

Bitte beachten Sie!

- Kein Mitarbeiter Ihres Institutes wird Sie jemals nach Ihrer PIN und TAN zum Online-/S-Internet Banking fragen, weder am Telefon noch per E-Mail.

Sparkasse
Neu-Ulm – Illertissen

Sicherheitshinweise für das S-Internet Banking

Die Sicherheit Ihrer Daten ist für die Sparkasse oberstes Gebot bei der Abwicklung Ihrer Geschäftsvorfälle. Daher gelten bei der Sparkasse strengste Regelungen für die Sicherheit der technischen und organisatorischen Abläufe. Besonders wichtig ist es sicherzustellen, dass niemand außer Ihnen Zugriff auf Ihr Konto oder Ihr Depot hat.

Neben unseren Aktivitäten zur Gewährleistung der Sicherheit ist auch Ihr Beitrag als Kunde unverzichtbar. Bei der Nutzung von S-Internet Banking und S-direktbrokerage gibt es Risiken, die nur durch Ihren bewussten Umgang mit diesen Diensten vermieden werden können. Aus diesem Grund ist es für uns als Ihre konto- bzw. depotführende Sparkasse ein Anliegen, Ihnen die Durchführung der nachfolgend aufgeführten Sicherheitsmaßnahmen nahe zu legen. Nur so kann Ihrer Sicherheit optimal Rechnung getragen werden. Die Hinweise hierzu finden Sie im folgenden Abschnitt Ihr Beitrag zur Sicherheit.
Die von Ihrer Sparkasse getroffenen Vorkehrungen gewährleisten die Sicherheit der Systeme und der Datenübertragung im Internet und sind im Abschnitt Unser Beitrag zur Sicherheit beschrieben.

Hinweise zur Nutzung von S-Internet Banking und zum Umgang mit Passwörtern, sowie der PIN und den TAN´s:

1. Halten Sie alle Daten, die den Zugang zu Ihrem Rechner oder zum Onlinebanking ermöglichen (Benutzernamen, Passwörter, PIN, TAN-Listen) geheim.
2. Merken Sie sich Ihre PIN und notieren Sie sie nirgends.
3. Speichern Sie weder Ihre PIN noch TAN-Nummern auf der Festplatte Ihres Rechners.
4. Bewahren Sie Ihre PIN getrennt von Ihren TANs auf.
5. Lassen Sie sich beim Anmelden und bei der Nutzung von S-Internet Banking nie über die Schulter schauen. Im Zweifelsfall ändern Sie Ihre PIN, oder veranlassen Sie die umgehende Sperrung Ihres Onlinebanking Zugangs.
6. Verwenden Sie Ihre Onlinebanking PIN und/oder TAN nie auf Internetseiten anderer Anbieter.
7. Nutzen Sie Ihre PIN nur für das S-Internet Banking mit der Sparkasse. Verwenden Sie für weitere Internetdienste, wie beispielsweise E-Mail oder Internetauktionen, auf alle Fälle andere Passwörter.
8. Ändern Sie Ihre PIN regelmäßig. Verwenden Sie keine Kombinationen, die leicht zu erraten sind, wie z. B. "12345", "11111" oder "abcde".
9. Beenden Sie das S-Internet Banking nach Erledigung Ihrer Bankgeschäfte, indem Sie sich abmelden (Button: "Abmelden" drücken) und nicht einfach nur den Browser schließen.

Sicherheitszertifikat:
Sobald auf Ihrem Bildschirm das Fenster zur Anmeldung angezeigt wird, sollten Sie außerdem prüfen, ob das Zertifikat, sowie der dazugehörige Fingerprint korrekt ist. Dazu muss auf dem Bildschirm rechts unten ein gelbes Schloss- oder Schlüsselsymbol erscheinen. Klicken Sie auf das Symbol und vergewissern Sie sich, dass das Zertifikat mit dem zugehörigen Fingerprint für den Namen "portal.izb.de", "portal1.izb.de" oder für "portal5.izb.de" ausgestellt wurde. Die aktuellen Fingerprints unserer Zertifikate erhalten Sie hier.

Das Zertifikat garantiert Ihnen, das die Kommunikation mit dem Informatik-Dienstleister Ihrer Sparkasse stattfindet, und die Daten verschlüsselt übertragen werden. Das Zertifikat enthält den öffentlichen Schlüssel des Absenders, sowie Angaben, die den Absender eindeutig identifizieren.

Die Zertifikate für "portal.izb.de", "portal1.izb.de" oder für "portal5.izb.de" wurden für den Informatik-Dienstleister Ihrer Sparkasse ausgestellt (Besitzer/Antragsteller). Hierbei handelt es sich um die:

Informatik Zentrum Bayern Softwareges. d. bay. Spark. GmbH&Co.KG

Achtung: Nicht vertrauenswürdige Internet-Verbindungen meldet Ihr Browser über Warnmeldungen, die Sie auf keinen Fall ignorieren sollten. Brechen Sie die Verbindung sofort ab, wenn eine Warnmeldung bzgl. des Zertifikats erscheint.

Sparkasse
Neu-Ulm – Illertissen

Prüfen:
Nehmen Sie sich regelmäßig Zeit, die Kontoauszüge zu überprüfen. So kommen Sie Missbrauch und anderen Unregelmäßigkeiten schnell auf die Spur.

Software:
Installieren Sie niemals Software aus unbekannter Quelle auf dem eigenen Computer. So handelt es sich z.B. auch bei Bildschirmschonern um Programme, die durchaus schädliche Funktionen besitzen können. Halten Sie die Betriebssystemsoftware (z.B. Microsoft Windows) und den Internet Browser auf dem neuesten Stand. Wenn ein Hersteller (z.B. Microsoft) Pressemitteilungen über Fehler in der Software veröffentlicht und auch entsprechende Korrekturen anbietet, installieren Sie diese bitte.
Darüber hinaus ist es auch durchaus empfehlenswert, sich von Fachleuten Rat für eine sichere Einstellung von Browser und Betriebssystem einzuholen.
(z.B. Browsercheck http://www.heise.de/security/dienste/browsercheck/)

Virenscanner / Personal Firewall:
Nutzen Sie Programme, die Ihren Computer regelmäßig auf Viren und auf sogenannte Trojaner (spionieren z.B. Passwörter aus) untersuchen. Aktualisieren Sie diese Programme regelmäßig. Über Personal Firewall Programme können Sie Ihren Rechner vor unbefugter Datenübertagung aus oder in das Internet schützen. Mit diesen Programmen können sie Ihren Rechner vor Angriffen schützen, die aus dem Internet kommen.
Aktuelle Informationen zu diesen Themen finden Sie z.B. auch unter http://www.heise.de/security/.

Löschen:
Wenn Sie den Computer mit anderen Leuten teilen, sollten Sie nach dem Onlinebanking den Zwischenspeicher (Browser-Cache) löschen. Im Internet-Explorer geht das über Extras\Internetoptionen\Allgemein\Temporäre Internetdateien\Dateien löschen.

Fremde Computer:
Loggen Sie sich nie von einem unbekannten Computer aus in das Onlinebanking ein. Besonders Internetcafes bieten oft keine sichere Plattform für das Onlinebanking. Aber auch bei Nutzung von Computern am Arbeitsplatz kann ein Zugriff Dritter auf Ihre Onlinebanking Daten möglich sein.

Phishing:
Seit kurzem ist eine neue Art von Angriff auf Internetbenutzer aufgetaucht, über die wir Sie hier informieren möchten. Während die bekannten Würmer, Viren und Trojanische Pferde überwiegend technische Maßnahmen zur Schädigung des PCs eines Internetnutzers einsetzen, erhalten sogenannte "Phishing" Opfer eine E-Mail mit gefälschten Absenderdaten einer vermeintlich seriösen Internetpräsenz. Der Internetnutzer wird mittels einer plausibel klingenden Erklärung aufgefordert, einen Link innerhalb der E-Mail anzuklicken (z.B. Sparkasse.ru anstatt Sparkasse.de), oder auf die E-Mail zu antworten. Der Link führt den Nutzer allerdings nicht auf das Internetangebot des seriösen Unternehmens, sondern auf einen nachgebildeten Internetauftritt. Die Benutzer werden auf diesen teilweise täuschend echt nachgebildeten Internetseiten aufgefordert, z.B. die Konto-, Kreditkarten- oder Zugangsdaten einzugeben (PIN und TAN). Einziges Ziel ist es, durch täuschen des Benutzers an diese vertraulichen Daten zu gelangen, um ihn in der Folge zu schädigen. Wir möchten Ihnen deshalb empfehlen, folgende Sicherheitshinweise für den E-Mailverkehr zu beachten:

- Rufen Sie das S-Internet Banking nicht durch einen Link auf, den Sie mittels einer E-Mail erhalten haben.
- Rufen Sie den Link in einer E-Mail auch dann nicht auf, wenn die E-Mail von einer scheinbar vertrauenswürdigen Person oder Quelle stammt. Der Link innerhalb der E-Mail kann gefälscht sein. Mögliche Angreifer können Sie so auf eine der S-Internet Banking Anwendung nachempfundenen Internetseite führen und zur Eingabe von persönlichen Daten oder Zugangsinformationen auffordern.
- Sollten Sie Kenntnis über Unregelmäßigkeiten im Mail-Verkehr zu oder von Ihrer Sparkasse erhalten, bitten wir Sie dies umgehend Ihrer Sparkasse zu melden.
- Um sich zu vergewissern, dass Sie mit dem S-Internet Banking ihrer Sparkasse verbunden sind, prüfen Sie bitte das Zertifikat wie im Abschnitt Sicherheitszertifikat beschrieben.

Wichtig: Ihre Sparkasse wird Sie niemals auffordern, persönliche Daten, insbesondere Zugangsdaten, per E-Mail zu versenden!

Sparkasse
Neu-Ulm – Illertissen

Weitere Informationen zu "Phishing" erhalten Sie auch auf folgenden Internetseiten:

http://www.antiphishing.org
http://www.bsi-fuer-buerger.de/abzocker/05_08.htm

Unser Beitrag zur Sicherheit im S-Internet Banking

Abschottung der S-Internet Banking Systeme:
Das S-Internet Banking System ist durch eine Firewall vom allgemein zugänglichen Internet getrennt. Die Firewall wirkt wie ein Filter: sie lässt ausschließlich diejenigen Daten vom Internet zum S-Internet Banking System gelangen, die für die S-Internet Banking Anwendung bestimmt sind. Alle anderen Daten werden abgefangen. Ein direkter, unbefugter Zugriff auf das S-Internet Banking aus dem Internet wird dadurch verhindert.

Authentifizierung von S-Internet Banking:
Wenn Sie eine Verbindung zum S-Internet Banking herstellen, identifiziert sich das S-Internet Banking System automatisch mit Hilfe eines Zertifikats. Dieses Zertifikat wurde von einer unabhängigen, vertrauenswürdigen Organisation, der Zertifizierungsstelle (VeriSign, RSA Data Security, Inc.), ausgestellt und enthält unter anderem die Internet-Adresse des S-Internet Banking Anschlusses, mit dem Sie verbunden sind. Die Beachtung der Hinweise zum Thema Sicherheitszertifikat in "Ihr Beitrag zur Sicherheit" garantiert Ihnen, dass Sie tatsächlich mit dem S-Internet Banking Ihrer Sparkasse verbunden sind.

Autorisierung der Kunden:
Die Benutzung des S-Internet Banking Systems ist nur nach erfolgreich durchgeführter Anmeldung möglich. Dazu geben Sie auf der Login-Seite Ihre für das S-Internet Banking freigeschaltete Kontonummer und Ihre Geheimzahl (PIN) ein. Durch Ihre Kontonummer werden Sie als Kunde identifiziert. Durch die PIN wird sichergestellt, dass niemand außer Ihnen selbst Zugriff auf Ihre Kundendaten hat. Ihr Zugang zum S-Internet Banking wird automatisch gesperrt, wenn die PIN dreimal nacheinander falsch eingegeben wurde. Sie haben dadurch die Sicherheit, dass Ihre PIN nicht durch mehrmaliges Ausprobieren ermittelt werden kann.

Vertraulichkeit der Datenübertragung:
Bei der Kommunikation zwischen Ihrem Rechner und S-Internet Banking werden alle Daten verschlüsselt. Dies wird durch ein komplexes Verfahren sichergestellt, das auf symmetrischen und asymmetrischen Verschlüsselungsprinzipien beruht. Der verwendete Schlüssel ist nur Ihrem Rechner und dem S-Internet Banking Rechner bekannt. Für Unbefugte sind die verschlüsselten Nachrichten lediglich eine scheinbar zufällige Folge von Zeichen. Selbst wenn jemand die Datenleitungen abhören sollte, ist ausgeschlossen, dass verwertbare Informationen ausfindig gemacht werden können.

Datenintegrität bei der Datenübertragung:
Da aufgrund der Verschlüsselung niemand außer Ihnen und dem S-Internet Banking System die Daten entschlüsseln kann, kann auch niemand diese Nachrichten gezielt verändern. Wahllose Änderungen einer Nachricht werden durch Verwendung des Secure-Socket-Layer-Protokolls (SSL) im S-Internet Banking System ausgeschlossen. SSL garantiert die Integrität von Nachrichten durch einen Message Authentication Code (MAC), eine Art Prüfsumme, die zusammen mit der Nachricht übertragen wird. Veränderte Nachrichten werden an einem fehlerhaften MAC erkannt und zurückgewiesen.

Autorisierung von Transaktionen:
Jede Ihrer Transaktionen autorisieren Sie mit Hilfe einer eigenen Transaktionsnummer (TAN). Dadurch wird verhindert, dass Ihre Transaktionen mehrfach ausgeführt werden können.
Wiederholungstransaktionen würden vom S-Internet Banking zurückgewiesen, da die TAN nur für eine einzige Transaktion Gültigkeit besitzt. Die dreimalige Eingabe einer ungültigen TAN führt zu einer sofortigen Sperre des Zugangs.