

Inhalt

Identifikationsmerkmale	1
Das erste Login	1
Sicherheitszertifikate	2
Schutz für Ihren PC/Mac	2
Gefahren im Internet	3
Dialer	4
Spyware	4
Das Wichtigste in Kürze	4
Kontakt RegioNet HotLine	4



Online Banking leicht gemacht

RegioNet – die sichere Bank bei Ihnen zu Hause

Unsere Plattform für Online Banking, *RegioNet*, verfügt über einen sehr hohen Sicherheitsstandard, den wir laufend überprüfen und verbessern. Wir möchten Ihnen nachfolgend einige Informationen und Tipps für ein sicheres Online Banking und für den Umgang mit Ihren persönlichen Identifikationsmerkmalen geben.

Identifikationsmerkmale

Für das Login benötigen Sie drei Identifikationsmerkmale:

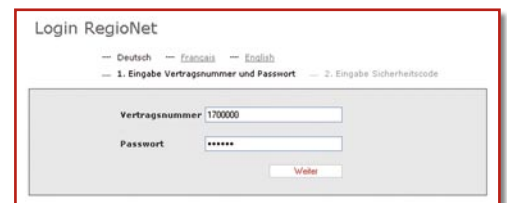
- Ihre persönliche Vertragsnummer
- Ihr persönliches Passwort
- Ihre Sicherheitscodeliste

Nach Vertragsabschluss werden Ihnen diese Informationen persönlich und mit separater Post zugestellt. Das Initialpasswort muss beim ersten Login zwingend durch ein persönliches Passwort ersetzt werden. Das neue Passwort sollte nicht aufgeschrieben oder abgespeichert werden. Wählen Sie ein Passwort, das Sie sich leicht merken können, das aber von Dritten nicht erraten werden kann (mindestens 8- bis maximal 16-stellig, Buchstaben und/oder Zahlen, keine Namen, Telefonnummern, Geburtsdaten etc.). Die Klein- und Grossschreibung ist relevant. Bewahren Sie die Sicherheitscodeliste an einem sicheren Ort auf (nicht kopieren oder im Computer abspeichern). Bei Verlust Ihrer Sicherheitscodeliste melden Sie sich umgehend bei der RegioNet HotLine.

Das erste Login

Mit RegioNet arbeiten Sie unter Windows, Mac OS oder Linux ohne vorherige Programminstallation. Sie loggen sich einfach über den Internet-Browser ins RegioNet ein, wo immer Ihnen ein Computer zur Verfügung steht. Im ersten Login-Fenster werden Sie aufgefordert, Ihre Vertragsnummer und Ihr persönliches Passwort

einzugeben. Achten Sie auf die Klein- und Grossschreibung bei der Eingabe des Passwortes.




Im zweiten Login-Fenster geben Sie den Sicherheitscode ein. Vergewissern Sie sich vor der Eingabe des Sicherheitscodes, dass folgende Angaben angezeigt werden:

- Name des Vertragsinhabers
- Angaben zum letzten Login
- Aktuelle Sicherheitscode-Position

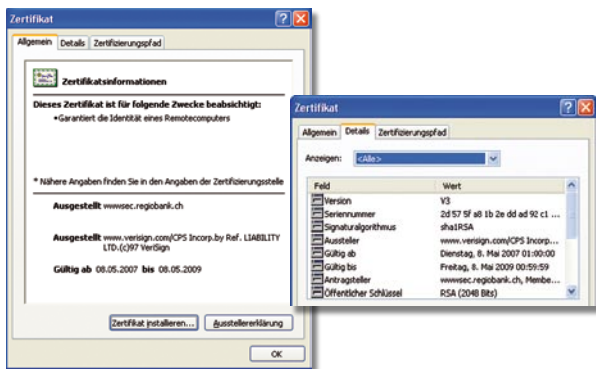


Werden diese Angaben nicht angezeigt, loggen Sie sich nicht ein! Wenden Sie sich an unsere RegioNet HotLine. Prüfen Sie die Echtheit des Sicherheitszertifikates, bevor Sie Ihre persönlichen Informationen auf der Loginseite eingeben.

Sicherheitszertifikate

Um sicherzustellen, dass Sie sich auf der Loginseite von RegioNet befinden, überprüfen Sie das Sicherheitszertifikat im Browser. Geben Sie keine Ihrer persönlichen Informationen auf der Loginseite ein, bevor Sie das Sicherheitszertifikat nicht wie folgt überprüft haben: Unsere Login-Seite ist im SSL-Verfahren verschlüsselt. (https://...). Dies wird durch ein geschlossenes Schloss  in der Statusleiste des Browsers symbolisiert. Hier kann auch das Zertifikat abgerufen und überprüft werden.

1. Offizielle Internetadresse (URL) von RegioNet.
Ein Merkmal ist die SSL-Verschlüsselung (https://wwwsec.regiobank.ch)
2. Geschlossenes Schloss: Diese Seite ist 128-bit verschlüsselt.
3. Die Regiobank Solothurn AG als Inhaberin der Seite ist aufgrund des Sicherheitszertifikates eindeutig identifizierbar.



Schutz für Ihren PC/Mac

Wer seine Daten nicht schützt, erleichtert es Hackern, bei der Datenübertragung mitzulesen, Daten zu verändern oder sogar zu löschen. Wir empfehlen Ihnen deshalb, auch bei Ihrem PC/Mac Schutzmassnahmen zu treffen, die einen Angriff auf Ihren Rechner verhindern oder zumindest das Risiko erheblich minimieren. Zum Grundschutz Ihres PCs oder Mac gehört mindestens:

- der Einsatz eines aktuellen Virencanners
- die Installation einer Personal Firewall
- das regelmässige Einspielen der Sicherheits-Updates Ihrer Browser- und Betriebssystem-Software.

Virencanner

Da fast täglich neue Computerviren entdeckt werden, empfehlen wir den Einsatz eines leistungsfähigen Virencanners. Damit auch neue Viren erkannt werden können, sollte der Virencanner permanent aktualisiert werden.

Personal Firewall

Gegen Angriffe von aussen bietet die Installation einer persönlichen Firewall zusätzlichen Schutz. Die Aufgabe einer Firewall ist ähnlich wie die einer Brandschutzmauer bei Häusern. Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, werden überprüft, aber auch jene, die ins Netz gestellt werden. Mit folgenden grundlegenden Massnahmen, die sehr einfach umzusetzen sind, beugen Sie missbräuchlichen Zugriffen vor:

- Prüfen Sie mit Hilfe von Viren-Erkennungssoftware (sog. Virencanner) Ihren Rechner regelmässig auf Viren.
- Lassen Sie im Hintergrund immer einen Virenwächter laufen, der Downloads und E-Mail Anhänge bereits beim Herunterladen aus dem Internet prüft.
- Aktualisieren Sie den Virencanner regelmässig, nur so findet er auch neue Viren.
- Bei den Programmen, die Sie auf Ihrem PC installieren, setzen Sie bitte nur Original-Software ein. Bitte achten Sie darauf, die Software aus einer vertrauenswürdigen Quelle zu beziehen.
- Aktualisieren Sie regelmässig Ihre Betriebssystem- und Browsersoftware. Auf den Homepages der Anbieter werden jeweils die aktuellen Sicherheitspatches und -updates angeboten.
- Öffnen Sie keinesfalls Dateianhänge von E-Mails, die Sie nicht angefordert haben und deren Absender Ihnen unbekannt ist.
- Sichern Sie häufig Ihre Daten und Dokumente.
- Konfigurieren Sie Ihre Firewall so, dass nur Ports (Zugangsportale zum Internet) geöffnet sind, die Sie benötigen. Beispiele für Portfreigaben: 80 (http) fürs Surfen, 443 (https) für Internetbanking und 110 (POP3) für E-Mail-Kommunikation.
- Rufen Sie während dem Arbeiten mit RegioNet keine fremden Internetseiten auf. Dies gilt nicht für Links, die Ihnen innerhalb von RegioNet vorgegeben werden.
- Schalten Sie Warnungen und Meldungen nicht einfach aus, sondern lesen Sie diese vor dem Bestätigen.



Gefahren im Internet

Gefahren lauern überall – auch im Internet. Wer seine Daten und seinen Computer aktiv schützt, minimiert das Risiko eines Hacker- oder Virengriffes erheblich.

Viren sind...

Programmteile, die sich selbst vervielfältigen können und sich an andere Programme (oder Dateien) hängen. Die infizierte Datei dient dabei als «Wirt», mit dem der Virus weiter verbreitet wird. Ihr PC kann sich infizieren, wenn Sie Dateien aus dem Internet auf Ihren Rechner laden, aber auch über Disketten, USB-Sticks oder CD-ROMs auf Ihren PC gelangen. In jeder ausführbaren Datei, wie zum Beispiel *.exe oder *.com, kann sich ein Virus verstecken. Auch Textdokumente vom Typ *.doc oder Tabellen vom Typ *.xls können virenverseucht sein.

Ein Trojaner ist...

ein scheinbar nützliches Programm verbirgt im Innern ein anderes Programm, das unbemerkt eindringt und sich auf dem PC installiert. So können beispielsweise Passwörter und andere vertrauliche Daten ausgespäht, verändert, gelöscht oder bei einer Daten-

übertragung an den Angreifer verschickt werden. Dieser «Datendiebstahl» bleibt in der Regel unbemerkt, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt. Anders als Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

Des Weiteren gibt es auch wesentlich «klügere» Trojanische Pferde, die sich hinter einem durchaus brauchbaren Programm verbergen. Wird das Programm installiert, kann es oft Monate dauern, bis ein Anwender bemerkt, dass sich ein schädliches Programm auf seinem System befindet.

Viele Trojaner richten sich auf den Systemen so ein, dass sie bei jedem Systemstart ebenfalls gestartet werden und ständig im Hintergrund mitlaufen. Andere Trojanische Pferde starten erst, wenn ein bestimmter Vorgang (Start eines anderen Programmes) auf dem System stattfindet.

Wie schützen Sie sich gegen Viren und Trojaner?

- Verwenden Sie eine aktuelle Antiviren-Software. Aktualisieren Sie den Virens scanner regelmässig.
- Verwenden Sie eine Personal Firewall.

Phishing E-Mails

Das Wort setzt sich aus «Password» und «fishing» zusammen. Gemeint ist damit «nach Passwörtern angeln». Phishing-Betrüger fälschen E-Mails und auch Internetseiten von Banken, um unachtsame Bankkunden dazu zu verleiten, vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern preiszugeben. Dabei erhält der Kunde eine E-Mail mit dem gefälschten Absender seiner Bank. In dieser E-Mail wird der Kunde entweder direkt aufgefordert seine Vertragsnummer, sein persönliches Passwort und den nächsten Sicherheitscode in der Rückantwort anzugeben oder die E-Mail verlinkt auf eine gefälschte Internetseite, die das Aussehen der offiziellen Banken-Homepage hat. Als seriöse Bank getarnt, gelangen Phishing-Betrüger so an die Daten argloser Kunden.

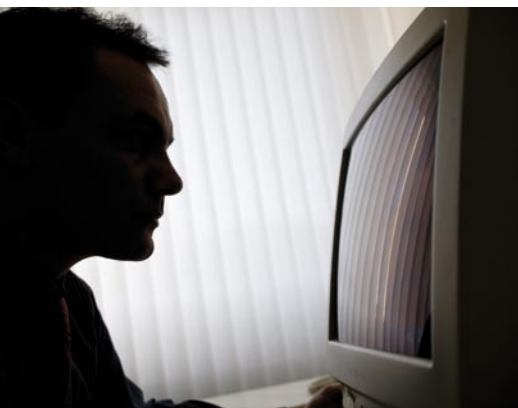
Wie können Sie sich vor Phishing-Mails schützen?

- Verlassen Sie sich nicht auf das Aussehen der Webseite, sondern prüfen Sie deren Echtheit.
- E-Mails sind in der Regel unverschlüsselt und können mitgelesen werden. Vermeiden Sie deshalb, persönliche Daten in einem E-Mail zu versenden.
- Teilen Sie auch vermeintlich seriösen Absendern nie persönliche Daten, etwa zu Ihrer Bankverbindung, per E-Mail mit. Häufig wird die Absenderkennung einer E-Mail-Nachricht gefälscht, um vom Empfänger persönliche Informationen abzufragen. Diese werden dann, für den Absender nicht erkennbar, an unberechtigte Personen versandt.

Die Regiobank Solothurn AG wird von Ihnen unter keinen Umständen irgendwelche vertraulichen Informationen (z.B. Kontonummer, Vertragsnummer, Passwörter, Sicherheitscodes) per E-Mail erfragen oder Sie per E-Mail dazu auffordern, einen Link anzuklicken und sich dort anzumelden. Die Regiobank Solothurn AG wird Ihnen niemals Software per E-Mail zusenden. >

< Fortsetzung von Seite 3

- Bedenken Sie, dass Betrüger Sie mit sogenannten «SCAM E-Mails» (E-Mails mit gefälschten Absenderdaten) dazu verleiten möchten, Dateien (Viren) herunterzuladen oder Webseiten aufzurufen. Begegnen Sie E-Mails mit dem Absender der Regiobank Solothurn AG kritisch: Die Regiobank Solothurn AG kommuniziert mit Ihnen nur mittels E-Mail, wenn Sie dies ausdrücklich wünschen.



- Löschen Sie E-Mails unbekannter Herkunft im Zweifel sofort, ohne diese vorher zu öffnen. Seien Sie besonders vorsichtig bei E-Mails mit Anhängen.

Vishing-Anrufe

Das Wort setzt sich aus «Voice» und «Fishing» zusammen. Dabei versuchen Betrüger mittels VoIP (Voice over IP = Internet Telefonie) oder Telefon den Empfänger irrezuführen. Mittels automatisierten Telefonanrufen wird die Herausgabe von Zugangsdaten, Passwörtern und/oder Kreditkartendaten versucht. Die Betrüger machen sich dabei die niedrigen Kosten der Internettelefonie zu Nutze und rufen mittels Dialer unzählige Telefonnummern an.

Dialer

Dialer, auch Einwahlprogramme genannt, sind kleine Programme, die auf

dem Rechner einen neuen Internetzugang einrichten. Nach dem Download und der Installation auf dem PC wählt sich der Dialer über das Modem oder die ISDN-Karte ins Internet ein. Bei rechtskonformen Einwahlprogrammen geschieht dies nach ausdrücklicher Bestätigung des Nutzers, bei illegalen Dialer kann die Einwahl auch ohne Bestätigung des Benutzers erfolgen. Eine zu dieser Zeit bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. Die Zugangsnummer, die der Dialer bei der neuen Einwahl benutzt, bestimmt die Höhe der anfallenden Kosten. In der Regel haben Dialer bei Ihnen keine Chance, wenn Sie über ADSL oder Breitband (z.B. GAW) im Internet surfen. Dabei kann sich der Dialer nämlich nicht unbemerkt bei einem fremden Provider einwählen. Doch aufgepasst: Wenn Sie eine ISDN- oder Modem-Kombination benutzen, ist kein Schutz vorhanden. Dann kann sich ein Dialer unbemerkt einschleichen. Prüfen Sie vor jedem Dial-up zu Ihrem Provider, ob die angewählte Nummer korrekt erscheint. Nur so können Sie verhindern, dass ein unbemerkter Dialer sich bei teuren Provider-Nummern (0900er) einwählt.

Spyware

Mit Spyware (Spionageprogramme) bezeichnet man Programme, die Informationen über den PC und das Online-Verhalten des Anwenders ohne dessen Wissen an Datenbanken übermitteln. Die Empfänger der Informationen können dann die Gewohnheiten des Anwenders beim Surfen und beim Einkaufen nachvollziehen. Meistens richten sich Spionageprogramme während dem Installieren von Shareware- oder Freeware-Programmen auf Ihrem Computer ein. Schutz bieten die meisten Virens Scanner, welche auch Anti-Spionage sicherstellen.

Das Wichtigste in Kürze

Schützen Sie Ihren Computer

- mit einem aktuellen Virenscanner;
- mit einer Firewall;
- mit regelmässigen Updates Ihrer Browser- und Betriebssystem-Software.
- Löschen Sie E-Mails unbekannter Herkunft im Zweifel sofort, ohne diese vorher zu öffnen und seien Sie besonders vorsichtig bei E-Mails mit Anhängen.
- Teilen Sie auch vermeintlich seriösen Absendern nie persönlichen Daten mit (z.B. Bankdaten, Identifikationsmerkmale für das RegioNet-Login, Kreditkartenangaben).

Mit diesen Vorkehrungen können Sie ohne Bedenken Ihre Konti / Depots mit RegioNet bewirtschaften.

Kontakte RegioNet

RegioNet HotLine
032 624 15 55

Montag bis Freitag
08:00 bis 21:00 Uhr

Samstag
08:00 bis 12:00 Uhr

Sonn- und allg. Feiertage
geschlossen

ebanking@regiobank.ch