

Das Internet ist ein offenes Kommunikationssystem, das weltweit vernetzt ist. Die Bank Thalwil gewährt die bestmöglichen Sicherheitsvorkehrungen. Mit entsprechenden Vorsichtsmassnahmen können Sie das Restrisiko Ihrerseits minimieren, sodass Ihre Daten vor fremden Zugriffen geschützt sind. Wir bitten Sie selbst einen Beitrag zu Ihrer Sicherheit zu leisten, indem Sie folgende Empfehlungen befolgen.

Internet allgemein

- Virensoftware und Firewall
Benützen Sie in jedem Fall auf Ihrem Computer eine aktuelle Virensoftware und Firewall.
- Betriebssystem und Browser
Bitte halten Sie Ihr Betriebssystem und Ihr Internet-Browser in Bezug auf neue Sicherheits-Updates stets auf dem aktuellen Stand.
- E-Mails
Öffnen Sie keine E-Mails aus unbekannter Herkunft oder mit nicht erwarteten Anhängen.
- Fremde Software
Installieren Sie keine Programme von nicht vertrauenswürdigen Anbietern auf Ihrem Computer.

NetBanking

- Anmelden im NetBanking
Beenden Sie sämtliche Aktivitäten im Internet bevor Sie sich im NetBanking der Bank Thalwil anmelden. Melden Sie sich bitte immer über den dafür vorgesehenen Link der Bank Thalwil an. Setzen Sie eine Virenschutzsoftware ein und aktualisieren Sie diese regelmässig, insbesondere bevor Sie Dateien aus dem Internet herunterladen.
- Passwort und Streichliste
Ändern Sie Ihr Passwort sofort nach Erhalt. Schreiben Sie es nirgends auf und speichern Sie es auch nicht auf Ihrem Computer ab. Wählen Sie ein Passwort, das Sie leicht behalten können, aber von anderen nicht erraten werden kann, keine Namen, Telefonnummern, Automarken, Geburtstage etc. Bewahren Sie Ihre Streichliste an einem sicheren Ort auf. Speichern Sie die Streichliste niemals auf Ihrem Computer ab.
- E-Mails (Phishing-Mails)
Reagieren Sie auf keine Aufforderung via E-Mail und Links Ihre Sicherheitsmerkmale einzugeben, auch wenn der Absender angeblich die Bank Thalwil sein soll. Loggen Sie sich nur auf der offiziellen NetBanking-Autorisierungsseite der Bank Thalwil ein. Betrügerische E-Mails - sogenannte "Phishing-E-Mails", hergeleitet aus den Wörtern "Password fishing" - haben zum Ziel, die Empfänger zur Preisgabe von persönlichen Sicherheitsmerkmalen auf gefälschten Internetseiten zu verleiten. Die E-Mails und die Internetseiten täuschen einen seriösen Absender vor, um Bankkunden zur Eingabe von eBanking-Passwörtern, PIN-Codes oder Streichlisten-Nummern zu bewegen.
- Zahlungen
Überprüfen Sie nach der Erfassung von Zahlungsdaten nochmals deren Korrektheit online im Menu "Zahlungen / Pendent".
- Abmelden
Beenden Sie Ihre geschützte NetBanking-Session immer mit der dafür vorgesehenen Programmfunktion <Abmelden>, bevor Sie das Browserfenster ganz schliessen. Leeren Sie den Cache des Browsers nach dem Verlassen des NetBanking. Beim Microsoft Internet Explorer wäre dies zum Beispiel unter dem Menu: Extras -> Internetoptionen -> Temporäre Internetdateien -> Dateien löschen.

Bei ungewöhnlichen Fehlermeldungen, insbesondere im Zusammenhang mit Passwörtern und Sicherheitscode, nehmen Sie bitte sofort Kontakt mit uns auf. Falls Sie weitere Fragen zu NetBanking haben wenden Sie sich bitte an uns, wir helfen gerne.