# Sicher im Netz

## Mehr vom Leben

Tipps und Tricks für einen
sicheren Umgang im Internet
und im E-Banking

Nidwaldner
Kantonalbank

# Geschätzte Leserin, geschätzter Leser

Phishing-Mails, Hacking und Malware – diese Erscheinungsformen der Cyberkriminalität stehen für Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets verübt werden. Mit diesen und anderen Mitteln versuchen Betrüger auf Ihrem Computer, Tablet oder Smartphone Viren zu installieren oder über gefälschte Webseiten an Ihre vertraulichen Daten wie Passwörter oder Nutzernamen zu gelangen.

Die Nidwaldner Kantonalbank (NKB) stellt ihren Kundinnen und Kunden ein äusserst zuverlässiges E-Banking nach höchst möglichem Sicherheitsstandard zur Verfügung. Trotzdem sind auch unsere Kunden nicht gefeit vor Cyberattacken im E-Banking. Cyberkriminelle schaffen es immer wieder, die Unachtsamkeit oder das Unwissen der User auszunutzen. Wenn Sie sich bewusst sind, auf was Sie achten und wie Sie sich verhalten sollten, können Sie Schaden- und Betrugsfälle vermeiden.

«eBanking – aber sicher!» (EBAS) von der Hochschule Luzern bietet hier Unterstützung. Mit dieser Broschüre liefern wir Ihnen, liebe Leserinnen und Leser, zusammen mit unserem Partner viel Wissenswertes zum Thema «Sicherheit im Netz» sowie wertvolle Tipps und Tricks, wie Sie Ihr Leben im Netz sicherer gestalten können.

Ihre
Nidwaldner Kantonalbank

# Sicher im E-Banking

## Unser Beitrag

**Verschlüsselte Datenübermittlung**
Kundendaten werden verschlüsselt zu unseren Servern übertragen und können somit von Dritten nicht eingesehen werden.

**Geschützter Datenzugriff**
Mit einem mehrstufigen Loginverfahren schützen wir den Zugang zu Ihren Daten vor unbefugtem Zugriff.

**Transaktionsüberwachung**
Alle übermittelten Kundenzahlungen durchlaufen ein spezielles Regelwerk von Prüfroutinen, bevor sie ausgeführt werden.

**Sichere Datenaufbewahrung**
Schweizer Finanzinstitute verfügen im internationalen Vergleich über einen sehr hohen Sicherheitsstandard. Geschützte Rechenzentren und Sicherheitssysteme gewährleisten, dass die Daten und Finanzen der Kunden sicher aufbewahrt werden.

## Ihr Beitrag

Um Ihren Grundschutz zu gewährleisten, ist es sehr wichtig, dass Sie folgende Punkte beachten:

- Schützen Sie Ihre Geräte mit den «5 Schritten für Ihre digitale Sicherheit» (www.ebas.ch/5steps)
- Speichern Sie die Zugangsdaten nicht auf Ihrem Mobilgerät und geben Sie diese verdeckt ein.
- Verwenden Sie nur verschlüsselte WLAN-Netze.
- Verwenden Sie niemals einen E-Banking-Link, der Ihnen per E-Mail zugestellt wurde, sondern tippen Sie diesen immer manuell in der Adresszeile Ihres Browsers ein.
- Achten Sie darauf, dass Sie sicher mit Ihrem Finanzinstitut verbunden sind («https» und Schlosssymbol in der Adresszeile).
- Nutzen Sie während des Arbeitens mit der Bankapplikation (z. B. E-Banking) keine anderen Internetseiten.
- Loggen Sie sich am Ende der Session korrekt aus und leeren Sie Ihren Browser-Cache.
- Verwenden Sie ein sicheres Passwort (siehe Tipps auf der folgenden Doppelseite).
- **Nehmen Sie bei ungewöhnlichen Fehlermeldungen und Vorgängen sowie bei nicht erfolgreicher Anmeldung umgehend Kontakt mit uns auf (041 619 22 22).**

# Sicherer Umgang mit Passwörtern

Mit einem sicheren Passwort schützen Sie Ihre Daten vor unerwünschtem Zugriff. Folgende Merkpunkte sollten Sie dabei beachten:

- Notieren Sie Ihre Passwörter niemals auf Notizzettel. Kleben Sie keine diesbezüglichen Informationen an den Monitor, unter die Tastatur oder an andere gut sichtbare Stellen.
- Wenn Sie das Gefühl haben, dass Ihr Passwort nicht mehr sicher oder vertraulich ist, ändern Sie es sofort.
- Verwenden Sie keine Passwörter mit persönlichen Informationen, wie z.B. Ihre Telefonnummer, den Vornamen Ihrer Frau oder Ihres Mannes, das Geburtsdatum Ihrer Kinder, Ihr Autokennzeichen usw.
- Verwenden Sie keine selbsterklärenden Passwörter: Sieht man zufällig ein fremdes Passwort, so darf es nicht offensichtlich sein, worum es sich handelt, z. B. MuellerMai01 («BenutzernameMonatJahr»).
- Speichern Sie in Ihrem Browser keine Passwörter für den Zugriff auf geschützte Webseiten ab. Browser verwalten diese Passwörter in der Regel nicht genügend sicher.

Merken Sie sich Ihre Passwörter oder bewahren Sie sie an einem sicheren Ort – zum Beispiel in einem digitalen Passwort-Tresor – auf. Nachfolgend finden Sie eine Auswahl von Anbietern solcher Tresore:

- SecureSafe (www.securesafe.com)
- Password Safe (www.passwordsafe.de)
- 1Password (www.1password.com)
- KeePass (www.keepass.info)

**Beachten Sie:** Den Zugriff auf einen solchen Tresor müssen Sie ebenfalls mit einem Passwort sichern.

# So erstellen Sie ein sicheres Passwort

Kurze, nicht komplexe Passwörter sind unsicher, da sie von einem Angreifer in wenigen Minuten geknackt werden können. Insbesondere Nachnamen, Namen von Kindern oder Haustieren, Wörter einer bekannten Sprache, Tastaturfolgen (z. B. «asdfg» oder «45678») sowie Geburtsdaten sollten nicht verwendet werden. Am besten eignen sich willkürliche, mindestens 10-stellige Kombinationen aus Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Verwenden Sie für verschiedene Angebote verschiedene Passwörter, die Sie niemandem bekanntgeben.

Nachfolgend stellen wir Ihnen zwei Varianten vor, wie Sie auf einfache Art und Weise ein sicheres Passwort erstellen, das Sie sich auch merken können:

1. Wählen Sie einen leicht einprägsamen Satz und bilden Sie Ihr Passwort mit den jeweiligen Anfangsbuchstaben und Ziffern:
   **Meine Tochter Tamara hat am 19. Januar Geburtstag!**

   So entsteht ein Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können:
   **MTTha19.JG!**

2. Wählen Sie einen leicht einprägsamen Begriff aus:
   **Fasnacht**

   - Fügen Sie vor oder mitten im ausgewählten Begriff Zahlen und Sonderzeichen, wie z.B: % & ? £ $, ein.
   - Nach dem Sonderzeichen fahren Sie GROSS fort.
   - Am Ende des Begriffes setzen sie eine Zahl ein.

   So entsteht ein Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können:
   **%Fas&Nacht23**

**Beachten Sie:** Diese zwei Beispiele dienen der Veranschaulichung. Verwenden Sie keinesfalls exakt diese Passwörter.

# In fünf Schritten zu erhöhter Sicherheit

Schützen Sie sich und Ihr System mit den folgenden einfachen Handlungsempfehlungen.

**1 – Sichern der Daten**
Wie wertvoll sind Ihre Daten? Sichern Sie diese regelmässig auf externe Medien oder online. Kontrollieren Sie, ob Ihre Daten tatsächlich gespeichert worden sind.

**2 – Schützen mit Virenschutzprogramm**
Welche Viren gelangen auf Ihren Computer, Ihr Tablet oder Ihr Smartphone? Praktisch keine, wenn Sie ein Virenschutzprogramm installiert haben. Konfigurieren Sie das Programm so, dass es automatisch und regelmässig seine Virenliste aktualisiert und damit auch neue Bedrohungen erkennt.

**3 – Überwachen dank Firewall**
Ihr Computer oder Ihre mobilen Geräte öffnen im Internet viele unsichtbare Türen. Wenn Sie eine Firewall installieren, werden diese zuverlässig geschlossen. Zusätzlich überwacht die Firewall automatisch die Aktivitäten im Internet und alarmiert Sie bei Problemen.

**4 – Vorbeugen mit Software-Updates**
Wer kann die Sicherheit besser gewährleisten als die Hersteller all Ihrer Programme? Warten Sie Ihre Programme und Apps. Richten Sie diese so ein, dass Updates automatisch heruntergeladen und installiert werden.

**5 – Aufpassen und wachsam sein**
Wie verhalten Sie sich verantwortungsbewusst? Indem Sie Ihre Geräte (z. B. Computer, Tablet oder Smartphone) mit je einem cleveren Passwort schützen. Wenn Sie gezielt entscheiden, wo und wann Sie Ihre Informationen im Internet preisgeben. Und wenn Sie dem Internet – mit gesundem Misstrauen – nicht alles glauben.

Detaillierte Informationen erhalten Sie unter **www.ebas.ch/5steps**.

# Glossar

**Firewall**
Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen durch Trojaner, Phishing-Attacken oder weiteren schädlichen Programmen schützt.

**Hacker**
Hacker sind Personengruppen, die dank ihren ausgezeichneten Programmierkenntnissen in Computersysteme eindringen. In der öffentlichen Wahrnehmung haben sich zwei gegensätzliche Ausprägungen des Begriffs entwickelt. Die gesetzestreuen «White-Hat»-Hacker setzen ihre Fähigkeiten dafür ein, Sicherheitslücken aufzuzeigen und zu beseitigen. Die «Black-Hat»-Hacker wiederum handeln mit krimineller Energie und beabsichtigen zum Beispiel, das Zielsystem zu beschädigen oder Daten zu stehlen. Sie werden auch als Cracker bezeichnet.

**Malware**
Malware sind Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Sie werden auch Schadprogramme oder Schadsoftware genannt.

**Phishing**
Phishing (engl. Angeln) beschreibt die Technik, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

**Trojaner**
Als Trojanisches Pferd – im EDV-Jargon auch Trojaner genannt – bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine unerwünschte und schädliche Funktion ausführt. Trojaner zählen zur sogenannten Malware.

Weitere Begriffserklärungen zum Thema Informationssicherheit finden Sie unter **www.ebas.ch/glossar**.

# Kontakt

**Nidwaldner Kantonalbank**
**Stansstaderstrasse 54**
**6370 Stans**
**Telefon 041 619 22 22**
**info@nkb.ch**
**nkb.ch/cyber**

Folgen Sie uns auf Facebook und Instagram.
Sie finden uns auf Facebook unter www.facebook.com/nkb.ch und auf Instagram unter «nkb.ch».

07.2018 Sicherheit im Netz – Änderungen und Irrtümer vorbehalten