**Wichtiger Sicherheitshinweis**

Es tut uns leid: Im Zusammenhang mit einem Sicherheitsvorfall bei unserem Buchungstechnologie-Dienstleister HotelNetSolutions aus Berlin könnten Daten zu Ihrer Buchung bei uns unberechtigt abgerufen worden sein. Die identifizierte Schwachstelle wurde am **19. September 2026 geschlossen**.

HotelNetSolutions hat einen **externen Cybersecurity-Spezialisten ausgewählt**; der Umfang der **unabhängigen Untersuchung und Sicherheitsprüfung wird derzeit abgestimmt**. Der Vorfall wurde dem **Landeskriminalamt** gemeldet.

Kriminelle nutzen Buchungsinformationen für sehr glaubwürdig wirkende Nachrichten, etwa zu einer Gästeregistrierung, einem Online-Check-in oder einer zusätzlichen Zahlung.

**Wichtig: Auch korrekte Buchungsdaten sind kein Echtheitsbeweis.** Eine Nachricht mit Ihrem Namen, Reisezeitraum oder Ihrer Buchungsnummer muss nicht tatsächlich von uns oder einem von uns eingesetzten Dienst stammen.

**So kommunizieren wir mit Ihnen**

Wir verwenden keinen Online- oder Pre-Check-in und keine separate digitale Gästeregistrierung vor der Anreise.

Digitale Zahlungsaufforderungen erfolgen bei uns ausschließlich über **Nexi Group** unter **nexigroup.link**.

Unsere E-Mails erhalten Sie von **info@seeblick** oder von **res@seeblick.ch**. Das kann Ihnen bei der Einordnung helfen. Ein bekannter Absender allein beweist jedoch nicht, dass eine Nachricht tatsächlich von uns stammt, denn Absenderangaben lassen sich fälschen.

Wenn eine Nachricht davon abweicht oder Sie unsicher sind, verwenden Sie den enthaltenen Link bitte nicht. Prüfen Sie die Nachricht über unsere offiziellen Kontaktdaten – unter **+41 33 655 60 80** oder über unsere offizielle Website www.seeblick.ch – und nicht über Kontaktdaten aus der Nachricht selbst.

Das gilt auch nach Ihrer Abreise. Aktuell werden bereits bekannt gewordene Buchungsinformationen etwa für E-Mails zu angeblichen Nachzahlungen oder Rückerstattungen genutzt, die auf einen Link führen.

Nach aktuellem Kenntnisstand liegen keine Hinweise darauf vor, dass Kreditkarten- oder sonstige Zahlungsdaten über die identifizierte Schwachstelle bei HotelNetSolutions abgeflossen sind.

Haben Sie auf einer verdächtigen Seite Zahlungsdaten eingegeben, wenden Sie sich bitte umgehend an Ihre Bank oder Ihren Kartenanbieter.

Mit freundlichen Grüßen

**Strandhotel Seeblick AG**

**Häufige Fragen zu verdächtigen Nachrichten**

Die identifizierte Schwachstelle bei HotelNetSolutions wurde am **19. September 2026 geschlossen**. HotelNetSolutions hat zusätzlich einen **externen Cybersecurity-Spezialisten ausgewählt**; der Umfang der **unabhängigen Untersuchung und Sicherheitsprüfung wird derzeit abgestimmt**. Der Vorfall wurde dem **Landeskriminalamt** gemeldet.

**Sind Nachrichten vor meiner Anreise grundsätzlich verdächtig?**

Nein. Nachrichten vor der Anreise sind nicht automatisch verdächtig. Entscheidend ist, ob sie zu den Diensten und Internetadressen unseres Hotels gehören.

Digitale Zahlungsaufforderungen erfolgen bei uns ausschließlich über **Nexi Group** unter **nexigroup.link**.

Wir verwenden keinen Online- oder Pre-Check-in und keine separate digitale Gästeregistrierung vor der Anreise. Eine entsprechende Aufforderung gehört daher nicht zu unserem regulären Ablauf.

Wenn Sie unsicher sind, kontaktieren Sie uns bitte direkt unter **+41 33 655 60 80** oder über unsere offizielle Website www.seeblick.ch.

**Woran erkenne ich eine betrügerische Nachricht?**

Leider nicht immer zuverlässig. Die aktuell bekannten Betrugsnachrichten können echte Angaben zu Ihrer Buchung enthalten, zum Beispiel Ihren Namen, Reisezeitraum oder Ihre Buchungsnummer.

**Auch korrekte Buchungsdaten sind deshalb kein Beweis dafür, dass eine Nachricht tatsächlich von uns stammt.**

Prüfen Sie insbesondere, ob der verwendete Dienst und die Internetadresse zu den oben genannten offiziellen Wegen unseres Hotels passen.

Im Zweifel verwenden Sie bitte nicht die Kontaktdaten aus der fraglichen Nachricht, sondern kontaktieren Sie uns direkt unter **+41 33 655 60 80** oder über unsere offizielle Website www.seeblick.ch.

**Ich habe eine verdächtige Nachricht erhalten. Was soll ich tun?**

Öffnen Sie den enthaltenen Link im Zweifel nicht und nehmen Sie darüber keine Zahlung vor.

Bewahren Sie die Nachricht zunächst auf und kontaktieren Sie uns unter **+41 33 655 60 80** oder per E-Mail an **res@seeblick.ch**. Wir prüfen gerne, ob die Nachricht tatsächlich von uns oder einem von uns verwendeten Dienst stammt.

**Ich habe auf den Link geklickt. Was soll ich tun?**

Wenn Sie **keine Daten eingegeben, keine Datei heruntergeladen und keine App installiert** haben, schließen Sie die Seite und verwenden Sie den Link nicht weiter.

Bewahren Sie die Nachricht zunächst als möglichen Beleg auf.

Wenn etwas heruntergeladen oder installiert wurde oder sich Ihr Gerät anschließend ungewöhnlich verhält, lassen Sie das Gerät sicherheitstechnisch prüfen.

**Ich habe ein Passwort oder Zugangsdaten eingegeben. Was soll ich tun?**

Ändern Sie das betroffene Passwort möglichst sofort über die **offizielle Website oder App des jeweiligen Dienstes** – nicht über den Link aus der Nachricht.

Wenn möglich:

- beenden Sie aktive Sitzungen,
- prüfen Sie das Konto auf unbekannte Änderungen,
- ändern Sie dasselbe Passwort auch bei anderen Diensten, falls Sie es dort ebenfalls verwenden,
- aktivieren Sie eine Zwei-Faktor-Authentifizierung, sofern verfügbar.

**Ich habe Kreditkarten- oder Bankdaten eingegeben. Was soll ich tun?**

Kontaktieren Sie **unverzüglich Ihre Bank oder Ihren Kartenanbieter** und erklären Sie, dass die Daten möglicherweise auf einer betrügerischen Website eingegeben wurden.

Ihre Bank beziehungsweise Ihr Kartenanbieter kann beurteilen, welche weiteren Maßnahmen erforderlich sind.

Kontrollieren Sie anschließend Ihre Umsätze auf Vorgänge, die nicht von Ihnen stammen.

**Ich habe bereits bezahlt. Was soll ich tun?**

Kontaktieren Sie **sofort Ihre Bank oder den verwendeten Zahlungsdienstleister** und fragen Sie, ob die Zahlung noch gestoppt, zurückgerufen oder reklamiert werden kann.

Bewahren Sie möglichst folgende Informationen auf:

- die ursprüngliche Nachricht,
- Absender beziehungsweise Telefonnummer,
- Link oder Internetadresse,
- Screenshots,
- Zahlungsbeleg.

Bitte informieren Sie auch uns per E-Mail an **res@seeblick.ch**, damit wir den Fall dokumentieren können.

**Können solche Nachrichten auch nach meinem Aufenthalt kommen?**

Ja. Aktuell treten auch nach der Abreise Phishing-E-Mails auf, die sich auf den Hotelaufenthalt beziehen.

Dabei geht es beispielsweise um angebliche Nachzahlungen oder Rückerstattungen und die Aufforderung, einem Link zu folgen.

Wenn eine solche Forderung angeblich von uns stammt und Sie unsicher sind, kontaktieren Sie uns bitte direkt unter **+41 33 655 60 80** oder über unsere offizielle Website www.seeblick.ch.

**Sind meine Kreditkarten- oder Zahlungsdaten bei HotelNetSolutions abgeflossen?**

Nach aktuellem Kenntnisstand liegen **keine Hinweise darauf vor, dass Kreditkarten- oder sonstige Zahlungsdaten über die identifizierte Schwachstelle bei HotelNetSolutions abgeflossen sind.**

Davon zu unterscheiden sind Zahlungs- oder Zugangsdaten, die ein Gast anschließend selbst auf einer betrügerischen Website eingegeben hat.

**Muss ich meine Reservierung ändern oder neu buchen?**

Nein. Eine verdächtige Nachricht bedeutet nicht automatisch, dass mit Ihrer Reservierung etwas nicht stimmt.

Wenn Sie unsicher sind, prüfen wir Ihren Buchungsstatus gerne direkt für Sie unter **+41 33 655 60 80** oder per E-Mail an **res@seeblick.ch**.