Wi-Fi im Hotel: Gute Reflexe vor dem Einloggen auf Reisen

By Floriane

Es ist zu einem echten Problem geworden: Auf unseren Reisen ist das Internet heutzutage fast unverzichtbar. Da wir oft aus der Ferne arbeiten und viel Zeit damit verbringen, unsere Reiserouten online zu planen, verbinden wir uns mit vielen Wi-Fi-Netzwerken: in Hotels, Cafés, Bahnhöfen und Flughäfen.

Mit der Zeit haben wir uns daher einige Gewohnheiten angeeignet. Bevor wir uns mit einem öffentlichen Wi-Fi verbinden, überprüfen wir immer den **Namen des Netzwerks**, vermeiden bestimmte **sensible Aktionen** und **aktivieren** vor allem **fast immer unser VPN**.

Mit ein paar einfachen Schritten können Sie das Wi-Fi in Ihrem Hotel oder anderswo nutzen, ohne sich unnötig zu exponieren, und mit einem leichteren Gewissen weiterreisen.

Warum Wi-Fi im Hotel ein Minimum an Wachsamkeit erfordert

Wenn Sie sich mit dem Wi-Fi eines Hotels verbinden, treten Sie in der Regel einem Netzwerk bei, das von vielen anderen Personen genutzt wird.

In den meisten Fällen läuft alles reibungslos. Man **checkt seine E-Mails**, plant **den nächsten Tag, schickt ein paar Nachrichten** und denkt nicht mehr daran.

Ein **öffentliches Netzwerk ist** jedoch gefährdeter **als eine private Verbindung**. Es kann schlecht konfiguriert oder unsicher sein oder einfach von Personen genutzt werden, die Sie nicht kennen. Es ist gerade diese „gemeinsame“ Seite, die ein wenig Vorsicht erfordert.

Das bekannteste Risiko ist **das Abfangen von Daten**. Einfach ausgedrückt kann eine Person mit böswilligen Absichten versuchen, sich zwischen Ihr Gerät und das Netzwerk zu stellen, um zu beobachten, was in Ihrem Gerät passiert. Dies wird oft als „Man-in-the-Middle“-Angriff bezeichnet, aber Sie müssen sich den technischen Begriff nicht merken. Was Sie verstehen müssen, ist, dass ein öffentliches Wi-Fi nicht immer den gleichen Grad an Privatsphäre bietet wie eine persönliche Verbindung.

Heute sind viele Websites glücklicherweise besser gesichert als früher, dank HTTPS, dem berühmten kleinen Vorhängeschloss, das man im Browser sieht. Das ist eine gute Sache. Dies bedeutet jedoch nicht, dass Sie überall blindlings klicken sollten, insbesondere wenn Sie sich von einem unbekannten Netzwerk aus einloggen.

Wi-Fi im Hotel: Gute Reflexe vor dem Einloggen auf Reisen

Wi-Fi im Hotel: Gute Reflexe vor dem Einloggen auf Reisen

Falsche Wi-Fi-Netzwerke: Die einfache Falle

Es gibt ein weiteres sehr konkretes Risiko auf Reisen: falsche Wi-Fi-Hotspots, wie sie in einigen Flughäfen gefunden wurden.

Das Prinzip ist recht einfach. Eine Person mit bösen Absichten richtet ein Wi-Fi-Netzwerk mit einem glaubwürdig klingenden Namen ein, um Reisende dazu zu bringen, sich ohne viel nachzudenken mit dem Netzwerk zu verbinden. Sobald Sie sich mit dem falschen Netzwerk verbunden haben, wird Ihr Internetverkehr über einen Zugangspunkt geleitet, den Sie nicht kontrollieren können.

Hier sind einige Beispiele für Namen, die auf den ersten Blick vertrauenswürdig erscheinen:

- Hotel Guest
- Hotel WiFi Free
- NameDeLHotel_Guest
- Internet-Lobby
- Kostenlose Hotel WiFi

Gute Gewohnheiten, die Sie sich vor dem Einloggen aneignen sollten

Überprüfen Sie den genauen Namen des Netzwerks beim Empfang.

> Fragen Sie an der Rezeption nach dem genauen Namen des Wi-Fi-Netzwerks des Hotels.

Bevor Sie sich einloggen, nehmen Sie sich ein paar Sekunden Zeit, um an der Rezeption nach dem offiziellen Namen des Wi-Fi-Netzwerks des Hotels zu fragen. Diese einfache Überprüfung beseitigt das Risiko, auf einen falschen Hotspot zu stoßen.

VPN, unser Sicherheitsreflex auf Reisen

Im Laufe der Jahre ist VPN zu einem unserer Reisewerkzeuge geworden. Zugegeben, nicht das glamouröseste. Es ist nicht so traumhaft wie ein Sonnenaufgang am Strand oder eine vertrauliche Adresse, die man zufällig in einer Gasse findet. Aber in der Praxis macht es uns das Leben wirklich leichter.

Wenn Sie verreisen, gehen Sie überall ins Internet: Hotels, Cafés, Bahnhöfe, Flughäfen, Unterkünfte, Coworking Spaces... Manchmal, um eine Reiseroute abzurufen, manchmal, um Reservierungen zu verwalten, manchmal, um zu arbeiten. Und in diesen Momenten möchte man nicht nur von der Sicherheit des Netzwerks abhängen, in das man sich begibt.

Ein VPN (**Virtual Private Network**) ermöglicht es, die Verbindung zwischen Ihrem Gerät und dem Internet zu verschlüsseln. Einfach ausgedrückt: Es schafft eine Art **sicheren Tunnel**. Selbst wenn Sie das Wi-Fi eines Hotels nutzen, sind Ihre Daten für jemanden, der versucht, sie abzufangen, viel schwerer zu lesen.

Was uns besonders gefällt, ist die automatische Funktion. Sobald die Anwendung installiert ist, müssen **Sie sie nur noch aktivieren, bevor Sie sich mit dem öffentlichen Wi-Fi verbinden.** Sie wählen einen Server aus, warten ein paar Sekunden und nutzen dann das Internet ganz normal.

Warum ein logfreies VPN wählen?

Nicht alle VPNs sind gleich. Wenn es um Reisen und Datenschutz geht, wird ein Punkt oft angesprochen: die Datenaufbewahrungspolitik.

Ein No-Log-VPN bedeutet, dass der Dienst ankündigt, den Browserverlauf seiner Nutzer nicht zu speichern. In der Praxis bedeutet dies, dass er keine detaillierten Aufzeichnungen darüber führt, was Sie online tun.

Dies ist ein wichtiges Kriterium, da die Nutzung eines VPN auch bedeutet, dass Sie dem Anbieter des VPN vertrauen. Es geht also nicht nur darum **, einen zufälligen Anbieter zu installieren**, weil er bei einer Suche als erstes erscheint. Es ist besser, sich die Zeit zu nehmen, um sich seinen Ruf, seine Datenschutzrichtlinien, die Länder, in denen er operiert, die kompatiblen Geräte und die Benutzerfreundlichkeit anzusehen.

Auf Reisen ist ein einfach zu bedienendes VPN am wichtigsten. Denn das beste Sicherheitstool ist das, das man wirklich benutzt. Wenn die Anwendung zu kompliziert, zu langsam oder zu instabil ist, wird sie schließlich deaktiviert. Und dann ist sie nicht mehr nützlich.

Die Kriterien, die unserer Meinung nach am wichtigsten sind :

- eine einfache Anwendung auf Telefon und Computer ;
- eine stabile Verbindung ;
- Eine Politik ohne klare Logs;
- Server in mehreren Ländern;
- eine schnelle Aktivierung ;
- eine gute Kompatibilität mit der Nutzung auf Reisen.

Situationen, in denen wir unser VPN immer aktivieren

Es gibt Zeiten, in denen man sich diese Frage nicht einmal mehr stellt.

> Wenn Sie sich in einem öffentlichen Wi-Fi befinden, wird das VPN automatisch aktiviert.

Dies ist natürlich im **Hotel** der Fall, aber auch auf **Flughäfen** und **Bahnhöfen**. Die langen Wartezeiten zwischen zwei Flügen sind oft der Moment, in dem man den Computer hervorholt, um zwei oder drei Dinge zu erledigen. Flughafennetzwerke sind jedoch stark frequentiert, manchmal offen, manchmal mit ähnlich klingenden Namen. In diesem Zusammenhang wird VPN zu einem echten Grundreflex.

Dasselbe gilt für **Cafés.** Wir lieben es, uns mit einem Computer und einem Getränk irgendwo niederzulassen. In solchen Momenten wird oft die weitere Reise geplant, Fotos sortiert oder auf Nachrichten geantwortet. Aber auch hier wird das Wi-Fi mit allen Gästen um uns herum geteilt.

Sie wird auch in **Coworking Sp** aces aktiviert, wenn Sie mit der Konfiguration des Netzwerks nicht vertraut sind.

Was Sie im öffentlichen Wi-Fi besser nicht tun sollten

Auch wenn Sie ein VPN haben, sollten Sie einige einfache Reflexe beibehalten. Im Wi-Fi eines Hotels, eines Cafés, eines Bahnhofs oder eines Flughafens, hier unsere kleine Checkliste :

- **Verbinden Sie sich nicht mit dem erstbesten Netzwerk**: Sie sollten immer den genauen Namen des Wi-Fi überprüfen, insbesondere in Hotels, indem Sie an der Rezeption nachfragen.
- **Vermeiden Sie es, sensible Dokumente zu versenden**: Reisepass, Personalausweis, Bankunterlagen oder wichtige Geschäftsinformationen.
- **Geben Sie Ihre Bankdaten nicht auf einer zweifelhaften Website** ein: Bevor Sie bezahlen, überprüfen Sie, ob die Website auf **https** eingestellt ist und ob das kleine Vorhängeschloss im Browser erscheint.
- **Vergessen Sie nicht, Ihr VPN zu aktivieren**: Sobald Sie ein öffentliches Wi-Fi benutzen, wird es fast automatisch aktiviert, insbesondere wenn Sie Ihre E-Mails abrufen, eine Fahrt buchen oder sich in ein persönliches Konto einloggen.
- **Vermeiden Sie es, in sensiblen Konten eingeloggt zu bleiben**: Bank,

Versicherung, Verwaltungsbereich, geschäftliche E-Mails… wenn Sie einmal fertig sind, loggen Sie sich aus.

- **Deaktivieren Sie die automatische Wi-Fi-Verbindung**: Dies verhindert, dass das Telefon oder der Computer sich selbstständig mit einem unsicheren Netzwerk verbindet.
- **Aktualisierungen vor der Abreise durchführen**: Telefon, Computer, Browser, wichtige Anwendungen… das ist zu Hause immer einfacher als mit einem launischen Hotel-Wi-Fi.

Unsere einfache Routine vor dem Einloggen auf Reisen

Wenn wir heute in ein Hotel kommen, ist unsere Routine fast immer die gleiche.

Sie fragen an der Rezeption nach dem genauen Namen des Wi-Fi. Sie verbinden sich nur mit dem angegebenen Netzwerk. Aktivieren Sie das VPN auf dem Telefon und dem Computer. Wir überprüfen, ob die verwendeten Websites sicher sind. Und wenn uns etwas seltsam vorkommt, gehen wir lieber über unsere mobile Verbindung.

Es ist keine perfekte Routine, aber sie ist einfach. Und auf Reisen funktioniert sie oft am besten.

Bitte hinterlassen Sie uns unten eine **kurze Nachricht,** wenn Sie hier oder auf Instagram Fragen haben, wir werden Ihnen gerne antworten.