# Keeper Security: 6 Sicherheitstipps für die Urlaubszeit

*Im Sommerurlaub sollte man sich nicht nur vor einem Sonnenbrand schützen, sondern auch vor Cyberrisiken*

**München, 04. Juli 2023** – Die Sommerreisezeit ist in vollem Gange und viele freuen sich über ihren wohlverdienten Urlaub. Doch während Millionen von Menschen voller Freude ihre Reise planen und antreten, schmieden Cyberkriminelle ihre Taktik, wie sie ahnungslose Reisende angreifen oder ausnutzen können. Die Aussichten auf Beute sind verlockend, da sich die potenziellen Opfer während des Urlaubs beispielsweise weit weniger in gesicherten Netzwerken befinden und damit leichter angreifbar sind. Umso wichtiger ist es ein paar grundlegende Sicherheitsaspekte zu beachten, um sensible Daten und Informationen bestmöglich zu schützen. Schon einfache Handlungen wie etwa die Nutzung eines öffentlichen Wi-Fis in Flughäfen, Hotels oder Touristenorten können dazu führen, dass Geräte gehackt werden. Um die Identität, Finanzdaten, sensiblen Dokumente und Passwörter der Reisenden zu schützen, rät Keeper Security folgendes:

**#1 Zeigen Sie in den sozialen Netzwerken nicht Ihren Standort an.**
Das Posten in den sozialen Medien ist die Lieblingsbeschäftigung vieler Reisender, wenn sie einen besonderen Ort besuchen. Das Veröffentlichen des genauen Standorts (inkl. Geotags) während eines Aufenthalts, kann jedoch sehr gefährlich sein, denn sobald der Standort öffentlich bekannt ist, können Sie Cyberkriminelle ins Visier nehmen. Auch wenn Ihnen das als Tourist unwahrscheinlich erscheint, können Kriminelle, die mit der Umgebung gut vertraut sind, Sie leichter finden. Sollten Sie dennoch aus Ihrem Urlaub etwas posten wollen, warten Sie, bis Sie an einen neuen Ort umgezogen sind. Noch besser: Sie heben sich das Posten auf, bis Sie wieder zu Hause sind.

**#2 Vermeiden Sie öffentliches Wi-Fi.**
Auch wenn es schwierig ist, auf Reisen ein zuverlässig sicheres WLAN zu finden, sollte die Sicherheit immer vorgehen. Wenn es möglich ist, sollten Sie es vermeiden, eine riskante Verbindung zu einem öffentlichen WLAN-Netz herzustellen. Der Grund: Sobald ein Gerät mit einem öffentlichem WLAN verbunden ist, können Angreifer einen so genannten MITM-Angriff (Man-in-the-Middle) durchführen, der es ihnen ermöglicht, auf Ihren Browser oder Ihre Apps zuzugreifen und gespeicherte Daten abzurufen. Als allgemeine Faustregel gilt: Öffentliche WLAN-Netze sollten immer gemieden werden.

**#3 Ziehen Sie die Verwendung eines VPN in Betracht.**
Mit einem Virtual Private Network (VPN) sind Sie auf Reisen geschützt, egal von welchem Ort sie sich ins Internet einloggen. Mit einem VPN können Sie nicht nur Ihre Online-Identität schützen und überall auf eine sichere Verbindung zurückgreifen, sondern können auf diese Art und Weise auch eine Bandbreitendrosselung vermeiden.

**#4 Laden Sie wichtige Dokumente zur Absicherung hoch.**
Reisen zu neuen und unbekannten Zielen können durchaus chaotisch sein. Das erhöht die Gefahr, dass wichtige Unterlagen - wie Pässe, Visa, medizinische Dokumente usw. - gestohlen oder verlegt werden. Wenn Sie Kopien dieser wichtigen Dokumente in einem sicheren Passwort-Manager hochladen, haben Sie jederzeit Zugriff auf dieses digitale Backup, für den Fall, dass Dokumente verloren gehen oder gestohlen werden.

**#5 Nehmen Sie niemals Zugangsdaten in Klartext mit auf Reisen.**
Auf Reisen benötigt man immer wieder Zugangsdaten zu digitalen Diensten, beispielswese zum Online-Banking, Reiseveranstalter, zur Krankenkasse oder für Kommunikationsdienste. Selten weiß man alle Zugangsdaten und Passwörter auswendig, weshalb diese irgendwo auf

digitalen oder manuellen Notizen notiert werden. Auf keinen Fall sollten Zugangsdaten auf Mobiltelefonen, Tablets oder gar handschriftlich mitgeführt werden, die jeder, der das Gerät oder den Zettel in die Hände bekommt, lesen und nutzen kann. Speichern Sie alle Zugangsdaten in einem sicheren Passwortmanager – idealerweise in einem, der das Teilen von ausgewählten Zugangsdaten, beispielsweise in der Familie, erlaubt.

**#6 Geben Sie Notfallinformationen an eine vertrauenswürdige Quelle weiter.**
Gehen Sie in puncto Sicherheit noch einen Schritt weiter und teilen Sie wichtige Informationen mit vertrauenswürdigen Personen wie Familienmitgliedern oder Freunden, um sicherzustellen, dass diese im Notfall Zugang haben. Nutzen Sie einen verschlüsselten Dienst wie One Time Share, um Versicherungsinformationen oder Ausweispapiere sicher und zeitlich begrenzt an eine vertrauenswürdige Person weiterzugeben. Auf diese Weise kann Ihre Vertrauensperson im Falle eines medizinischen oder anderen Notfalls Hilfe leisten, ohne dass sensible Informationen per E-Mail, Textnachricht oder Messaging preisgegeben werden müssen.

Lassen Sie es nicht zu, dass Hacker Ihnen den Urlaub verderben. Wer diese sechs Tipps auf seiner Reise befolgt, kann zu einem hohen Maß sicher sein, dass er sich um Aktivitäten von Cyberkriminellen keine Sorgen machen muss.

**Über Keeper Security Inc.**
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwortmanagement, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie mehr unter KeeperSecurity.com.

**Pressekontakt für Keeper in DACH:**
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de