KEEPER | Pressemitteilung

Mit diesen fünf Sicherheitsmaßnahmen lassen sich Cyberbedrohungen während der Urlaubszeit minimieren

Keeper warnt vor Cyberrisiken, die die Online-Sicherheit von Reisenden gefährden können

München, 14. März 2024 – In Zeiten der umfassenden Digitalisierung und Vernetzung gilt es auch während eines Urlaubs oder einer Reise verantwortungsvoll mit der eigenen digitalen Sicherheit umzugehen. Das ist im Prinzip keine neue Botschaft. Allerdings bestätigt eine Studie von Keeper, dass viele Nutzer von Computern, Tablets oder Mobilgeräten noch keinen genügenden Schutz für ihre Passwärter etabliert haben, um den digitalen Zugang zu sensiblen privaten und geschäftlichen Applikationen und Daten sicherzustellen. Weltweit 64 Prozent der Befragten nutzen entweder nur schwache Passwörter oder Variationen von Passwörtern zum Schutz ihrer Online-Konten. Gleichzeitig sind aber 80 Prozent der Datenschutzverletzungen auf kompromittierte Anmeldeinformationen zurückzuführen. Um die digitale Sicherheit auch auf Reisen und in ungeschützten Umgebungen aufrecht zu erhalten, gibt Keeper hilfreiche Tipps – denn die bevorstehenden Oster-, Pfingst- und Sommerferien sind auch Hochsaison für Cyberkriminelle.

Reiselust statt Cyberfrust

Laut einer aktuellen Untersuchung der Stiftung für Zukunftsfragen nimmt die Reiselust der Deutschen weiter zu: Mehr als sechs von zehn Bundesbürgern planen bereits ihren nächsten Urlaub und die Reisefrequenz hat inzwischen das Vor-Corona-Niveau von 61 Prozent erreicht und liegt sogar drei Prozentpunkte über dem Vorjahresniveau. Egal, aus welchem Grund man reist - in jedem Fall kommt der Sicherheit von Online-Konten, persönlichen sowie Finanzdaten eine große Bedeutung zu. Scheinbar harmlose Gewohnheiten wie schlechte Passwörter, das Speichern von Passwörtern in unsicheren Dokumenten oder Tools oder etwa das Veröffentlichen eines Reiseziels in sozialen Medien können dazu führen, dass sensible Informationen oder wichtige Kontendaten von versierten Cyberkriminellen attackiert werden.

Diese fünf Tipps zur Cybersicherheit helfen, sich vor Cyberangriffen zu schützen:

1. Gerätesicherheit steht an erster Stelle

Stellen Sie sicher, dass alle elektronischen Geräte mit den neuesten Sicherheitsupdates und Patches ausgestattet sind. Achten Sie auf wichtige Benachrichtigungen und installieren Sie Updates möglichst umgehend. Am einfachsten ist es, wenn man die automatische Update-Funktion aktiviert. Mit Software-Updates werden nicht nur bestehende Funktionen verbessert, Fehler behoben und die Leistung erhöht, sondern auch Sicherheitslücken geschlossen und neue Sicherheitsmaßnahmen hinzugefügt – deshalb sind sie wichtiger Bestandteil einer Sicherheitsstrategie.

2. Online-Konten bestmöglich schützen

Legen Sie sichere und eindeutige Passwörter fest, die mindestens 16 Zeichen lang sind, keine gängigen Wörter, Muster oder fortlaufende Zahlen enthalten, sondern aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen bestehen. Die Sicherheit eines Kontos lässt sich außerdem durch eine Zwei-Faktor-Authentifizierung (2FA) deutlich verbessern. Diese

zusätzliche Schutzebene stellt sicher, dass selbst bei einer Kompromittierung des Passworts ein unbefugter Zugriff verhindert wird. Erleichterung bietet an dieser Stelle ein Passwort-Manager. Er kann sichere Passwörter erstellen, speichern und automatisch ausfüllen.

3. VPN first - öffentliche Ladestationen und Wi-Fi meiden
Vermeiden Sie öffentliche USB-Ladestationen, um Juice-Jacking-Angriffe zu verhindern. Denn Cyberkriminelle können Malware auf diese Ladestationen laden und damit auf fremde Geräte zugreifen. Zudem sollte das automatische Verbinden von WLAN- und Bluetooth-Verbindung ausgeschaltet sein und öffentliche WLAN-Netzwerke vermieden werden, weil sie meist ungesichert und anfällig für Angriffe sind. Verwenden Sie stattdessen die Hotspot-Funktion Ihres Telefons und nutzen Sie ein virtuelles privates Netzwerk (VPN), um Ihre Verbindung zu verschlüsseln und sich vor Cyber-Bedrohungen zu schützen, wenn Sie von unterschiedlichen Standorten aus auf Ihre Konten zugreifen,

4. Achtsamer Umgang mit den sozialen Medien
Im Umgang mit den sozialen Medien sollte man vorsichtig sein und keine Reisepläne und Urlaubsinformationen veröffentlichen. Die Bekanntgabe eines Standorts in Echtzeit macht Sie zur Zielscheibe von Cyberangriffen und physischen Straftaten. Sie geben nicht nur Ihren Standort und Ihre persönlichen Daten preis, sondern machen Diebe auch darauf aufmerksam, dass Sie nicht zuhause sind. Am besten ist es, wenn Sie diese Informationen nur mit vertrauenswürdigen Kontakten austauschen und Reisedetails erst nach der Rückkehr posten.

5. Für den Notfall: Zugriff auf wichtige Dokumente einrichten
Das Risiko, dass wichtige Finanz-, Ausweis- und andere Dokumente verloren gehen oder gestohlen werden, ist auf Reisen besonders hoch. Reisende sollten sich deshalb Sicherheitskopien wichtiger Karten und Dokumente machen und diese in einen sicheren Passwort-Manager hochladen. Alternativ kann auch ein verschlüsselter Dienst wie One Time Share genutzt werden, um wichtige Informationen sicher an ein Familienmitglied oder eine vertrauenswürdige Person weiterzugeben, damit diese im Notfall darauf zugreifen kann.

"Da die Cyberkriminalität immer und überall präsent ist, ist die Umsetzung robuster Cybersicherheitspraktiken auf Reisen unerlässlich", sagt Darren Guccione, CEO und Mitbegründer von Keeper. "Daher halten wir es für wichtig, den Menschen Tools an die Hand zu geben, die ihre digitale Widerstandsfähigkeit erhöhen. Mit einem sicheren Passwort-Manager können sich Reisende auf ein unbeschwertes und sicheres Reiseerlebnis freuen."

Keeper kennt die dynamische Natur von Cyberbedrohungen und empfiehlt deshalb zusätzlich zur Einhaltung von Best Practices auch die Förderung der digitalen Kompetenz und Bereitschaft, sich mit den Herausforderungen der Cyberkriminalität auseinander zu setzen. Keeper bietet deshalb zahlreiche Wissensbeiträge zu Cybersicherheitsthemen, die von Tipps zu Reisevorbereitungen bis hin zu Cyberangriffen reichen.

###

Über Keeper Security:
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 Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Sie Keeper auf Facebook, Instagram, LinkedIn, X, YouTube

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