



## **Wenn die mobilen Daten baden gehen: Der ultimative Urlaubsscheck für die sichere Nutzung von Smartphone, Tablet & Co.**

*Der Schnappschuss vom Wasserskifahren, die eigene Urlaubs-Playlist für gute Stimmung oder ein kleines Spiel zur Überbrückung – unsere Handys, Tablets und Laptops sind auch im Urlaub immer dabei - und damit auch unsere Software, Hardware und persönlichen Daten. Sophos hat ein paar Tipps zusammengestellt, damit diese alle wieder sicher zuhause ankommen.*

Urlaubszeit bedeutet auch immer viel Organisation und Vorbereitung. Mittlerweile gehören nicht nur Sonnencreme und Badehose obligatorisch ins Reisegepäck, sondern auch Handy, Tablet oder für manch einen sogar das Arbeitslaptop. Aber unsere nützlichen Helfer sind unterwegs vielen Gefahren ausgesetzt – Diebstahl, Tauchgang oder sogar Virenbefall.

Sophos hat daher ein paar Maßnahmen zusammengestellt, mit denen Geräte und Daten sicher durch den Urlaub kommen. Am besten VOR der Abreise anzuwenden:

### **1. Backup aller Geräte machen**

So regelmäßig wie Zahnarzt-Checkup und Co. sollte man auch Sicherheitskopien seiner Daten machen. Viele Systeme machen das nach einem bestimmten Turnus selbst, wenn das noch nicht geschieht, ist vor dem Urlaub der richtige Zeitpunkt dafür. Und wie das immer so ist mit der Sicherung von Sachen – wer vorher ausmistet, hat danach weniger zu lagern. Also eine gute Gelegenheit, sich von angesammelten Daten zu trennen oder sie in einer sicheren Cloud abzulegen. Mit weniger Gepäck reist es sich leichter – auch ins Ausland, wo man in bestimmten Regionen nämlich seine Datenmenge angeben muss.

### **2. Alle Geräte verschlüsseln**

Je einfach der Sperrcode zu merken ist, desto leichter ist er auch zu knacken. Als Gedankenstütze kann man seine PIN nach einem System, das man selbst auch in Chaosituationen noch durchschaut, an einem anderen Ort sicher hinterlegen. Für die SIM-Karte sollte auch ein eigener PIN eingerichtet und aktiviert sein (bei Diebstahl des Geräts sehr nützlich).

Bei Mitnahme eines Firmenlaptops gilt: sehr gutes Passwort auswählen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen und lang) und auch die Festplatte gesondert verschlüsseln.

### **3. Öffentliches Wi-Fi nutzen, ja, aber:**

Kann man machen, da die Gefahren hier kalkulierbar und aufzuhalten sind. Aber bitte auf sicheren Seiten surfen, erkennbar an <https://>. Noch sicherer ist die Einrichtung eines VPN-Tunnels für jeglichen Internetverkehr. Wer kein öffentliches Wi-Fi verwenden möchte, kann sich eine lokale SIM-Karte mit einem Prepaid-Datentarif für die Dauer des Aufenthalts kaufen. Aber: da die meisten Länder von ihren Telefonanbietern verlangen, dass sie über so genannte legale Abhörmöglichkeiten verfügen, sind diese mobilen Datentarife nicht anonym.

### **4. Keine Kiosk-PCs an Flughäfen oder Hotels nutzen**

Nur wenn es die einzige Alternative ist, sollte man dieses Angebot nutzen. Dabei gilt: So wenig Logins oder persönliche Daten angeben wie möglich, nur die nötigsten Anwendungen wie zum Beispiel Ausdruck einer Bordkarte oder ähnliches ausführen. Niemals Online Banking.

## **5. Einreisebedingungen des Urlaubslandes beachten**

Meist verläuft die Einreise problemlos. Es gibt aber auch Länder, die die mitgeführten Geräte sehr gewissenhaft prüfen und zum Teil Kopien von Datenspeichern machen. Wer das nicht möchte, sollte die Mitnahme des Gerätes noch einmal überdenken. Einige Urlaubsparadiese verlangen Adresse (auch der E-Mail) und Telefonnummer. Am besten VOR der Einreise die entsprechenden Bestimmungen des Ziellandes beachten.

## **6. Sonderfall: Unerwartete geschäftliche E-Mail**



Nur weil man selber Ferien macht, urlauben ja nicht auch alle Kollegen. Kommt eine unerwartete und seltsame Nachricht von einem Mitarbeiter oder Geschäftspartner, sollte man nicht direkt darauf antworten, sondern diese erst einmal via anderer Kanäle (Telefon, SMS, Firmen-Chatprogramm) verifizieren. Denn die Chance einer zielgenauen Phishing-E-Mail ist groß.

Ein letzter Rat zum Schluss: Mit den oben genannten Tipps kann man seine Geräte guten Gewissens mit in den Urlaub nehmen. Aber ob Zuhause oder im Ausland hat sich der internationale Merksatz bewährt: „If in doubt, let it out!“ – im Zweifel lieber Finger weg.

Sophos wünscht einen sorglosen Sommer!

## **Social Media von Sophos für die Presse**

Wir haben speziell für Sie als Journalist\*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos\_info

## **Pressekontakt:**

Sophos  
Jörg Schindler, PR-Manager Central & Eastern Europe  
[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications  
Arno Lücht, +49-8081-954619  
Thilo Christ, +49-8081-954617  
Ulrike Masztalerz, +49-30-55248198  
Ariane Wendt +49-172-4536839  
[sophos@tc-communications.de](mailto:sophos@tc-communications.de)