

Ausgespähte Kontodaten: Im Urlaub besser auf Online-Banking verzichten

R+V-Infocenter: Allgemein zugängliche Computer und WLANs haben oft Sicherheitslücken – wichtige Bankgeschäfte per Telefon tätigen

Wiesbaden, 16. Juli 2014. Schnell eine Überweisung erledigen oder den Kontostand prüfen: Online-Banking ist bequem und von überall aus möglich – auch im Urlaub. Doch das kann mit hohen Risiken verbunden sein. „Wer am Urlaubsort öffentlich zugängliche Computer oder Netze für Online-Banking nutzt, muss damit rechnen, dass Betrüger persönliche Daten ausspähen. Im schlimmsten Fall räumen sie im Anschluss das gesamte Konto leer“, sagt Dr. Mirko Saam, Sicherheitsexperte beim Infocenter der R+V Versicherung. Er rät, auf Bankgeschäfte zu verzichten oder sie nur telefonisch zu erledigen.

Internet-Cafés, „Free WIFI“ oder Hotel-Computer: Nutzer haben keine Garantie auf Viren-Schutz, Firewall oder Datensicherheit bei öffentlichen Geräten und WLAN-Netzen. Oft sind die Rechner veraltet und wichtige Updates fehlen. Oder die Systeme sind mit Schadsoftware infiziert. „Am besten erledigen Urlauber alle wichtigen Finanzangelegenheiten vor ihrer Reise“, so R+V-Experte Dr. Saam. „Dasselbe gilt für Internet-Buchungen mit Kreditkartenzahlung, beispielsweise Flüge oder Hotels.“

Die sicherste Methode für unvermeidbare Bankgeschäfte: im Bankinstitut anrufen oder eine Filiale vor Ort aufsuchen. Auch ein eigenes Notebook oder Laptop mit Surfstick ist besser als ein fremdes Gerät. Allerdings können so im Ausland hohe Kosten entstehen.

Das mTAN-Verfahren via Smartphone ist ebenfalls nur bedingt geeignet. Dabei wird eine TAN-Nummer per SMS auf das Mobiltelefon verschickt. Doch Kriminelle schlagen vermehrt über manipulierte Apps zu. „Im ersten Quartal des Jahres 2014 haben sich die Smartphone-Attacken laut BKA versechsfacht“, warnt Dr. Saam. „Nutzer sollten Apps nur aus dem App-Store herunterladen.“

Weitere Tipps des R+V-Infocenters:

- Auch E-Mail, Facebook und Co. nicht auf öffentlichen Computern oder in fremden WLANs aufrufen. Besser ist es, das eigene Laptop oder Smartphone mit Mobilfunknetzen wie UMTS oder LTE zu nutzen.
- Bei Webseiten auf verschlüsselte Datenübertragung achten: Diese erkennen Nutzer am Schloss-Symbol im Browser und den Buchstaben „https“ vor der URL.
- Vor der Reise ein Limit für Geldbewegungen mit der Bank vereinbaren – so bleibt der Schaden im Ernstfall überschaubar.