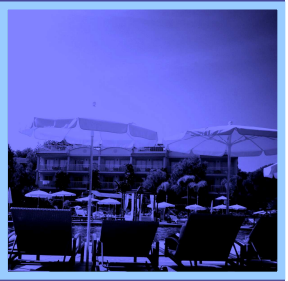
Technik in der Urlaubszeit

Was Sie vor und im Urlaub tun können, um sich und Ihre Daten zu schützen!

Die Technik, die wir täglich mit uns führen und benutzen und die Dienste, die wir regelmäßig im Internet in Anspruch nehmen, nehmen stetig zu. Wir verlassen uns zunehmend auf diese Technik und können zum Teil schon gar nicht mehr ohne sie, wir sind teilweise schon abhängig und nicht selten bestimmt die Technik unser Handeln.

Doch dann ist sie da, die Urlaubszeit. Die Möglichkeit, endlich mal von all diesen Dingen loszukommen und abzuschalten. Aber viele von uns wollen oder können inzwischen nicht mehr abschalten. Der Zwang, überall erreichbar zu sein, überall auf alles im Internet Zugriff zu haben oder jedem davon jederzeit zu berichten, ist für viele Urlauber weiterhin gegeben. Vielleicht ist es durch den ausgeübten Beruf sogar erforderlich. So wird das nötigste für den Urlaub an Technik eingepackt: Smartphone, Tablet-PC oder Notebook, Digitalkamera, Lade- und Datenkabel. Weitere Absicherungen vor und während des Urlaubes werden aber vollkommen vergessen.
Was können Sie also tun, damit der inzwischen technisierte Urlaub zumindest ein wenig entspannter wird?

Was Sie bereits zu Hause machen können:



Neben den inzwischen schon weiter verbreiteten Maßnahmen zur Absicherung des Eigenheimes, der Benachrichtigung der Nachbarn und dem Abbestellen der Zeitung, sollte sich auch um die Technik zu Hause gekümmert werden.

- ☑ Machen Sie ein Backup (Sicherheitskopie) von den privaten und wichtigen Daten Ihrer Endgeräte, die Sie in den Urlaub mitnehmen. Lassen Sie dieses Backup gesichert zu Hause. Vermeiden Sie somit den Verlust Ihrer privaten Daten z.B. bei einem Diebstahl Ihres Notebooks oder Smartphones.

- ☑ Notieren Sie die Seriennummern und Gerätebezeichnungen der Geräte, die Sie mitnehmen und bewahren Sie diese an einem getrennten Ort (z.B. bei den Reiseunterlagen im Hotelsafe und zu Hause) auf. So haben Sie diese Daten zumindest im Falle eines Diebstahls oder Verlustes für die örtliche Polizei griffbereit.

- ☑ Vermeiden Sie das öffentliche Bekanntgeben („posten“) von Urlaubsnachrichten in Sozialen Netzwerken. Auch Einbrecher können möglicherweise auf Ihre Einträge stoßen und erkennen, dass Sie in den nächsten 3 Wochen ungestört Ihr Haus aufsuchen können.

- ☑ Richten Sie eine neue Mailadresse (Wegwerfadresse) ein, die Sie lediglich für den Urlaub gebrauchen und teilen Sie diese den gewünschten Daheimgebliebenen mit. Diverse E-Mail-Anbieter stellen solche Dienste zur Verfügung. So vermeiden Sie, dass z.B. an Hotelrechnern Ihr echtes Postfach ausgespäht wird.

- ☑ Richten Sie spezielle Sicherheitsdienste (z.B: VPN-Dienste, Antivirensoftware) ein, die Sie im Urlaub verwenden sollten. Ggf. sind hier zusätzliche Kosten zu erwarten. Einige Antivirenhersteller bieten zusätzlichen Schutz für die Hotspotnutzung an. Bei VPN-Diensten (Virtuelle private Netzwerke) handelt es sich u.a. um eine Möglichkeit, innerhalb einer Internetverbindung, wie z.B. über ein kostenloses Wlan im Hotel, eine verschlüsselte „eigene“ Verbindung aufzubauen, die von Unbekannten nicht „abgehört“ werden kann. Somit bleibt Ihr Datenverkehr vertraulich und sicher.

- ☑ Verstauen Sie, soweit möglich, wertvolle Elektronik (z.B. Notebook) sicher in das Handgepäck und lassen Sie dieses nicht aus den Augen (z.B. im Flughafencafe oder in der Warteschlange beim Check-In)

Bitte wenden →

Was Sie unterwegs und am Urlaubsort machen können:

Flughäfen, Hotels, Cafés usw. bieten zum Teil kostenfreie Hotspots an. Dies sind Wlan-Zugänge (Funknetzwerke), die die Gäste für das Surfen im Internet nutzen können. Doch solche Netze sind nicht immer sicher für die Gäste. Da Sie die Betreiber nicht kennen, sollten Sie vorsichtig bei der Nutzung eines solchen Angebotes sein. Es ist den Tätern sogar möglich, ein eigenes Wlan anzubieten, welches der Gast nicht als gefälscht erkennt. Unverschlüsselter Datenverkehr kann somit sehr leicht ausgelesen und für illegale Zwecke missbraucht werden. Bedenken Sie dieses bei der Eingabe von sensiblen Daten wie Onlinezahlungen, Mailverkehr oder Soziale Netzwerke. Gleiches gilt für Computer, die Ihnen zum Teil auch kostenfrei in Hotels oder Cafés zur Verfügung gestellt werden. Sie können nicht wissen, was Täter absichtlich oder andere Nutzer versehentlich an Schadsoftware aufgespielt haben.

- ☑ Behalten Sie Ihr Gepäck ständig im Auge. Nutzen Sie z.B. Schlösser, um einen schnellen Zugriff in die Taschen durch Unbekannte zu vermeiden. Täter nutzen Ihre Unachtsamkeit z.B. beim Stadtbummel, in Bussen oder am Hotelpool aus oder versuchen, Sie von Ihrem Gepäck räumlich und gedanklich wegzulocken oder abzulenken.

- ☑ Tragen Sie Ihr Smartphone an sicheren Orten innerhalb Ihrer Kleidung. Nutzen Sie Verschlussmöglichkeiten wie Knöpfe und Reißverschlüsse. Aussentaschen (z.B. an Cargohosen oder an Rucksäcken) sind für Täter leichter erreichbar.

- ☑ Seien Sie sich der oben genannten Gefahren eines Hotspots bewusst.

- ☑ Nutzen Sie Hotspots nicht für wichtigen Datenverkehr (Mailempfang und Versand, Zahlungsverkehr, Einkäufe, Buchungen, Flugbestätigungen, Clouddienste, Soziale Netzwerke usw.). Ein „Mitlesen“ durch Unbekannte ist leicht möglich.

- ☑ Nutzen Sie, wenn möglich VPN-Dienste (ggf. kostenpflichtig), so können Unbekannte Ihren Datenverkehr nicht „mitlesen“. Gleiches gilt in der Regel bei der Nutzung von gesicherten Internetseiten (geschlossenes Schlosssymbol im Browser oder https://-Verbindungen)

- ☑ Loggen Sie sich bei Webanwendungen (auch am eigenen Computer) immer vollständig aus. Ein Schließen des Programmfensters ist nicht ausreichend.

- ☑ Lassen Sie Ihren Computer/Tablet-PC/Smartphone z.B. in der Hotellobby, im Internetcafé oder am Pool nicht unbeaufsichtigt und ungesichert stehen und nutzen Sie an den Geräten einen sicheren Passwortschutz/PIN-Schutz.

- ☑ Nutzen Sie während der Abwesenheit zur Aufbewahrung im Hotel den Zimmer-Safe. Schließen Sie auch Balkontüren zu. Geben Sie Gelegenheitstätern keine Chance.

- ☑ Lassen Sie die Endgeräte (z.B. Smartphone oder Navi) nicht im Auto liegen.

- ☑ Vermeiden Sie das Einstecken mitgebrachter Speicherkarten und USB-Sticks in fremde Computer. So verhindern Sie eine spätere Übertragung von Schadsoftware auf Ihre Computer zu Hause.

- ☑ Geben Sie private Daten, Passwörter und PIN an Computern und Smartphones an öffentlichen Orten (z.B. Bahn oder Café) verdeckt ein. Sie werden möglicherweise von fremden Personen dabei beobachtet.

Wir wünschen einen erholsamen, entspannten und sicheren Urlaub!

Kostenlose Beratung und weitere Informationen erhalten Sie beim Präventionsteam Ihrer Polizeidienststelle.

Impressum:
Landeskriminalamt Niedersachsen - Zentralstelle Prävention - Am Waterlooplatz 11, 30169 Hannover