Cybercrime

- es kann jeden treffen und jederzeit -

Sicher im Urlaub

Wie man sich in Sachen vernetzter Technik auf eine Urlaubsreise vorbereitet und im Urlaub sicher handelt

Eine Kurzübersicht

LANDESKRIMINALAMT
NIEDERSACHSEN

Inhalt

Endlich ist es soweit. Der wohlverdiente Urlaub steht kurz bevor. Die für viele wohl schönste Zeit des Jahres beginnt, die im Idealfall auch perfekt verlaufen sollte. Doch jedes negative Erlebnis kann die Urlaubsfreude mindern und den Urlaub zu einer unvergesslichen negativen Erfahrung werden lassen.

Immer mehr Urlaubs-, aber auch Geschäftsreisende können, wollen oder dürfen nicht auf Reisen auf ihre digitalen Geräte verzichten. Das Smartphone gehört inzwischen bei den meisten Menschen zum täglichen Gebrauchsgegenstand, zu einem Allrounder, der Maildienste, Shopping, Onlinebanking, Navigation, Social Network, Fotoapparat und alle übrigen Internetdienste beinhaltet.

Gerade aus diesem Grund sollte auch auf diese Geräte besonders geachtet werden und die darin befindlichen und vernetzten Daten geschützt werden.

In der nachfolgenden Kurzübersicht zeigen wir Ihnen, was Sie schon bereits zu Hause, aber auch später auf der Reise machen können, um Ihre digitalen Geräte und Ihre persönlichen Daten zu schützen.

1. Zu Hause – Was Sie rechtzeitig vor Ihrer Abreise durchführen sollten

Bereits zu Hause sollten die ersten Vorbereitungen für den Urlaub getroffen werden, um im oder nach dem Urlaub keine böse analoge/digitale Überraschung zu erleben. Da diese Maßnahmen nicht immer kurzfristig erfolgen können, sollten Sie ebenfalls diese Maßnahmen **rechtzeitig** in Ihre Reiseplanung mit einschließen

1.1 Was bleibt zu Hause?

Überlegen Sie genau, welche Geräte Sie auf der Reise wirklich benötigen. Reicht Ihnen eine „kleine Version“ aus (z.B. Tablet statt Notebook) oder müssen Sie doch tatsächlich mehr mitnehmen? Denken Sie z.B. auch an die Lagermöglichkeit im Hotel. Während Smartphones oder Tablet-Computer in der Regel in die typischen **Hotelsafes** passen, kann es bereits mit normalgroßen Notebooks bereits Probleme geben. Eine ungesicherte Aufbewahrung ist nicht zu empfehlen.

Gleiches gilt aber auch für die Zeit der Abwesenheit zu Hause. Hinterlasse ich meine Geräte zu Hause in Sicherheit? Wer hat hier möglicherweise während meiner Abwesenheit Zugriff auf meine Geräte?

Was kann zu Hause ausgeschaltet werden? Benötigen irgendwelche Geräte während Ihrer Abwesenheit zum Beispiel noch WLAN? Wenn Sie WLAN nicht benötigen, dann können Sie diese Schnittstelle auch während Ihrer Urlaubszeit auch deaktivieren. Haben Sie jedoch Smart-Home-Sicherheitstechnik, die eventuell auf WLAN angewiesen ist, dann sollten Sie dieses natürlich nicht ausschalten, es jedoch gegen Fremdzugriffe ordentlich gesichert haben.

1.2 Smart Home

Neben „Wachsamer Nachbar“ und Aufsicht durch Nachbarn kann Smart-Home-Technik ergänzend verwendet werden. Die Möglichkeiten sind mittlerweile vielseitig und auch preislich für die Endanwender inzwischen interessant. Eine smarte Lichtsteuerung zur Anwesenheitssimulation wäre eine denkbare Lösung. Auch die automatisierte Steuerung von

Fensterrolladen kann hier vorbeugend genutzt werden. Ein möglicher Fernzugriff macht die Regelung der Technik von nahezu überall möglich.

Der Markt bietet derzeit massenhaft Überwachungskameras und vergleichbare Sicherheitstechnik an. Viele Nutzer möchten aus der Ferne sehen können und informiert werden, was während der Abwesenheit zu Hause geschieht. Seien Sie sich aber auch darüber im Klaren, dass Sie entsprechend handeln sollten, wenn es zu einem Zwischenfall, wie z.B. zu einem Einbruch kommt. Wo läuft dieser Alarm auf? Bekommen Sie die Meldung rechtzeitig mit, um Maßnahmen einleiten zu können? Was passiert, wenn Sie z.B. in einem Funkloch sind und ohne Internetverbindung keine rechtzeitige Meldung bekommen? Ist Ihre verbaute Technik zuverlässig und auch gegen Fremdzugriffe abgesichert?

Ihre Polizei kann Sie auch in Sachen Einbruchschutz beraten. Eine mechanische Sicherung ist immer noch der beste Grundschutz.

1.3 Provider- und Vertragsprüfung

Haben Sie eigentlich schon einmal Ihren Mobilfunktarif genauer betrachtet? Wissen Sie, welche Optionen für Sie auch im Ausland gelten? Innerhalb der EU sollte dies inzwischen beim sogenannten Roaming nicht mehr ein so großes Problem sein, jedoch sollten Sie zeitig vor Ihrer Abreise ihr „Kleingedrucktes“ lesen. Vielleicht können Sie noch einige Optionen freischalten, damit Sie im Urlaub keine böse Kostenfalle ereilt.

Beachten Sie auch, dass gewisse Dienste auf einem Smartphone auf eine laufende Internetverbindung angewiesen sind. Ggf. reichen da nicht immer kostenfreie WLAN-Hotspots in Cafés oder Hotels aus.

Verschiedene Anbieter stellen für Auslandsreisen eigene SIM-Karten zur Verfügung. Hier bekommen Sie für einen mehr oder weniger hohen Betrag z.B. eine eigene Rufnummer und ein Datenvolumen. In Zusammenhang mit einem passenden Smartphone oder einen mobilen Hotspot können Sie Ihre vernetzten Geräte dann auch unabhängig von Hotel oder Café nutzen. In vielen Ländern können Sie solche SIM-Karten auch vor Ort im Ausland erwerben. Dort gibt es sie dann oft auch günstiger.

1.4 Mobiler Hotspot

Viele aktuelle Smartphones bieten die Möglichkeit an, einen eigenen Hotspot, also einen WLAN-Zugang für andere Geräte zu erstellen. Die Internetverbindung, die das Telefon hat, kann somit auch auf anderen Geräten genutzt werden. Dies beansprucht den Akku des Smartphone sehr und möglichweise fehlt im entscheidenden Moment der Strom zum Surfen oder Telefonieren. Mehrere Hersteller bieten auch eigenständige Geräte als mobile Hotspots bzw. mobile WLAN-Router an. Mit einer eigenen SIM-Karte (zum Beispiel von einem ausländischen Provider) kann dann das Internet in der Tasche getragen und von mehreren Geräten genutzt werden. Im Zweifelsfall kann auch ein ausgemustertes Smartphone als Hotspot verwendet werden.

1.5 Ortungsdienste und Sperren

„Big Brother is watching you!" - Hiervor haben viele Nutzer Angst. Sie möchten nicht von Ihren Anbietern oder unbekannten Dritten geortet werden. Eine Ortung kann aber gerade im Notfall oder Verlustfall des Smartphones von großer Wichtigkeit sein.

Wer über die Zugangsdaten (Loginname und Passwort) verfügt, kann sich in der Regel von jedem internetfähigen Computer aus der Ferne in die Ortung einschalten. Ggf. können Nachrichten oder Signaltöne abgespielt oder das Smartphone geortet, deaktiviert bzw. gelöscht werden. Hierfür muss das entfernte Gerät jedoch über eine Internetanbindung verfügen. Wurde z.B. das Roaming im Ausland deaktiviert oder das Surfvolumen ist aufgebraucht, kann es hier ggf. zu Problemen kommen.

Am besten, man testet die Ortungsfunktion und übt für den Ernstfall.

Denken Sie auch an das Sperren von Accounts, die möglicherweise auf dem Gerät frei zugänglich sind (z.B. Mailaccount, Shopping App usw.). Im Falle eines Diebstahls können hier die Täter noch mehr Schaden anrichten.

1.6 Backup

Wahrscheinlich ist für viele der Verlust der Daten (Urlaubsfotos, Adressen und mehr) auf einem gestohlenen Smartphone das Schlimmste, was einem im Urlaub passieren kann. Nicht selten nutzen auch die Täter ungeschützte Daten von solchen Geräten, um weitere Straftaten zu begehen. Neben einem Schutz des Gerätes sollte man somit auch an ein Backup (Sicherungskopie) denken.

- ✓ Machen Sie ein Backup 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. Sie können auch ein Backup bei einem Cloud-Dienst machen. Hier wären dann die Daten über das Internet verfügbar. An entsprechende Sicherungen sollte dann aber natürlich gedacht werden.

1.7 Seriennummern und Hotlines

Kennen Sie die IMEI Nummer Ihres Telefones oder auch die korrekte Bezeichnung und die Seriennummer? Können Sie Ihr Gerät bei einer Anzeigenaufnahme bei der Polizei nach einem Diebstahl genau beschreiben?

- ✓ 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.
- ✓ Die IMEI (International Mobile Equipment Identity), eine einmalig vergebene Seriennummer ihres Mobilgerätes, erfahren Sie z.B. an der Produktverpackung, in den Geräteinformationen im Einstellungsmenü oder über die Eingabe folgender Zeichen im Wählmenü des Telefons ***#06#**
- ✓ Halten Sie auch Notrufnummern (z.B. für Sperren bereit). Die 116 116 bzw. +49 116 116 (aus dem Ausland) ist eine allgemeine Sperrrufnummer, bei der auch gestohlene

Bankkarten gemeldet und gesperrt werden können. Smartphones können hier in der Regel nicht gesperrt werden. Hier müssten Sie Ihren Provider kontaktieren. Ist die Karte jedoch gesperrt, ist auch eine Ortung ggf. nicht mehr möglich.

1.8 Soziale Netzwerke und auch Einbruchschutz

Das schöne Hotel, der Pool, die beeindruckende Landschaft, der Cocktail und das Essen. Beliebte Urlaubsmotive landen nicht nur auf dem Smartphone, sondern auch mal recht schnell in sozialen Netzwerken wie Facebook. Jeder Freund kann nahezu live mitverfolgen, wo man sich gerade befindet und was man Wundervolles erlebt hat. Aber nicht nur Freunde können dies eventuell sehen. Je nach Einstellung im sozialen Netzwerk können auch unbekannte Dritte diese Meldung sehen.

- ✓ Aus diesem Grund sollten Sie das öffentliche Bekanntgeben („posten“) von Urlaubsnachrichten in sozialen Netzwerken, vor und während Ihrer Reise, vermeiden. Auch Einbrecher können möglicherweise auf Ihre Einträge stoßen und erkennen, dass sie in den nächsten 3 Wochen ungestört Ihr Haus aufsuchen können.

1.9 Mailadresse auf Reisen

Immer wieder muss man, auch im Urlaub seine eigene Mailadresse bei irgendeinem Anbieter angeben. Dies kann für eine gebuchte Rundreise vor Ort oder für einen Hotspot oder das Hotel sein. Leider weiß man nicht immer, was später mit den angegeben Mailadressen noch so alles geschieht.

- ✓ Aus diesem Grund empfehlen wir, dass Sie sich vor der Abreise noch eine neue Mailadresse einrichten. Diverse E-Mail-Anbieter stellen solche Dienste zur Verfügung. Einige Provider bezeichnen diese auch als **Wegwerfadresse**. Nach Reiseende können Sie diese Mailadresse auch problemlos wieder löschen, wenn Sie z.B. mit ungewollter Werbung überflutet werden. Haben Sie sich ein eigenes Mailkonto eingerichtet, so können Sie sich sogar nahezu ohne großes Risiko an fremden Rechnern auf dieses Extra-Mailkonto anmelden. Sollte es zu einem Zwischenfall kommen (z.B. Ausspähen an einem mit Schadsoftware manipulierten Computer), so bleibt ihr eigenes privates Mailkonto davon unberührt.

1.10 VPN – Virtuelle Private Netzwerke

VPN-Dienste bieten mobil agierenden Personen die Möglichkeit, nahezu sicher im Internet zu surfen. Virtuelle Private Netzwerke kann man sich als zusätzlichen verschlüsselten Tunnel durch eine bestehende Internetverbindung vorstellen. Wenn Sie sich in einem fremden Netzwerk (z.B. Hotel, Flughafen, Internetcafé mit kostenfreiem WLAN/LAN) befinden, können sich dort auch andere Personen aufhalten, die böse Absichten haben. Täter können es auf Ihre Daten im Netzwerk abgesehen haben. Nutzen Sie eine VPN-Verbindung, so können Außenstehende nicht auf Ihren Datenverkehr zugreifen.

Für VPN gibt es verschiedene Dienstanbieter. Einige Antivirenprogramm-Hersteller bieten den Service, aber auch andere Anbieter, die mit der Datensicherheit Geld verdienen wollen. Neben kostenpflichtigen Diensten können Sie aber auch kostenfreie Versionen nutzen. Hier müssen Sie aber mit verminderten Geschwindigkeiten und kleinem Datenvolumen rechnen. Zudem kann es auch schwarze Schafe in der Branche geben, die Ihre Kundendaten zu

Werbezwecken missbrauchen. Informieren Sie sich also rechtzeitig vor Abreise, welche Dienste als vertrauenswürdig und sicher getestet wurden. Erfahrene Nutzer können eventuell sogar eine Verbindung nach zu Hause mit dem eigenen Router eine eigene VPN-Verbindung herstellen. Der Hersteller der Fritzbox bietet beispielsweise diesen Dienst an. Hier könnte man dann mittels VPN sogar über das eigene Internet (also auch seine private IP-Adresse aus Deutschland) zu Hause surfen. Ein zusätzlicher Vorteil wäre, dass man zum Teil sogar auf die heimische Telefonie, angeschlossenes Smart Home oder gebuchte Streamingdienste zugreifen könnte. Wer jedoch die gleiche Surfgeschwindigkeit wie zu Hause erwartet, der wird möglicherweise enttäuscht. Die Geschwindigkeit hängt zusätzlich vom genutzten VPN-Dienst und der vor Ort genutzten Internetverbindung ab.

Egal für welchen Dienst man sich entschieden hat, ist der Dienst korrekt im Endgerät eingerichtet, so sollte man Ihn auch zu Hause und in anderen fremden Netzen einmal testen. Je nach genutztem Endgerät kann die Einrichtung und Nutzung simpel oder kompliziert sein. Smartphones mit Android lassen in der Regel eine nahezu dauerhafte VPN-Verbindung zu. iOS-Geräte (z.B. iPhone) dagegen unterbrechen nach einiger Zeit der Inaktivität (z.B. bei einem längeren Stand-By) die VPN-Verbindung. Im Display des Telefons wird bei erfolgreicher Verbindung ein kleines VPN-Logo eingeblendet.

Einige Hotels haben jedoch die Möglichkeit einer VPN-Nutzung in deren Netzwerk technisch unterbunden. Somit kann der Dienst dort nicht genutzt werden. Möglicherweise ist die VPN-Nutzung in einem bestimmten Land gesetzlich untersagt. Hier sollte man sich vor Abreise Gewissheit verschaffen.

Inzwischen gibt es Anbieter, die eigene mobile VPN-Lösungen über externe Boxen zur Verfügung stellen oder diese in sogenannten Reiseroutern ermöglichen. Hier können die Geräte und die VPN-Dienstleistung kostenpflichtig, aber auch zum Teil kostenfrei erworben werden. Über solche Geräte können dann aber längerfristige Hotspots (z.B. am Hotel-LAN-Anschluss) genutzt werden.

2. Kofferpacken und los geht‘s

Nun haben Sie wahrscheinlich alle wichtigen Maßnahmen durchgeführt, die Sie bereit längerfristig vor Ihrer Reise durchführen konnten. Die Abreise steht nun kurz bevor und es geht ans **Kofferpacken**.

- ✓ Verstauen Sie, soweit möglich, wertvolle Elektronik (z.B. Notebook, Smartphones) sicher in das Handgepäck oder in die verschließbaren Innentaschen von getragener Kleidung und lassen Sie dieses nicht aus den Augen (z.B. im Flughafencafé oder in der Warteschlange beim Check-In, bei der Gepäckausgabe, im Transferbus usw.). Zusatzschlösser an den Koffern können einen schnellen Zugriff durch Taschendiebe verhindern.
- ✓ Beachten Sie aber unbedingt die Hinweise der Fluggesellschaften in Bezug auf Gerätenutzung und Transport (Explosionsgefahr von Akku) an Bord.
- ✓ Möglicherweise müssen Sie diese auf Verlangen beim Sicherheitscheck am Flughafen gesondert vorzeigen und sogar vorführen und gesondert auf das Laufband für die Röntgen-Kontrolle legen. Eventuell müssen die Geräte zwangsläufig auch besonders verpackt oder transportiert werden.

2.1 Unterwegs und im Urlaub

- ✓ Behalten Sie Ihr Gepäck ständig im Auge. Nutzen Sie weiterhin die Schlösser, um einen schnellen Zugriff in die Taschen durch Unbekannte zu vermeiden. Die 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. Eine Zeitung oder ein Stadtplan können die Sichtverbindung zu Ihrem Smartphone auf dem Tisch unterbrechen. Einen Diebstahl bekommen Sie somit gar nicht mit.
- ✓ Die Täter handeln jedoch nicht immer allein. So kann ein Mittäter nahezu unbemerkt auf Taschen zugreifen, während eine andere Person Sie ablenkt. Es gibt sogar Tätergruppen, die einem telefonierenden Menschen auf der öffentlichen Straße das Smartphone aus der Hand reißen. Durch ein geschicktes Zusammenspiel mehrerer Personen mit Anrempeln des Opfers und Weiterreichen des gestohlenen Telefons kann das Opfer die Täter nicht mehr erkennen.
- ✓ 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 (und auch mit Cutter-Messern oder extrem scharfen Skalpellen leicht aufschneidbar) und weniger spürbar.

2.2 Nutzung fremder Hotspots

Teure Datentarife oder geringe Geschwindigkeiten führen dazu, dass viele Nutzer sich im Ausland auf kostenfreie WLAN-Hotspots einlassen. 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 eines fremden Hotspots nicht kennen, sollten Sie immer 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. Der Name „Hotel-Guest-WLAN“ oder „Airport-WLAN“ ist für einen Cyberkriminellen leicht erstellbar und verführt einen unvorsichtigen Internetsuchenden zum schnellen Verbinden mit diesem Netzwerk. Unverschlüsselter Datenverkehr kann somit in diesem Netzwerk durch den Täter sehr leicht ausgelesen und für illegale Zwecke missbraucht werden.
- ✓ 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 die von Ihnen vorher eingerichteten VPN und surfen Sie auf Seiten, die https verwenden (geschlossenes/grünes Schlosssymbol im Browser).
- ✓ Deaktivieren Sie WLAN und andere Schnittstellen, wenn Sie diese nicht benötigen.
- ✓ Wer über genug eigenes Datenvolumen verfügt surft im Idealfall über das eigene Telefonnetz. Hier ist man in der Regel sicher (Ggf. Roaming-Gebühren beachten).

2.3 Nutzung von Hotelcomputer und Computern in Internetcafés

- ✓ Generell gilt Vorsicht vor unbekannten Computern! Sie können nicht wissen, was ein Täter absichtlich oder andere Nutzer versehentlich an Schadsoftware oder Spionagesoftware aufgespielt haben. Sie können sich nicht sicher sein, dass diese Geräte sich in einen aktuellen und sicheren Zustand befinden. Nutzen Sie solche Geräte nicht für sensible Dienste. Hier kann man sich eher den lokalen Wetterbericht, Informationen über Ausflugsziele oder die heimische Tageszeitung anschauen.

2.4 Ausloggen nicht vergessen!

- ✓ Loggen Sie sich bei Webanwendungen (auch am eigenen Computer) immer vollständig aus. Ein Schließen des Programmfensters ist nicht ausreichend. Dies sollten Sie insbesondere an frei zugänglichen Computern (z.B. Hotellobby) bedenken.

2.5 Datenübertragung per Kabel/Lesegerät/USB

- ✓ Vermeiden Sie auch das Einstecken mitgebrachter Speicherkarten und USB-Sticks in fremde Computer. So verhindern Sie eine Infektion des Datenträgers und spätere Übertragung von Schadsoftware auf Ihre Computer zu Hause.
- ✓ Vorsicht auch beim Aufladen/Verbinden Ihrer Smart-Geräte an unbekannten Schnittstellen. Neben billigen und unsicheren Netzteilen, die Ihr Gerät zerstören können, können auch ungewünschte Daten übertragen werden. Ein sogenanntes „USB-Kondom“ oder ein sogenannter „Daten-Blocker“ kann verwendet werden, um Datenübertragung zu unterbinden. Diese speziellen Adapter trennen im Lade- und Datenkabel den Datenverkehr und lassen nur noch den Ladestrom durch.

2.6 Wo lasse ich mein Smartphone?

Immer mehr sieht man beim Sonnenbaden die Touristen mit Ihren Smartphones. Ob nur Musik gehört, gelesen oder im Internet gesurft wird, spielt weniger die Rolle. Spätestens, wenn man schläft oder baden geht, verbleiben diese Geräte beim Badetuch auf der Sonnenliege.

- ✓ Lassen Sie Ihren Computer/Tablet-PC/Smartphone z.B. in der Hotellobby, im Internetcafé, Restaurant oder am Pool nicht unbeaufsichtigt und ungesichert liegen. Legen Sie die Geräte so ab, dass diese geschützt vor Fremdzugriffen sind. Nutzen Sie zudem an den Geräten einen sicheren Passwortschutz/PIN-Schutz.

2.7 Ist der Hotelsafe sicher?

Ob ein Hotelsafe sicher ist oder nicht, kann hier leider nicht beantwortet werden. Hier bieten die unterschiedlichen Hotels verschiedenste Varianten an. Es kursieren im Internet sogar Anleitungen, wie man gewisse Hotelsafes angeblich mit Leichtigkeit öffnen kann.

- ✓ Eine Verwahrung der Geräte ist dennoch deutlich sicherer als auf dem Tisch im Hotelzimmer. Gelegenheitstäter werden somit weniger in Versuchung geführt. Schließen Sie beim Verlassen Ihres Hotelzimmers auch die Balkontüren zu.

2.8 Unterwegs im Auto

Sollten Sie mit dem Auto reisen oder vor Ort einen Mietwagen gebucht haben, so müssen Sie leider auch mit dem Diebstahl von Wertgegenständen aus dem Auto rechnen.

- ✓ Lassen Sie die Wertgegenstände (z.B. Smartphone oder Navi) nicht im Auto liegen. Verschließen Sie z.B. beim Tanken, an Raststätten und an spontanen Stopps bei Sehenswürdigkeiten immer Ihr Fahrzeug, wenn keine Person im Auto verbleibt. Ein kurzer Stopp für ein schnelles Foto kann dazu führen, dass diese Ablenkung schon ausreicht. Fremde Personen öffnen leicht und unbemerkt die unverschlossenen Türen und gelangen so auch an Handtaschen und Smartphones, die auch als Navi im Auto befestigt sind oder auf dem Beifahrersitz liegengelassen werden.

2.9 Ausspioniert

Unterwegs an öffentlichen Orten oder mit öffentlichen Verkehrsmitteln möchte man möglicherweise die Reisezeit gern auch mit dem Surfen im Smartphone oder Tablet überbrücken. Sogenannte Shoulder-Surfer können bereits beim Blick durch Sitzreihen, im Bus neben einem stehend oder im Café sitzend schon einiges über diese Personen und die Geräte erfahren. Schnell hat man den PIN oder Zugangsdaten gesehen und sich gemerkt, wo die Person im Anschluss das Gerät verstaut. Im dichten Gedränge und Anrempeln beim Aussteigen aus der Bahn, auf dem Marktplatz oder an überfüllten Sehenswürdigkeiten wird ein Smartphone sehr schnell aus der rückwertigen Hosentasche oder Rucksack nahezu unbemerkt gezogen.

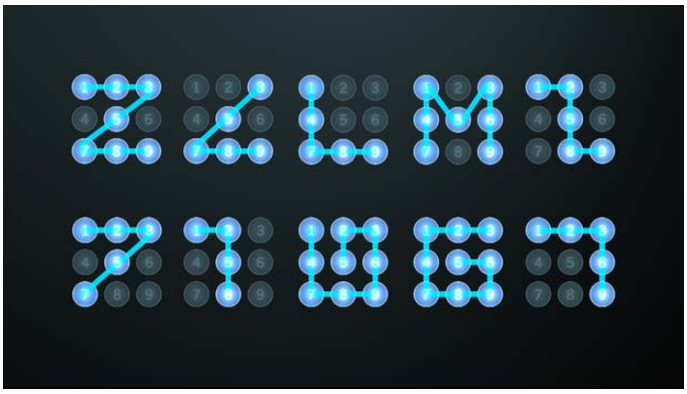
- ✓ Geben Sie private Daten, Passwörter und PIN an Computern und Smartphones an öffentlichen Orten (z.B. Bus, Bahn oder Café) nur verdeckt ein. Sie werden möglicherweise von fremden Personen dabei beobachtet. Es gibt im Handel Sichtschutzfolien, die Einblicke von der Seite verhindern.

2.10 Auch für Smartphones gilt

- ✓ Nutzen Sie einen sicheren PIN Code, einen sicheren alphanumerischen Code oder den Fingerabdruckscanner. Übrigens, eine PIN muss nicht immer vierstellig sein! Besondere Vorsicht gilt bei der Verwendung von Wischmustern, der einfachen Gesichtserkennung und der Nutzung von keiner eingerichteten Sperre!

- ✓ Wischmuster sind leicht zu merken. Es gibt häufige Muster, die immer wieder verwendet werden. Ggf. ist auf dem Display auch noch das Wischmuster als Schmierfilm erkennbar.

Wischmuster Studie 2015 von Tobias Schrödel (für SternTV) und LKA Niedersachsen zeigt häufigste Muster (Top 10).



Quelle: Stern TV
http://www.stern.de/tv/handys-vor-fremdzugriff-schuetzen--so-unsicher-sind-mustersperren-auf-dem-smartphone-6426898.html

3. Bedenken Sie immer

- ✓ Smartphones und Tablets sind wie Computer zu Hause, nur sehr wahrscheinlich mit noch mehr Inhalten!
- ✓ Was haben Sie alles dem Gerät gespeichert?
- ✓ Wofür nutzen Sie es? (privat, Beruf, beides)
- ✓ Was kann es alles und was ist damit alles verbunden? (Mail, Adressen, Zahlungsdienste , Shopping usw.)

Aus diesem Grund sollten Sie diese Geräte besonders schützen und im Auge behalten!

4. Ratgeber Internetkriminalität und mehr Links

Allgemeine Tipps rund um das Thema Cybercrime finden Sie im Ratgeber Internetkriminalität unter www.polizei-praevention.de

Diese ausführlichen Tipps finden Sie auch unter „Themen und Tipps“ – „Auf Reisen und im Urlaub“ oder als Kurzversion in unserer Mediathek.

Unsere Tipps online finden Sie hier im Ratgeber unter „Auf Reisen und im Urlaub“

Tipps zum Thema Smarthome

Weitere Tipps zur Sicherheit im Urlaub bzw. zur Vorbereitung finden Sie hier bei

www.polizei-beratung.de:

Thema Taschendiebstahl

Faltblatt Vorsicht! Karten-Tricks!

Faltblatt Langfinger machen niemals Urlaub

Faltblatt Schlauer gegen Klauer

Broschüre Klicks-Momente - Internetnutzer

Broschüre Sicher wohnen

Faltblatt Bremsen Sie Diebe rechtzeitig aus!

Impressum:

Landeskriminalamt Niedersachsen, Dezernat 32
Am Waterlooplatz 11, 30169 Hannover

www.lka.niedersachsen.de

www.polizei-praevention.de

Stand Mai 2021