CORPORATE TRUST
business risk & crisis management

HANDBUCH

FÜR PERSÖNLICHE SICHERHEIT

„So schützen Sie sich und Ihre Familie zu Hause und unterwegs.“

Dieses Handbuch wurde von den Experten der Corporate Trust Business Risk & Crisis Management GmbH verfasst. Es soll Ihnen dabei helfen, mittels einfacher Sicherheitsmethoden und erprobter Taktiken bestimmte Risiken für Sie und Ihre Familie zu reduzieren. Vieles davon gilt zwar für Gegenden mit erhöhtem Sicherheitsrisiko, doch können Ihnen Sachkenntnis, Wachsamkeit und die richtige Reaktion im entscheidenden Moment überall auf der Welt das Leben retten oder Sie vor Schaden bewahren.

Stand: 2015

1. Sicherheit und Familie

2. IT-Sicherheit

3. Reisesicherheit

Sicherheit zu Hause

- Sorgen Sie dafür, dass Ihr Haus von einem Zaun oder einer Mauer umgeben ist. Zugangstore für Personen und Fahrzeuge sollten aus Vollholz oder Metall bestehen. Die Zufahrt ist mit einem automatischen Garagenöffner zu versehen, der von allen Fahrzeugen sowie vom Haus aus bedient werden kann. In alle Tore sollte eine Überwachungslinse für den Blick nach außen integriert sein.

- Sichern Sie Ihren Eingang durch Außentüren aus Vollholz, Metall oder durch eine Stahlverkleidung. Statten Sie die Türe mit einem Weitwinkel-Türspion aus.

- Weisen Sie alle Familienmitglieder und Haushaltshilfen an, Fremden erst dann zu öffnen, wenn sie die Identität des Besuchers festgestellt und sich vergewissert haben, dass die Person erwartet wird.

- Beleuchten Sie Außentüren und -tore durch Bewegungsmelder und verwenden Sie eine Sprechanlage sowie eine Videoüberwachungsanlage.

- Sichern Sie die Türangeln der Türen und Tore durch Riegel und Hinterhaken.

- Schützen Sie Fenster mit Schlössern und erforderlichenfalls mit fest in den Rahmen und ins Mauerwerk eingelassenen Stahlstäben.

- Alle Außentüren und Fenster sollten durch eine Alarmanlage geschützt sein, die nach Möglichkeit mit einem verlässlichen zentralen Sicherheitsdienst verbunden ist.

- Bringen Sie in den Schlafzimmern, an Außentüren und im Küchenbereich Panikknöpfe an, die mit der Alarmanlage gekoppelt sind.

- Prüfen Sie regelmäßig alle Schlüssel auf Vollzähligkeit. Kommt ein Schlüssel abhanden oder wechselt das Hauspersonal, sollten die Schlösser ausgetauscht bzw. die Schließzylinder auf neue Schlüssel umgestellt werden.

- Wohnungen sind zwar sicherer als Häuser, bedürfen aber dennoch einiger Sicherheitsvorkehrungen. Von außen zugängliche Fenster und Balkone sollten mit Stahlstäben geschützt werden. Besondere Vorsicht gilt bei Balkonen oder Fenstern, die von angrenzenden Dächern aus erreichbar sind.

- Sicherheitskräfte, die das Gebäude von außen bewachen, sind dahingehend zu schulen, dass sie Bewohner beim Verlassen des Gebäudes im Auge behalten und feststellen, wenn diese beobachtet werden.

- Halten Sie zu Hause jederzeit ein Mobiltelefon bereit. Nehmen Sie es nachts mit ins Schlafzimmer. Denken Sie daran, dass ein Einbrecher die Telefonkabel durchtrennen und einen Festnetzanschluss unbrauchbar machen kann.

Fluchtplan bei Feuer

- Alle Schlafzimmer sowie der Küchen- und Garagenbereich sollten über Rauchmelder und CO_2-Sensoren verfügen.
- In jedem Stockwerk sowie im Küchen- und Garagenbereich sollte ein Mehrzweckfeuerlöscher vorhanden sein.
- Alle Familienmitglieder sollten üben, wie sie das Gebäude bei Ausbruch eines Feuers so schnell wie möglich verlassen können. Mit Stahlstäben gesicherte Türen und Fenster müssen von innen leicht zu öffnen sein.
- Für die Evakuierung mehrstöckiger Gebäude sollte an geeigneter Stelle eine Abstiegshilfe parat liegen.
- Am Haupttelefon des Gebäudes sollten die Notfallnummern angeschrieben, in den Smartphones die wesentlichen Erreichbarkeiten gespeichert sein.

Dienstleister

- Beauftragen Sie nur Personen oder Unternehmen, die einen guten Ruf genießen und verlässliche Referenzen vorweisen können. Überprüfen Sie diese Referenzen.
- Lassen Sie gegebenenfalls das Personal durch Sicherheitsspezialisten überprüfen.
- Lassen Sie unangemeldetes Servicepersonal nicht ins Haus.
- Servicepersonal sollte sich stets mit einer Kennkarte des Arbeitgebers ausweisen können.
- Haushaltshilfen oder Personen, die sich regelmäßig im unmittelbaren Umfeld der Familie aufhalten, sollten vor ihrer Anstellung mit einem Background-Check überprüft werden. Sie sollten außerdem Erste-Hilfe-Maßnahmen beherrschen und den Evakuierungsplan kennen.
- Lassen Sie sich von diesem Personal einmal jährlich ein aktuelles Polizeiliches Führungszeugnis und eine Schufa-Auskunft vorlegen.
- Besprechen Sie im Beisein des Hauspersonals niemals vertrauliche Themen, wie geschäftliche und finanzielle Transaktionen, Privat- oder Geschäftsvermögen, persönliche Probleme, Reisevorhaben usw.
- Achten Sie darauf, dass Sie keine vertraulichen Informationen liegen lassen, die für das Hauspersonal leicht einsehbar oder zugänglich sind.

Sicherheit für Ihre Kinder

- Recherchieren Sie im Internet oder erkundigen Sie sich bei der örtlichen Polizeidienststelle, ob in Ihrer Gegend Sexualstraftäter leben.

- Sprechen Sie mit Ihren Kindern über mögliche Gefahren und über Sicherheitsmaßnahmen. Bringen Sie ihnen bei, wachsam zu sein und in potenziell gefährlichen Situationen richtig zu reagieren.

- Bringen Sie Ihren Kindern auch bei, dass sie nicht jedem vertrauen können und dass sie nicht mit Fremden sprechen oder auf sie zugehen sollen. Erklären Sie ihnen, dass sie nicht mit Älteren alleine sein oder mitgehen sollen.

- Lernen Sie die Freunde Ihrer Kinder und deren Eltern kennen, insbesondere, wenn es sich um enge Freunde handelt. Sie sollten auch andere Bezugspersonen Ihrer Kinder wie Trainer, Lehrer, Jugendgruppenleiter usw. kennen.

- Weisen Sie Ihre Kinder an, unbekannten Anrufern niemals unbedacht Auskünfte wie „Meine Eltern sind nicht da" zu geben.

- Stellen Sie sicher, dass Sie immer wissen, wo sich Ihre Kinder gerade aufhalten und dass sie sich von selbst bei Ihnen oder einem verantwortlichen Erwachsenen melden.

- Ihre Kinder sollten dafür sensibilisiert sein, ob sie verfolgt oder beobachtet werden oder ob sich ihnen jemand ungebührlich nähert. Falls sie etwas Verdächtiges bemerken, sollten sie sich sofort an einen sicheren Ort wie ein Geschäft, eine Bank oder eine Behörde begeben. Ist dies nicht möglich, sollten sie durch lautes Rufen auf sich und den mutmaßlichen Verfolger aufmerksam machen.

- Kinder sollten niemals zu Fremden ins Auto steigen.

- Vereinbaren Sie mit Ihren Kindern ein Codewort, das Sie benutzen, wenn ein Dritter sich um die Kinder kümmern soll, weil Sie selbst verhindert sind.

- Sensibilisieren Sie Ihre Kinder für die Gefahren im Internet. Setzen Sie sich mit den Anwendungen Ihrer Kinder auf Kommunikationsgeräten auseinander und prüfen Sie, welche Funktionen kritisch sind.

- Die Nutzung oder Anschaffung eines gepanzerten Fahrzeugs ist teuer, aber in manchen Situationen notwendig.

- Schulungen in sicherheitsgerechtem Fahren sind nützlich, damit Sie in gefährlichen Situationen richtig reagieren.

- Denken Sie daran, dass Sie durch ein auffälliges und teures Fahrzeug eher Gefahr laufen, Opfer eines Verbrechens zu werden.

- Es ist sicherer, während des Fahrens Fenster geschlossen und Türen verriegelt zu lassen.

- Machen Sie alle Autofenster zu und schließen Sie Ihr Fahrzeug beim Parken immer ab, insbesondere nachts.

- Transportieren Sie Wertgegenstände niemals so, dass sie von außen erkennbar sind. Verstauen Sie Pakete im Kofferraum, und verbergen Sie Handtaschen im Fußraum.

- Statten sie Ihr Fahrzeug mit einer Alarmanlage und/oder einem Notrufsender aus. Achten Sie darauf, dass sie den Notruftaster gut erreichen können, um bei einer bedrohlichen Situation schnell alarmieren zu können.

- Sorgen Sie dafür, dass Ihr Kraftstofftank immer gefüllt ist. Die Tankklappe sollte abschließbar sein.

- Halten Sie beim Fahren, an der Ampel sowie beim Parken immer Abstand, damit Sie genügend Platz zum Ausscheren haben und nicht am Wegfahren gehindert werden können.

Entführung und Erpressung

- Sowohl Einzelpersonen als auch Familien können durch präventive Maßnahmen das Risiko einer Entführung verringern. Entführungen, mit denen Lösegeld erpresst werden soll, finden meist unter der Woche, morgens und in aller Öffentlichkeit, auf dem Weg zwischen der Wohnung und der Arbeitsstelle bzw. Schule des Opfers, statt. Entführer observieren ihre Opfer meist über einen längeren Zeitraum und machen sich vorhersehbare Gewohnheiten zunutze.

- Ändern Sie deshalb ab und zu Ihre Gewohnheiten, seien Sie stets wachsam und reaktionsbereit!

- Variieren Sie Uhrzeiten, Strecken, Bewegungsmuster, Transportmittel, Aufenthaltsorte und alle Aktivitäten, die Rückschlüsse darauf zulassen, wo Sie sich zu einer bestimmten Zeit befinden.

- Beobachten Sie Ihr Umfeld aufmerksam und kritisch. Prägen Sie sich das normale Erscheinungsbild Ihrer Umgebung gut ein und achten Sie auf ungewöhnliche oder potenziell gefährliche Dinge. Nehmen Sie verdächtige Nummernschilder oder unbekannte Personen bewusst zur Kenntnis.

- Überlegen Sie, wie Sie reagieren könnten und handeln Sie unverzüglich, wenn Ihnen etwas oder jemand verdächtig erscheint.

- Prägen Sie sich entlang Ihrer üblichen Wege sichere Anlaufstellen wie Polizeidienststellen, Behörden oder Krankenhäuser ein.

- Achten Sie darauf, wo Ihre üblichen Routen gefährliche Stellen aufweisen, wie enge Kurven, scharfe Einmündungen oder Abschnitte, an denen die Sicht nach vorne und hinten nicht wenigstens mehrere Fahrzeuglängen beträgt.

- Teilen Sie, sofern nicht unbedingt nötig, niemandem persönliche Informationen über Finanzen, Vermögensverhältnisse, Investitionen oder Geschäftsvorhaben mit. Halten Sie auch Familienmitglieder und Kollegen dazu an, stets vertraulich mit solchen Angaben umzugehen.

- Empfangen Sie keine unangemeldeten Besuche und öffnen Sie keinesfalls sofort die Türe.

- Reagieren Sie niemals sofort oder direkt auf Erpressungsversuche. Die meisten Erpresser geben mit der Zeit bei ihren Forderungen nach, wenn sie merken, dass der Verhandlungspartner professionell reagiert. Verständigen Sie gegebenenfalls die Polizei.

- Wenden Sie sich bei versuchten oder vollendeten Entführungen bzw. Erpressungen an einen Sicherheitsspezialisten.

- Leisten Sie bewaffneten Entführern keinen Widerstand.
- Bleiben Sie im Falle einer Entführung ruhig und leisten Sie den Anweisungen genau Folge.
- Versuchen Sie keinesfalls, Entführern ihre Vermummung vom Kopf zu reißen, um sie zu demaskieren.
- Machen Sie die Entführer rechtzeitig darauf aufmerksam, wenn Sie Medikamente benötigen, die Sie regelmäßig nehmen müssen.

Vertraulichkeit Ihrer Daten

- Weisen Sie Kinder und Haushaltshilfen an, den Familiennamen erst dann am Telefon zu nennen, wenn sich der Anrufer selbst vorgestellt hat.
- Nennen Sie in der Ansage des Anrufbeantworters nicht den Familiennamen, sondern fordern Sie die Anrufer lediglich auf, eine Nachricht zu hinterlassen.
- Geben Sie niemals Fremden Ihre Telefonnummer, und beantragen Sie gegebenenfalls eine Geheimnummer.
- Geben Sie am Telefon oder im Internet nur dann persönliche Daten preis, wenn die Kontaktaufnahme von Ihnen ausgegangen ist und Sie die Person und/oder Organisation kennen, mit der Sie kommunizieren. Vertraulich zu behandeln sind insbesondere An- und Abwesenheitszeiten, Sozialversicherungsnummern, Geburtsdaten, Kreditkartennummern, Bankverbindungen, Angaben zu Krediten und Hypotheken sowie zu Krankenversicherungen.
- Bewahren Sie persönliche Informationen an einem abschließbaren, sicheren Ort auf und entsorgen Sie solche Unterlagen am besten im Reißwolf.
- Benutzen Sie einen verschließbaren Briefkasten, um Identitätsdiebstahl zu verhindern.
- Stellen Sie Ihren Computer an einem sicheren Ort auf, und beachten Sie die Sicherheitshinweise der folgenden Kapitel.
- Öffnen Sie keine E-Mails bzw. Anhänge unbekannter Absender, und besuchen Sie möglichst keine potenziell gefährlichen Websites.
- Verhalten Sie sich so anonym wie möglich, und machen Sie nicht öffentlich von sich reden. Vermeiden Sie, dass Ihr Name in Klatschspalten oder in Verzeichnissen von Wirtschaftsverbänden, Handelskammern usw. erscheint. Geben Sie keine Erklärungen an die Presse ab.
- Beantragen Sie eine „Übermittlungssperre für Kraftfahrzeugdaten" für Ihre Fahrzeuge sowie eine „Auskunftssperre im Melderegister" für Ihre persönliche Wohnanschrift.

Passwortsicherheit

- Legen Sie sich ein Passwortdatenblatt an, auf dem Sie alle wichtigen Passwörter notieren und schließen Sie dieses im Safe ein.

- Alle Passwörter, die Sie nur selten brauchen oder nur einmalig pro Gerät eingeben (Administrator, WPA/WPA2 für WLAN, etc.), sollten mindestens 20 Zeichen lang und völlig zufällig sein (auf dem Rechnerdatenblatt notieren).

- Versuchen Sie die Anzahl der aktiv zu merkenden Passwörter auf eines, zwei oder drei zu reduzieren. Dazu können Sie eine Passwort-Safe App oder die Passwortverwaltungsfunktionen Ihres Internetbrowsers benutzen.

- Passwort-Safe Programme gibt es in allen Preisklassen. Informieren Sie sich vor dem Kauf über den Hersteller und die Sicherheit des jeweiligen Programms.

- Für die Passwörter, die Sie sich aktiv merken müssen, verwenden Sie entweder Passwörter mit mindestens 8-12 Zeichen oder ganze Sätze aus mehreren Worten.

- Verwenden Sie keine gleichen Passwörter für mehrere Accounts.

- Ihr Passwort sollte aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen bestehen (alphanummerisches Passwort). Ersetzen Sie leicht zu merkende Buchstaben oder Wortlaute gegebenenfalls durch entsprechende Zahlen und Sonderzeichen.

- Verwenden Sie nie Namen von Familienmitgliedern, Haustieren, Geburtsdaten oder Begriffe rund um Hobbies, Lieblingsbücher und -filme, da sich solche Informationen unter Umständen einfach herausfinden lassen.

- Wählen Sie Ihr Passwort nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern, also z.B. nicht „1111", „asdfgh" oder „1234abcd".

- Es ist ebenfalls nicht ausreichend, einfach nur Ziffern am Anfang oder Ende eines ansonsten simplen Passwortes (z.B. Vorname eines Familienmitglieds) anzuhängen bzw. eines der üblichen Sonderzeichen zu ergänzen.

- Wenn Ihr System Umlaute zulässt, bedenken Sie bei Reisen ins Ausland, dass diese auf landestypischen Tastaturen eventuell nicht eingegeben werden können. Andererseits können schwer eingebbare Umlaute ein Passwort sinnvoll ergänzen.

- Verwenden Sie für Sicherheitsfragen keine öffentlich zugänglichen Informationen wie Geburtsdaten oder Vornamen aus dem Familienkreis. Im Idealfall geben Sie Phantasieantworten, die Sie auf dem Passwortdatenblatt notieren.

- Versenden Sie Ihre Passwörter nie in E-Mails und geben Sie diese nicht an Dritte weiter, da Sie ab diesem Zeitpunkt keine Kontrolle mehr über Ihre Accounts haben.

- Laden Sie regelmäßig System-Updates oder aktivieren Sie, sofern vorhanden, die automatische Update-Installation des jeweiligen Geräts.

- Geben Sie Internetadressen immer manuell ein oder verwenden Sie ein Lesezeichen bei dem Sie sicher sind, dass die Adresse korrekt geschrieben ist. Klicken Sie niemals direkt auf Links in E-Mails.

- Aktivieren Sie eine Festplattenverschlüsselung mit einem sicheren Passwort.

- Seien Sie vorsichtig, wenn Sie ein unbekanntes externes Speichermedium an Ihren Rechner anschließen. Zur Not lassen Sie sich die Informationen lieber per E-Mail senden.

- Deaktivieren Sie in keinem Fall die Firewall, auch nicht wenn eine Webseite oder ein Programm dies fordert.

- Stellen Sie sicher, dass der Benutzer-Account, mit dem Sie am Computer arbeiten, keine Verwaltungs- bzw. Administratorrechte besitzt.

- Erstellen Sie mehrere Benutzerkonten (Accounts), um wichtige Dinge wie Onlinebanking von anderen Anwendungen zu trennen.

- Löschen Sie regelmäßig „Cookies" in Ihrem Browser. Diese werden von den besuchten Webseiten auf Ihrem Computer gespeichert, um nutzerbezogene Werbung anzeigen zu können.

- Achten Sie auf Warnhinweise Ihres Gerätes.

- Nutzen Sie die Verschlüsselungsfunktionen von Word, Excel bzw. Ihrem Packprogramm (z.B. 7zip) zur Übertragung sensibler Dateien und versenden Sie das Passwort auf einem zweiten Übertragungsweg, z.B. als SMS.

- Erstellen Sie regelmäßig Backups auf externen Speichern (USB-Festplatte, Netzwerkserver).

- Installieren Sie einen „AdBlocker" für das Surfen im Internet, wenn Sie störende Werbung entfernen wollen und ein Tool wie „Ghostery", wenn Sie nicht wollen, dass Ihr Surfverhalten ausgewertet wird.

- Deinstallieren Sie eventuell installierte Flash-Plugins, wenn möglich.

- Nutzen Sie das Browser-Plugin „HTTPS Everywhere" der EFF, um beim Surfen im Internet nach Möglichkeit mit dem sichereren „SSL-Verfahren" auf Webseiten zuzugreifen.

- Aktivieren Sie die Festplattenverschlüsselung „File Vault". Notieren Sie den Wiederherstellungsschlüssel auf Ihrem Rechnerdatenblatt.
- Aktivieren Sie die Firewall.
- Erlauben Sie in den Systemeinstellungen die Installation von Programmen nur aus dem Mac App-Store.
- Stellen Sie sicher, dass Ihr Benutzer keine Verwaltungsrechte hat.
- Um gegen Datenverlust abgesichert zu sein, sollten Sie regelmäßig ein Backup Ihres PCs auf einer externen Festplatte mit dem Programm „Time Machine" durchführen.
- Stellen Sie sicher, dass in den Systemeinstellungen des App-Stores automatisch nach Updates gesucht wird und sowohl Apps, OSX als aus Systemdatendateien automatisch installiert werden.
- Verwenden Sie nach Möglichkeit immer die aktuellste Version des Betriebssystems OSX.
- Stellen Sie in den Einstellungen von Safari sicher, dass Internet-Plug-Ins deaktiviert sind, vor betrügerischen Inhalten gewarnt wird und Sichere Daten nach dem Laden NICHT sofort geöffnet werden.

- Arbeiten Sie von einem Account aus, der keine Administratorenrechte für den Computer besitzt.
- Verwenden Sie kein Betriebssystem, für das es keine Updates mehr gibt (z.B. Windows XP). Im Idealfall verwenden Sie ständig die neuesten Versionen.
- Installieren Sie ein Antivirus-Programm und aktualisieren Sie dieses regelmäßig. Nehmen Sie Warnungen Ihres Antivirus-Programmes ernst!
- Verwenden Sie einen Browser, der sich möglichst häufig aktualisiert und eine gute Sicherheitsbewertung hat.
- Prüfen Sie den Punkt „Sicherheit" im Windows Wartungscenter regelmäßig. (Windows-Suche nach „Wartungscenter")
- Achten Sie darauf, dass die Windows Firewall eingeschaltet ist. Im Idealfall werden alle eingehenden Verbindungen ohne Ausnahmen blockiert. (Windows-Suche nach „Firewall")
- Achten Sie darauf, dass Windows Updates automatisch installiert werden sobald sie verfügbar sind. (Windows-Suche nach „Updates")
- Verwenden Sie sämtliche Sicherheitsfunktionen die Ihre Betriebssystemversion bietet: Smartscreen, Benutzerkontensteuerung etc. Die Einstellungsmöglichkeiten finden Sie in der Windows-Suche unter dem jeweiligen Schlagwort.
- Installieren Sie das Programm EMET in der aktuellsten Version von der Microsoft Homepage aus.

- Die AppleID ist der Anmeldename, den Sie für alle Aktionen in Bezug auf Apple verwenden können. Geben Sie Ihre AppleID deswegen nie an andere weiter.

- Deaktivieren Sie unter „Einstellungen → Kontrollzentrum" alle Zugriffe auf den Sperrbildschirm.

- Wählen Sie ein Passwort mit mindestens 8-12 Stellen, verwenden Sie keine 4-stelligen PINs. Nutzen Sie den Fingerabdruck-Scanner „TouchID".

- Stellen Sie „Code anfordern" unter „TouchID & Code" auf „sofort".

- Aktivieren Sie „Mein iPhone suchen" auf mehreren Geräten (iPhone oder iPad) in der Familie, um ein verlorenes Gerät über einen Computer fernsperren oder fernlöschen zu können („Einstellungen → iCloud → Mein iPhone suchen" einschalten).

- Installieren Sie regelmäßig Software-Updates, die von Apple bereitgestellt werden.

- Lassen Sie Ihr iPhone nie in der Öffentlichkeit liegen oder geben es zum Telefonieren an Fremde heraus.

- Um das Speichern von personenbezogenen Informationen so weit wie möglich zu beschränken, sollten folgende Einstellungen vorgenommen werden:

  - „Einstellungen → Safari → Kein Tracking" einschalten. Alternativ können Sie auch den „Private"-Button in Safari benutzen.

  - „Einstellungen → Datenschutz → Werbung → Kein Ad-Tracking" einschalten.

  - „Einstellungen → Datenschutz → Ortungsdienste → Systemdienste → Ortsabhängige iAds" ausschalten, um keine Standortdaten zu übertragen.

- Um zu verhindern, dass sich Ihr iPhone oder iPad häufig besuchte Orte merkt, sollte diese Funktion deaktiviert werden. Gehen Sie dazu auf „Einstellungen → Datenschutz → Ortungsdienste → Systemdienste" und deaktivieren Sie „Häufige Orte".

Android Geräte

- Vom Gebrauch eines Android-Gerätes, sowohl im privaten als auch insbesondere im geschäftlichen Bereich, raten wir ab. Für Android sind wesentlich mehr schädliche Anwendungen im Umlauf als für andere Betriebssysteme und die Möglichkeiten sich zu schützen sind beschränkt.

Windows Phones

- Aufgrund der relativ geringen Verbreitung und des niedrigen weltweiten Marktanteils können wir zu diesem Betriebssystem zurzeit noch keine Sicherheitshinweise geben.

Social Networks

- Informieren Sie sich über die Datenschutzrichtlinien und die Erfahrungen anderer Nutzer (User), bevor Sie sich bei einem sozialen Netzwerk anmelden.
- Achten Sie auf die Seriosität des Anbieters.
- Gehen Sie vorsichtig mit Ihren Daten um. Dies macht es Dritten schwerer, ein Persönlichkeitsprofil von Ihnen zu erstellen.
- Verwenden Sie ein sicheres alphanummerisches Passwort (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen), um sich vor Identitätsdiebstahl zu schützen.
- Denken Sie bei allem, was Sie online schreiben und hochladen, an Ihre Zukunft.
- Klicken Sie nicht auf Links und öffnen Sie keine Dateien, die Ihnen über das Netzwerk geschickt werden.
- Verabreden Sie sich mit niemandem, den Sie nicht persönlich kennen. Wenn dies Ihr Ziel ist, beachten Sie bitte die Sicherheitshinweise zum Online Dating.
- Laden Sie keine Bilder hoch, auf denen Sie eindeutig identifiziert werden können oder auf denen Personen zu sehen sind deren Zustimmung Sie nicht besitzen.
- Geben Sie nie preis, wann und wie lange Sie das Haus verlassen oder niemand zu Hause ist. Insbesondere Hinweise, die einen Rückschluss darauf zulassen, dass Sie längere Zeit im Urlaub sind, bergen die Gefahr, dass Kriminelle dies für einen Einbruch, Identitätsdiebstahl oder zur Verwendung Ihres Profils ausnutzen.
- Ändern Sie bei Bedarf die Privatsphäre-Einstellungen Ihres Profils so, dass niemand außer Ihren Freunden Ihr Profil sehen und lesen kann.
- Akzeptieren Sie keine Freundesanfragen von Leuten, die Sie nicht persönlich (gut) kennen bzw. eindeutig identifizieren können.

- Geben Sie zur Registrierung bei einem Online-Spiel nie Ihre private E-Mail-Adresse an, sondern erstellen Sie einen neuen, neutralen E-Mail-Account, den Sie ausschließlich für Spiele verwenden.

- Geben Sie außerdem keine persönlichen Informationen an.

- Für den Fall, dass Informationen wie Name oder Geburtsdatum erforderlich sind, erfinden Sie falsche Daten, um zu verhindern, dass persönliche Informationen eventuell gespeichert oder anderweitig genutzt werden.

- Öffnen Sie außer erforderlichen Bestätigungsmails keine anderen E-Mails, die Ihnen von einem Anbieter zugeschickt werden.

- Klicken Sie nicht auf Links und öffnen Sie keine Dateien, die Ihnen von Dritten mit Bezug zu einem solchen Spiel zugeschickt werden
.

- Geben Sie niemals Ihr Passwort weiter, auch nicht, wenn sich jemand als „Support" ausgibt und nach Ihrem Passwort frägt.

- Laden Sie nur Dateien aus vertrauenswürdigen Quellen von seriösen Spieleanbietern herunter und meiden Sie illegale Tauschbörsen, um Schadsoftware zu vermeiden. Bevorzugen Sie die internen Aktualisierungsfunktionen der Spielesoftware.

- Bevor Sie ein Abo für ein Spiel abschließen, informieren Sie sich über die Kündigungsfrist und lesen Sie alle wichtigen Informationen aufmerksam durch.

- Achten Sie darauf, die Installation oder ein Spiel nicht zu starten, wenn auf Ihrem PC im Hintergrund gerade Onlinebanking-Seiten oder andere vertrauliche Dienste geöffnet sind.

- Lesen Sie sich die Sicherheitstipps Ihrer Bank durch und befolgen Sie diese, nicht zuletzt aus Haftungsgründen.

- Beobachten Sie Ihre Kontobewegungen regelmäßig. Wenn Sie eine unerlaubte Kontobewegung feststellen, lassen Sie Ihr Konto sofort sperren.

- Wenn Sie für bestimmte Konten kein Onlinebanking benötigen, deaktivieren Sie dieses.

- Wenn Sie eine Onlinebanking-Software oder -App nutzen wollen, die nicht direkt von Ihrer Bank stammt, recherchieren Sie zuvor deren Sicherheit in unabhängigen Testberichten.

- Nutzen Sie Onlinebanking nur über vertrauenswürdige Netzwerke. Vermeiden Sie den Zugriff in Internetcafés, über Hotel-WLANs oder andere öffentliche Netzwerke.

- Achten Sie auf eine verschlüsselte Kommunikation (https-Protokoll). Dies ist meist an einem Schloss in der Adresszeile erkennbar.

- Klicken Sie nicht auf Links (z.B. in E-Mails, SMS oder MMS), die Ihre Kontodaten abfragen, Sie vor Kontobewegungen warnen oder in sonstigem Zusammenhang mit Zahlungsverkehr stehen. Öffnen Sie Ihre Online-Konten ausschließlich durch manuelle Eingabe in der Adresszeile oder aus Ihren Bookmarks.

- Werden Sie misstrauisch, wenn sich die gewohnten Abläufe während des Banking-Vorganges ändern, zum Beispiel:

  - Aufforderung, mehrere TANs einzugeben

  - Plötzlicher Abbruch der Webseite nach Eingabe einer TAN

  - Browser schließt sich scheinbar grundlos während des Online-bankings

- Melden Sie Unregelmäßigkeiten und Auffälligkeiten sofort Ihrem Kreditinstitut und lassen Sie im Zweifel Ihr Konto sperren.

- Legen Sie ein Limit für tägliche Geld-Transaktionen fest, um möglichen Schaden zu begrenzen.

- Wurden Sie Opfer eines Angriffs auf Ihr Konto, legen Sie bei Ihrer Bank Widerspruch gegen die falsche Abbuchung ein und beantragen Sie eine Rückbuchung. Schalten Sie gegebenenfalls die Polizei, einen Rechtsanwalt sowie IT-Sicherheitsspezialisten ein.

- Prüfen Sie bei SMS-TAN Verfahren die mit der SMS übermittelten Empfängerdaten nochmals auf Richtigkeit, bevor Sie die Transaktion freigeben.

- Richten Sie einen Spamfilter ein.
- Seien Sie misstrauisch bei E-Mails, die in Ihrem Spamordner landen, und klicken Sie nicht auf die enthaltenen Links oder Anhänge.
- Auch von Menschen, die Sie persönlich kennen, kann Spam kommen der mit Schadsoftware infiziert sein könnte.
- Wenn Sie von der E-Mail-Adresse eines Bekannten Spam bekommen, informieren Sie ihn, da sein Computer möglicherweise mit Schadsoftware infiziert ist.
- Reagieren Sie nicht auf Rechnungen für Dienste, die Sie nicht in Anspruch genommen haben.
- Seien Sie vorsichtig, wenn Sie E-Mails von unbekannten Absendern erhalten.
- Idealerweise klicken Sie niemals direkt auf Links in E-Mails. Diese können gefälscht sein, um Sie in Sicherheit zu wiegen. Zur Not kontrollieren Sie Links, die Ihnen zugeschickt wurden, indem Sie mit der Maus über den Link fahren. Es erscheint ein Popup, in dem die tatsächliche Internetadresse angezeigt wird, auf die Sie beim Click auf den Link geführt werden.
- Überprüfen Sie genau, ob die in der E-Mail angegebenen Daten stimmen. Fehler in der Ansprache beim Vor- und Nachnamen sowie Grammatik- und Rechtschreibfehler können auf eine Fälschung hindeuten.
- E-Mail-Layouts von bekannten und häufig genutzten Diensten wie Amazon, eBay oder PayPal werden oft gefälscht, um Sie auf andere gefälschte Webseiten zu locken. Geben Sie dort niemals persönliche Daten oder Passwörter preis, auch nicht wenn Sie dort dazu aufgefordert werden. Fragen Sie im Zweifel telefonisch beim Anbieter nach.
- Lesen Sie sämtliche E-Mails aufmerksam durch. Löschen Sie alles, was Ihnen verdächtig vorkommt und lassen Sie sich nicht von angeblicher Dringlichkeit dazu verleiten, übereilt oder unvorsichtig zu handeln.
- Prüfen Sie, ob die Verschlüsselungsoptionen SSL oder TLS für Ihren E-Mail-Account in den Einstellungen aktiviert sind.

- Erstellen Sie für die Anmeldung und Kommunikation einen neuen E-Mail-Account, dessen Adresse keine persönlichen Informationen enthält. Wenn Sie den Account nicht mehr benötigen, ist es so einfacher, ihn komplett stillzulegen.

- Geben Sie in Ihrem Datingprofil weder Ihren echten Namen noch Ihren wahren Wohnort preis.

- Verwenden Sie nach Möglichkeit ein Prepaid Mobiltelefon bei der Kontaktaufnahme mit dem Datingpartner und vermeiden Sie es Ihr persönliches Mobiltelefon einzusetzen, um bei Bedarf anonym bleiben zu können.

- Bringen Sie Ihr Datingprofil nicht mit einem Account auf sozialen Netzwerken in Verbindung, da dieser zu viele persönliche Informationen enthalten könnte.

- Seien Sie misstrauisch! Ihr Chatpartner muss nicht die Wahrheit erzählen. Wenn Ihnen etwas komisch vorkommt, brechen Sie den Kontakt ab.

- Bevor Sie sich mit jemandem treffen, fragen Sie nach einem Foto und überprüfen Sie die Person im Internet mittels einer gängigen Suchmaschine.

- Lassen Sie sich beim ersten Date nicht von zu Hause abholen, sondern treffen Sie sich zu einer normalen Uhrzeit (untertags oder früher Abend) in der Öffentlichkeit.

- Teilen Sie einer dritten Person mit, wo und wie lange Sie sich mit dem Datingpartner treffen.

- Machen Sie beim Date deutlich, dass jemand weiß, wo Sie sich befinden. Lassen Sie sich während des Treffens anrufen oder nehmen Sie anfangs einen Freund mit und verabreden Sie sich im Beisein des Datingpartners für später.

- Nehmen Sie Ihr Handy überall mit hin.

- Achten Sie auf Ihr Getränk, damit niemand unbemerkt etwas hineinschütten kann. Haben Sie Ihr Getränk unbeaufsichtigt gelassen, dann bestellen Sie vorsichtshalber ein neues.

- Wenn Sie Ihr Profil nicht mehr benötigen, z.B. weil Sie einen Partner gefunden haben, sollten sie Ihr Datingprofil löschen und die zugehörige E-Mail-Adresse stilllegen.

- Seien Sie vorsichtig, was Sie in Chats schreiben. Alle Äußerungen in einem öffentlichen Chatroom können auch Jahre später noch gelesen werden. Denken Sie beim Schreiben an Ihre Zukunft.

- Geben Sie keine persönlichen Informationen wie Nachname, Geburtsdatum oder Adresse preis.

- Behandeln Sie persönliche Informationen von Freunden und Verwanden mit derselben Vorsicht wie Ihre eigenen.

- Werden Sie misstrauisch, wenn ein Fremder anfängt Sie auszufragen.

- Verwenden Sie keine kompromittierenden Profilbilder oder Bilder, auf denen Sie eindeutig zu identifizieren sind.

- Vertrauen Sie niemandem, der Ihnen nicht persönlich bekannt ist, auch nicht wenn er vorgibt einen Verwandten oder Freund von Ihnen zu kennen.

- Teilen Sie niemandem mit, wann und wie lange Sie das Haus verlassen.

- „Nicknames" in Chatrooms sollten nicht den eigenen Namen oder andere Informationen wie z.B. das Geburtsdatum enthalten.

- Wichtige Informationen sollten Sie nie in einem unverschlüsselten Chat austauschen.

- Für verschlüsselte Chats bietet sich die für iOS und Android erhältliche App „Threema" an. Für den PC gibt es die unterschiedlichsten Programme und Plugins, die Chats verschlüsseln.

Sichere Zahlungsmittel im Internet

- Im Internet existieren verschiedene Zahlungsmöglichkeiten. Seien Sie sich bewusst, dass nicht alle gleich sicher sind.

- Als anonyme Bezahlart gibt es z.B. die PaySafeCard, die im Wert von 10, 25, 50 und 100 Euro an Tankstellen und Lottoannahmestellen erhältlich ist. Mittels eines 16-stelligen Codes kann man sofort bezahlen. Aktuell wird die PaySafeCard in vielen Shops als Zahlungsmittel akzeptiert.

- Eine weitere bekannte Option, jedoch nicht anonym, ist PayPal, welches in den meisten Onlineshops als Zahlungsmöglichkeit wählbar ist. Aktivieren Sie die SMS-Bestätigung, wenn Sie PayPal verwenden, um Missbrauch vorzubeugen.

- Informieren Sie sich, welche Zahlungsmittel für einen spezifischen Onlineshop zugelassen sind.

- Von den meisten Finanzinstituten werden auch PrePaid-Kreditkarten für den Privatgebrauch angeboten. Dies begrenzt zumindest das Limit, falls einmal Missbrauch mit Ihren Daten betrieben werden sollte.

- Für detailliertere Informationen empfehlen wir die Webseite des Bundesamtes für Sicherheit in der Informationstechnik: www.bsi-für-bürger.de.

- Dort bekommen Sie Informationen zu folgenden Themen:
  - Wie mache ich meinen PC sicher?
  - Welche Gefahren begegnen mir im Netz?
  - Wie bewege ich mich sicher im Netz?
  - Wie bewege ich mich sicher im mobilen Netz?

- Beachten Sie die aktuellen Warnungen des BSI und informieren Sie sich regelmäßig im Internet zu den aktuellen Hacker-Angriffen.

- Zum Thema E-Mail-Sicherheit bietet die Webseite www.netzwelt.de/software/email-sicherheit.html einen umfangreichen News-Feed mit Lösungsvorschlägen.

- Ein gutes technisches Newsportal zum Thema IT-Sicherheit bietet der heise-Verlag: www.heise.de/security/

IT-Sicherheit auf Reisen

- Nehmen Sie nur die IT-Geräte mit, die für Sie unverzichtbar sind. Verschlüsseln Sie alle darauf gespeicherten sensiblen Daten. Führen Sie sensible Unterlagen bzw. Geräte mit sensiblen Informationen ausschließlich im Handgepäck mit sich. Bei besonderer Gefährdung lassen Sie bitte keine Geräte (Handy, Laptop, Tablet) mit sensiblen Informationen im Hotelsafe, sondern führen Sie wichtige Dokumente und Gegenstände (z.B. Laptop) ständig mit sich.

- Aktivieren Sie unbedingt die Passwortabfrage für alle Benutzerkonten Ihres Laptops, Tablets und Smartphones, sodass sich der Nutzer bei Neustart des Gerätes, beziehungsweise beim Wechseln vom gesperrten in den aktiven Modus, authentifizieren muss.

- Erstellen Sie vor der Reise eine Datensicherung auf einem externen Speichermedium und lassen Sie diese Daten an einem sicheren Ort zu Hause.

- Schalten Sie Ihr Heim-WLAN während Ihrer Abwesenheit aus. Die WLAN-Funktion finden Sie im Einstellungsmenü Ihres Routers.

- Vermeiden Sie die Eingabe vertraulicher Daten an öffentlich zugänglichen Computern und verzichten Sie auf Onlinebanking und -shopping in Hotels, Internetcafés sowie an anderen öffentlichen Computern. Verzichten Sie auf die Bearbeitung sensibler Informationen im Ausland.

- Wenn Sie auf fremden Geräten wichtige Dateien bearbeiten, speichern Sie diese regelmäßig (auch während der Bearbeitung) auf externen Medien wie USB-Sticks ab. Löschen Sie Informationen, die Sie auf fremden oder öffentlich zugänglichen Computern gespeichert haben, sorgsam.

- Achten Sie darauf, dass Ihre Daten verschlüsselt übertragen werden. Dies ist daran erkennbar, dass die Adresse der Seite mit „https://" beginnt.

- Sichern Sie Daten, die Online-Einkäufe oder Buchungen betreffen, auf einem externen Speichermedium oder drucken Sie sie aus.

- Unter „Social Engineering" versteht man die zwischenmenschliche Beeinflussung, meist unter Verwendung einer falschen Identität, mit dem Ziel, unberechtigt an Informationen oder technische Infrastrukturen zu gelangen. Dabei werden häufig weibliche Lockvögel oder vermeintliche „Kollegen aus der gleichen Branche" eingesetzt. Von der Begleitung oder Einladung flüchtiger Bekanntschaften und Prostituierten ist daher dringend abzuraten. Da häufig auch Betäubungsmittel oder sog. „k.o.-Tropfen" zum Einsatz kommen, sollten Sie sich nicht zu Drinks einladen lassen und Ihr Getränk im Auge behalten.

- Vermeiden Sie die Nutzung von Fernzugriffsmöglichkeiten (z.B. VPN- oder Webmail-Zugänge) Ihres Unternehmens, die nur durch einfache Passworteingabe geschützt sind. Führen Sie Geräte für eine Zwei-Faktor-Authentisierung (Token, Chipkarte, Smartphone) ständig mit sich. Verwenden Sie keine fremden Geräte für einen Zugriff auf Firmendaten (z.B. Webmail-Zugriff im Internetcafé oder Computer eines Geschäftspartners).

- Benutzen Sie keine unverschlüsselten Verbindungen in ungesicherten Netzen (Hotel-WLAN etc.). Übermitteln Sie keine kritischen Daten über ungesicherte Kanäle (Telefon, Fax, ungesicherte Internetverbindungen). Achten Sie auf ungewöhnliche Meldungen und brechen Sie im Zweifelsfall den Kommunikationsvorgang ab.

- Ändern Sie Ihre Passwörter vor und nach Reiseantritt. Führen Sie keinesfalls Passwörter in ungeschützter Form mit sich (Zettel, Notizen oder Kontakte im Handy). Geben Sie Ihr Passwort nur verdeckt ein, Sie werden womöglich beobachtet oder gefilmt. Verwenden Sie eine Sichtschutzfolie für Ihre technischen Geräte.

- Aktualisieren Sie das Betriebssystem sowie die Virenschutz- und Sicherheitssoftware Ihrer Geräte vor Reiseantritt.

- Verwenden Sie keinesfalls USB-Geräte, die Ihnen im Ausland geschenkt bzw. überlassen wurden. Diese können mit Schadsoftware infiziert sein. Bei besonderer Gefährdung verzichten Sie im Ausland generell auf die Verwendung tragbarer Datenträger (USB-Sticks, SD-Karten etc.). Nehmen Sie keine technischen Geschenke im Ausland an bzw. vernichten Sie diese bei nächster Gelegenheit. Solche Geschenke enthalten eventuell Malware oder Spionageequipment.

- Geben Sie Ihre technischen Geräte bzw. Mobile Devices (Smartphones oder ähnliches, inkl. USB-Sticks und -Festplatten, SD-Karten) grundsätzlich nicht aus der Hand und lassen Sie sie nicht unbeaufsichtigt liegen. Vermeiden Sie es, Ihre mobilen Geräte und Datenträger per USB mit fremden Ladegeräten oder fremden Computern zu verbinden.

- Bewahren Sie rezeptpflichtige Medikamente in der Originalverpackung und zusammen mit einer Kopie des Rezepts auf. Wenn Sie regelmäßig Medikamente einnehmen müssen, führen Sie auf Reisen immer einen größeren Vorrat mit sich, sodass Sie auch versorgt sind, wenn etwas Unvorhergesehenes passiert.

- Lassen Sie auffällige Gegenstände wie Schmuck, goldene Uhren und teure Gepäckstücke zu Hause. Mit solchen Wertgegenständen können Sie ungewollt Aufmerksamkeit erregen und das persönliche Risiko erhöhen.

- Tragen Sie keine Finanzbelege bei sich, die auf Ihren Wohlstand hindeuten.

- Tragen Sie keine Ausweise bei sich, die Sie mit der Polizei oder dem Militär in Verbindung bringen könnten.

- Meiden Sie Gebiete oder Einrichtungen, die von Militärpersonal jeglicher Nation frequentiert werden.

- Tragen Sie Ihren Reisepass sowie die Telefonnummer und Adresse der nächsten Botschaft bzw. des nächsten Konsulats bei sich.

- Informieren Sie sich vorab über die Länder, in die Sie reisen. Beachten Sie die lokalen Gesetze, religiösen Traditionen, Bräuche, Geschäftspraktiken und Verhaltensregeln.

- Bringen Sie vor der Reise oder direkt nach Ihrer Ankunft den Wechselkurs der Landeswährung in Erfahrung. Informieren Sie sich, wo, wann und wie Sie Geld wechseln können.

- Erkundigen Sie sich, wie das örtliche Telefonsystem funktioniert und halten Sie die lokalen Notrufnummern parat.

- Besprechen Sie persönliche oder geschäftliche Angelegenheiten nicht mit Fremden.

- Führen Sie vor allem in heißen Gebieten immer ausreichend Flüssigkeit mit sich und trinken Sie regelmäßig.

- Holen Sie Informationen über Ihr Reiseziel ein. Im Internet können Sie auf den Seiten des Auswärtigen Amtes über jedes Land und bestimmte Regionen viele Informationen über örtliche, religiöse und gesellschaftliche Gebräuche, das landesübliche Geschäftsgebaren, sonstige Verhaltensregeln, besondere Gefahren, Währungen, Wechselkurse und Visabestimmungen nachlesen.

- Es gilt die allgemeine Regel: je exotischer das Ziel, je mehr sich die Kultur des Ziellandes von unserer unterscheidet, umso wichtiger ist die Vorbereitung der Reise und die Einhaltung der Hinweise und Verhaltensregeln während der Reise.

- Bereiten Sie ein Informationsblatt mit den wichtigsten Hinweisen und Telefonnummern für den Notfall vor. Es dient Ihnen und ggf. Hilfspersonen, sofort die richtigen Maßnahme einzuleiten, um Gefahren abzuwehren und Folgen zu mindern. Für den Notfall sollten Sie Sorge tragen, dass Sie auf diese Telefonnummern im Mobiltelefon Zugriff haben.

- Für den medizinischen Notfall wird der Abschluss einer privaten Reisekrankenversicherung dringend empfohlen. Diese sollte eine 24/7-Hotline und die Rückholung im Krankheitsfall beinhalten, wenn sie medizinisch sinnvoll und vertretbar ist, wenn aufwändige Behandlungen erforderlich werden oder wenn ein stationärer Aufenthalt von mehr als 14 Tagen absehbar ist.

- Von folgenden Dokumenten sollten Sie Kopien anfertigen und im Reisegepäck getrennt von den Originaldokumenten mitführen oder elektronisch so ablegen, dass Sie im Bedarfsfall über das Internet hierauf zugreifen können: Reisepass, Personalausweis, Visum, Tickets, Hotelbuchung, Kreditkarten usw. Die Kopien können bei Verlust der Originaldokumente sehr hilfreich sein, um sich auszuweisen sowie Ersatzdokumente zu beschaffen und Kreditkarten zu sperren.

- Denken Sie rechtzeitig an die Beantragung notwendiger VISA und prüfen Sie die Gültigkeit Ihres Passes.

- Führen Sie persönlich notwendige Medikamente in ausreichender Menge im Handgepäck mit. Bewahren Sie verschreibungspflichtige Medikamente in der Originalverpackung zusammen mit einer Kopie des Rezeptes auf.

- Beachten Sie die Hinweise zur Sicherheit der IT auf Reisen.

- Planen Sie soweit wie möglich Ihre Reise auch unter Gesichtspunkten der Sicherheit. Vermeiden Sie es allein unterwegs zu sein. Versuchen Sie bestimmte Dinge im Voraus zu organisieren, z.B. den Transfer vom Flughafen ins Hotel und zum Geschäftsort.

- Verschließen Sie Ihre Koffer und beaufsichtigen Sie ständig Ihr Gepäck.
- Hartschalenkoffer beugen dem weltweit verbreiteten Aufschlitzen von Gepäckstücken vor.
- Das Gepäck sollte immer außen und innen identifizierbar sein. Bringen Sie außen verdeckt nur Ihren Namen und Telefonnummern an.
- Benutzen Sie nur lizensierte Taxis.
- Wenn Sie vom Flughafen abgeholt werden, sollten Sie ein Erkennungszeichen vereinbaren. Ihnen sollten die Person und/oder das Auto (Typ, Farbe, KFZ-Kennzeichen) bekannt sein. Es sollte vermieden werden, dass bei der Abholung am Flughafen ein Schild mit Ihrem Namen oder ihrem Unternehmen hochgehalten wird.
- Ihr Gepäck sollte neutral sein, d. h. nichts über Sie, Ihren Status, Ihr Unternehmen oder Ihre Zugehörigkeit aussagen.
- Führen Sie kein Gepäck anderer Personen mit sich.

- Fertigen Sie vor Ihrer Abreise für Ihren Ehegatten und Ihr Büro eine lückenlose Aufstellung der Flüge und der Hotelunterkünfte an. Teilen Sie alle Änderungen unverzüglich mit.

- Ihr Gepäck sollte keinen Aufschluss über Ihre Position, Ihr Unternehmen oder sonstige Verbindungen geben. Auf dem Gepäckanhänger sollten nur Ihr Name und Ihre Telefonnummer stehen. Zeigen Sie Ihr Firmenlogo nicht auf Gepäckanhängern, Kleidungsstücken, Taschen oder sonstigen augenfälligen Gegenständen.

- Packen und verschließen Sie Ihr Gepäck selbst, sodass Sie den genauen Inhalt kennen. Halten Sie gepackte Taschen und Koffer verschlossen und lassen Sie diese nicht unbeaufsichtigt, bis Sie sie am Flughafen abgeben.

- Nehmen Sie von Dritten weder Gepäck noch Pakete zur Beförderung an.

- Rufen Sie spätestens zwei Stunden vor Abflug bei der Fluggesellschaft an und lassen Sie sich die Abflugzeit bestätigen.

- Halten Sie sich bis zum Einsteigen in einem Sicherheitsbereich auf, und lassen Sie Ihre persönlichen Sachen nicht unbeaufsichtigt.

- Meiden Sie Personen, die von der Fluggesellschaft mit besonderer Aufmerksamkeit bedacht werden.

- Wählen Sie im Flugzeug einen Sitz in der Nähe einer Tragfläche oder eines Notausgangs. Setzen Sie sich nicht an den Gang oder in die Nähe der Eingänge.

- Achten Sie bei der Ankunft darauf, ob jemand offenkundig durch Beobachtung der Umgebung oder auffälliges Interesse an Gepäckanhängern nach möglichen Zielen sucht.

- Wenn Sie am Flughafen erwartet werden, sollten Sie wissen, wer Sie abholt und wie die Person ungefähr aussieht. Gehen Sie nicht mit jemandem mit, der nicht auf die Beschreibung passt oder behauptet, anstelle einer anderen Person geschickt worden zu sein.

- Wenn Sie am Flughafen einen Mitreisenden treffen wollen, warten Sie nicht in der Nähe von Abfallbehältern, da diese typischerweise dazu genutzt werden, Sprengkörper zu deponieren. Bleiben Sie auch unbeaufsichtigten Gepäckstücken oder Kisten fern. Verabreden Sie sich mit anderen Personen möglichst in Bereichen, die durch Zugangskontrollen geschützt sind, wie zum Beispiel Flughafenlounges.

- Wenn plötzlich auffällig viele uniformierte Sicherheitskräfte oder Polizeibeamte erscheinen, suchen Sie rasch Schutz an einer geeigneten Stelle, z.B. hinter einer Säule, einem großen Automaten oder Polstermöbeln.

- Machen Sie die nächstgelegenen Notausgänge ausfindig. Sollten Sie in einer Gruppe evakuiert werden, halten Sie sich in der Mitte der Gruppe, sodass Sie möglichst viele Leute um sich haben. Eilen Sie nicht voraus, und bleiben Sie nicht zurück.

- Bedenken Sie, dass sich bei einer Flugzeugentführung aus taktischen Gründen nicht immer alle Entführer sofort zu erkennen geben.

- Vermeiden Sie Blickkontakt zu Terroristen, insbesondere in den ersten 20 bis 60 Minuten nach der Übernahme des Flugzeugs.

- Sollten die Entführer Wertgegenstände und Pässe einsammeln, versuchen Sie nicht, irgendetwas zu verstecken oder zurückzuhalten.

- Verhalten Sie sich so ruhig und unauffällig wie möglich.

- Sprechen Sie nicht mit anderen Passagieren. Wenn Sie den Entführern den Eindruck vermitteln, dass Sie etwas vorhaben, werden sie Ihnen vermutlich etwas antun.

- Bitten Sie die Entführer nicht um Gefälligkeiten wie die Erlaubnis zu rauchen, den Sitz zu wechseln oder auf die Toilette zu gehen.

- Weigern Sie sich nicht, Essen, Getränke oder Tabak von einem Terroristen anzunehmen, aber nehmen Sie nur wenig davon zu sich. Wenn man Ihnen Alkohol anbietet, sollten Sie ihn annehmen, aber nicht trinken.

- Versuchen Sie nicht, mit den Terroristen zu verhandeln oder Ratschläge zu geben. Bleiben Sie während der Entführung so ruhig wie möglich und sparen Sie Ihre Kräfte.

- Rechnen Sie damit, dass die Entführer Sie mit vorgehaltener Waffe verhören und/oder Sie mit anderen Mitteln unter Druck setzen.

- Überlegen Sie sich für den Fall eines Verhörs eine plausible und einfache Darstellung Ihrer Tätigkeit sowie einen konkreten Grund für Ihre Anwesenheit im Flugzeug.

- Behalten Sie auch bei unangenehm hohen Temperaturen im Flugzeug so viele Kleidungsstücke wie möglich an.

- Wenn sich die Entführung über einen längeren Zeitraum erstreckt und Sie müde werden, versuchen Sie immer nur kurz einzuschlafen.

- Nutzen Sie Ihre Zeit dazu, die Situation einzuschätzen, und überlegen Sie, was Sie tun können, wenn es zu einem Schusswechsel oder Handgemenge kommt oder sich eine Fluchtmöglichkeit eröffnet.

- Versuchen Sie bei einem Schusswechsel, sich möglichst flach auf den Boden zu legen.

- Sagen Sie Hotel- oder Restaurantangestellten bzw. fremden Hotelgästen nicht, in welcher Eigenschaft, für welche Firma und zu welchem Zweck Sie unterwegs sind.

- Weisen Sie bei der Anmeldung im Hotel nur die benötigte Kreditkarte vor und zeigen Sie nicht, was sich sonst noch in Ihrer Geldbörse, Aktentasche oder Handtasche befindet. Benutzen Sie keine Firmenkreditkarten.

- Prägen Sie sich die Ein- und Ausgänge, Aufzüge, Treppenhäuser und Notausgänge des Hotels ein.

- Lassen Sie keine Dokumente in Ihrem Hotelzimmer liegen, aus denen Ihr Beruf oder der Zweck Ihrer Reise hervorgehen könnte. Bewahren Sie geschäftliche und persönliche Informationen am Körper oder im Hotelsafe auf.

- Achtung: In Ländern mit hoher Wahrscheinlichkeit für Spionage arbeitet das Hotelpersonal mit den staatlichen Behörden zusammen. Hier kann auch der Zugriff auf Dokumente im Hotelsafe erfolgen. Vertrauliche Unterlagen sollten daher besser am Körper mitgeführt werden.

- Teilen Sie Hotelangestellten oder Fremden in der Hotelbar, Lobby oder Lounge keine persönlichen Informationen mit.

- Treffen Sie sich mit anderen Personen nur in der Lobby und nicht auf Ihrem Zimmer. Die Zimmernummer sollten Sie Fremden niemals zugänglich machen.

- Achten Sie auf Personen, die sich auffallend für Ihre Tätigkeiten interessieren.

- Tauschen Sie keine wichtigen Informationen über das Hoteltelefon aus.

- Antworten Sie nur dann auf die elektronische Nachricht eines Hotels, wenn Sie prüfen können, ob sie tatsächlich daher stammt.

- Achten Sie darauf, was Sie am Hoteltelefon besprechen. In vielen Ländern besteht eine erhöhte Gefahr, im Hotel abgehört zu werden.

In der Öffentlichkeit

- Informieren Sie sich über Gegenden mit hoher Kriminalitätsrate, und meiden Sie solche Gebiete.
- Halten Sie Akten- und Handtaschen immer fest umschlossen. Stecken Sie Ihre Geldbörse in die vordere Hosen- oder innere Jackentasche.
- Geben Sie sich in Verhalten, Sprechweise, Sprache und Kleidung unauffällig.
- Vermeiden Sie es allein und insbesondere nachts durch verlassene Straßen zu gehen.
- Beobachten Sie Ihre Umgebung immer aufmerksam.
- Kaufen Sie in seriösen und bekannten Geschäften ein und meiden Sie Straßenhändler.
- Holen Sie beim Bezahlen nur die jeweils benötigte Kreditkarte oder Geldsumme hervor und zeigen Sie nicht, dass Sie gut situiert sind.
- Meiden Sie öffentliche Veranstaltungen und große Menschenmengen.
- Werden Sie von Personen in einem Fahrzeug angemacht, wenden Sie sich ab, schlagen Sie die der Fahrtrichtung des Fahrzeugs entgegengesetzte Richtung ein und begeben Sie sich an einen sicheren Ort.
- Sollten Sie verfolgt werden, bleiben Sie auf beleuchteten Straßen und steuern Sie einen sicheren Ort an.
- Wenn Sie aufgehalten werden, leisten Sie keinen Widerstand, es sei denn, Sie finden es gefährlicher zu kooperieren. Wenn Sie beschließen, sich zu wehren, sollten Sie schreien und den Angreifer treten und kratzen. Laufen Sie dorthin, wo Sie Licht und Menschen sehen.

- Tragen Sie keine wertvollen Gegenstände offen am Körper (Kameras, IT-Geräte, Schmuck). Vermeiden Sie offensichtliche Laptoptaschen.

- Verwahren Sie Wertsachen in schwer zugänglichen Taschen am Körper. Tragen Sie eine Brieftaschen oder Geldbörse niemals in der Gesäßtasche.

- Taschen und Rucksäcke sollen immer geschlossen sein und möglichst vorne am Körper getragen werden.

- Werden Sie misstrauisch, wenn Sie bedrängt und abgelenkt werden. Versuchen Sie den Ort rasch zu verlassen.

- Falls Sie Opfer eines Taschendiebstahls geworden sind, stellen Sie dem Dieb nicht nach. Er ist selten alleine und möglicherweise bewaffnet.

- Zeigen Sie keine großen Bargeldbeträge und heben Geld möglichst nur von Bankautomaten innerhalb einer Bank ab.

- Variieren Sie Ihre Abfahrtszeiten. Achten Sie beim Losfahren darauf, ob Sie beobachtet werden.

- Nehmen Sie nicht immer den gleichen Weg. Prägen Sie sich Polizeidienststellen, Krankenhäuser, Militärposten oder sonstige sichere Orte ein, die Sie im Notfall ansteuern können.

- Verhalten Sie sich so unauffällig wie möglich. Benutzen Sie Fahrzeuge, die keine unerwünschte Aufmerksamkeit erregen.

- Benutzen Sie nicht immer dasselbe Fahrzeug. Das ist vor allem in Gegenden wichtig, in denen ein hohes Entführungsrisiko besteht.

- Motorhaube, Kofferraum und Tankdeckel sollten verschlossen sein.

- Lassen Sie die Fenster immer geschlossen und die Türen verriegelt.

- Öffnen Sie die Fenster nicht mehr als 5 cm, wenn Sie lüften oder mit Personen außerhalb des Fahrzeugs sprechen.

- Meiden Sie, wenn möglich, abgelegene Straßen.

- Nehmen Sie keine Anhalter oder fremden Personen mit.

- Bleiben Sie nicht stehen, um Fußgängern oder Autofahrern Auskünfte zu erteilen.

- Fahren Sie nicht zu nahe am Straßenrand, sondern so weit wie möglich an der Mittellinie, damit das Fahrzeug nicht abgedrängt werden kann.

- Wenn Sie an einer Ampel anhalten müssen, halten Sie Abstand zu dem Fahrzeug vor Ihnen, damit Sie im Notfall noch ausscheren können.

- Parken Sie stets an einer gut beleuchteten Stelle. Wenn Sie zu Ihrem Fahrzeug zurückkehren, vergewissern Sie sich, dass Ihnen niemand am oder im Auto auflauert.

- Wenn Sie einen Fahrer engagieren, achten Sie darauf, dass dieser in Sicherheitsfahren geschult ist. Machen Sie mit Ihrem Fahrer ein Signal aus, das Sie im Not- oder Gefahrenfall benutzen können.

- Teilen Sie Ihrem Fahrer die Reiseroute nicht im Voraus mit, wenn es keinen zwingenden Grund dafür gibt.

- Werden Sie unter Androhung von Gewalt dazu gezwungen, Ihren Wagen herzugeben, leisten Sie keinen Widerstand. Verlassen Sie das Fahrzeug und rufen Sie die Polizei.

- Wenn Sie einen Unfall oder ein Verbrechen beobachten, entscheiden Sie nach eigenem Ermessen, ob Sie den Vorfall nur melden oder helfen können, ohne sich selbst zu gefährden.

- Hierunter wird das blitzartige Einschlagen von Autoscheiben mit anschließendem Entwenden von Wertgegenständen vom Beifahrersitz verstanden. Die Täter nutzen den Überraschungseffekt.

- Besonders in Afrika und Südamerika kommt diese Form der Kriminalität vor. Verriegeln Sie daher beim Autofahren ständig die Türen.

- Oft handelt es sich um Jugendliche, die mit einem Motorrad an das Opferfahrzeug heranfahren oder als Fensterwäscher oder Verkäufer am Straßenrand ihre Dienste anbietet. Sie geben anderen Bandenmitgliedern ein Zeichen, dass in dem Fahrzeug etwas zu holen ist.

- Gefahr besteht auch an roten Ampeln, in schlecht beleuchteten Straßen, in stark befahrenen Straßen mit Stop and go-Verkehr oder auf Parkplätzen und an Tankstellen.

- Legen Sie Wertsachen oder Taschen niemals sichtbar im Auto ab. Lassen Sie keine Wertsachen und Taschen im Auto zurück. Verstauen Sie Gepäck stets im Kofferraum.

- Lassen Sie die Kofferraumabdeckung bei einem Kombi demonstrativ offen. Damit bringen Sie zum Ausdruck, dass hier nichts zu holen ist.

- Wenn Sie einen Smash-and-Grab-Überfall beobachten, bewahren Sie Ruhe. Steigen Sie nicht aus dem Auto aus. Setzen Sie ggf. einen Notruf ab.

Tipps für Geschäftsreisende

- Reisen Sie so anonym wie möglich.
- Tragen Sie keine Kleidungsstücke oder Accessoires mit dem Namen oder dem Logo des Unternehmens.
- Tragen Sie keine geschäftlichen Dokumente mit sensiblen oder vertraulichen Informationen oder Finanzaufstellungen bei sich.
- Geben Sie bei Reservierungen und Ticketkäufen immer Ihren eigenen Namen an und nicht den des Unternehmens.
- Verwenden Sie Ihre persönliche Kreditkarte; zahlen Sie nicht mit Firmenkarten, aus denen der Name des Unternehmens hervorgeht.
- Melden Sie sich im Hotel nur mit Ihrem Namen an.
- Erwähnen Sie den Namen des Unternehmens nach Möglichkeit nicht gegenüber Einwanderungs- oder Zollbehörden.
- Reisen Sie in legerer Kleidung und tragen Sie nichts zur Schau, was auf Wohlstand hindeutet wie teure Schmuck- oder Gepäckstücke.
- Geben Sie auf Einwanderungsformularen als Reisezweck die Teilnahme an einer örtlichen Konferenz an.
- Teilen Sie nur Ihrer Familie und ein oder zwei Kollegen die Einzelheiten Ihres Reiseplans mit.
- Tragen Sie Ihr Gepäck selbst und fahren Sie nur mit vertrauenswürdigen Taxiunternehmen.
- Versuchen Sie ein Hotelzimmer zwischen dem dritten und dem siebten Stock zu bekommen.
- Machen Sie Gebrauch von allen vorhandenen Schlössern an Türen und Fenstern Ihres Hotelzimmers.
- Bewahren Sie Wertgegenstände im Hotelsafe auf.
- Tragen Sie nie mehr Bargeld oder Kreditkarten bei sich, als Sie gerade benötigen.
- Verlassen Sie das Hotel nicht jeden Tag zur gleichen Zeit und schlagen Sie nicht immer den gleichen Weg ein.
- Reagieren Sie nicht auf Lautsprecherdurchsagen in der Hotellobby oder im Hotelrestaurant, sofern Sie nicht einen Anruf erwarten.

- Auf den Kredit-, Vielflieger- oder Mietwagenkarten von Topmanagern sollte weder ein Firmenname noch ein Logo erscheinen.

- Das Reisebüro, das die Geschäftsreisen für Führungskräfte organisiert, muss sich mit den einschlägigen Sicherheitsmaßnahmen auskennen. Bei Hotelbuchungen ist niemals der Rang oder die Bedeutung des Reisenden zu erwähnen.

- Flugtickets, Tickethüllen und Reisepläne sollten nur auf den Anfangsbuchstaben des Vornamens sowie den Nachnamen des Reisenden lauten. Anreden wie Herr oder Frau sollten nicht verwendet werden. Auch militärische Dienstgrade, Berufsbezeichnungen oder akademische Titel wie Dr. oder Prof. sollten nicht erscheinen.

- Die Reisepässe von Topmanagern sollten regelmäßig kontrolliert werden. Enthält der Pass Ein- und Ausreisestempel oder Sichtvermerke politisch umstrittener Länder wie Israel oder verschiedener arabischer Staaten, sollte ein neuer Pass beantragt werden. In einigen Ländern müssen Ausländer bei der Anmeldung im Hotel ihren Pass aushändigen.

- Reist ein Topmanager in ein Land mit erhöhtem Sicherheitsrisiko, sollte möglichst ein einheimischer Verantwortlicher des Unternehmens die Hotels buchen, gegebenenfalls sogar unter seinem Namen.

- Der Verantwortliche vor Ort sollte das Hotel des Topmanagers nicht auffordern, die Hotelrechnung an die lokale Niederlassung des Unternehmens zu schicken. Stattdessen sollte er mit seiner eigenen Kreditkarte oder bar bezahlen, wenn der Gast abreist.

- Topmanager sollten weder in einem Firmenwagen noch in einem Privatwagen gefahren werden. Reguläre Firmenfahrzeuge können in der Regel leicht mit der Geschäftsleitung oder dem Unternehmen in Verbindung gebracht werden. Stattdessen sollte kurz vor Ankunft des Betreffenden eigens ein Fahrzeug angemietet werden.

- Topmanager sollten nicht zusammen mit anderen Führungskräften oder Regierungsbeamten befördert werden.

- Gegebenenfalls ist es nötig, frühzeitig einen Sicherheitsplan aufzustellen und mit Verantwortlichen aus Militärkreisen oder hochrangigen Behördenvertretern zusammenzuarbeiten.

- Je nach Risiko und Reiseziel muss für professionellen bewaffneten oder unbewaffneten Begleitschutz gesorgt werden. Wenden Sie sich nur an Unternehmen, deren Vertrauenswürdigkeit Sie vorher geprüft haben.

- Bewahren Sie Ruhe! Seien Sie stets aufmerksam und beobachten Sie Ihr Umfeld.

- Menschenrettung geht über die Erhaltung von Sachwerten.

- Die Rettung anderer sollte nie ohne entsprechende Eigensicherung erfolgen.

- Wenn möglich, setzen Sie einen Notruf ab. Beachten Sie dabei die 5W-Regel (Wo ist es geschehen? Was ist passiert? Wie viele Personen sind verletzt? Welcher Art sind die Verletzungen? Warten auf Rückfragen!).

- Provozieren Sie bei einem Überfall oder einer Entführung niemals die Täter, leisten Sie keinen Widerstand und unternehmen Sie keinen Fluchtversuch.

- Kontaktieren Sie bei jedem Sicherheitsvorfall im Ausland umgehend Ihre Familie, Ihren Arbeitgeber, Gastgeber und/oder die deutsche Vertretung vor Ort. Sprechen Sie erst mit einem erfahrenen Sicherheitsverantwortlichen, bevor Sie die Polizei oder sonstige Behörden vor Ort einschalten.

- Wenn Sie erkrankt sind oder sich verletzt haben, rufen Sie Ihre private Reisekrankenversicherung oder Ihren Sicherheitspartner an. Dort erhalten Sie Hinweise, wie Sie sich in Ihrer konkreten Situation verhalten sollten und an wen Sie sich wenden können, um Hilfe zu erlangen.

Express-Kidnapping

- Express-Kidnapping erfolgt spontan mit dem Ziel, das Opfer auszurauben oder die Herausgabe von Kreditkarte und PIN zu erzwingen.

- Ziel sind meistens Personen, die wohlhabend aussehen. Der Zugriff erfolgt oft in der Nähe von Restaurants, Bars, Hotels, Nobelgeschäften oder Banken (vor allem an den Geldautomaten), an schlecht beleuchteten Straßen oder bei der Benutzung nicht lizensierter Taxis.

- Express-Kidnapping breitet sich zunehmend in Großstädten Lateinamerikas und Südafrikas aus.

- Am häufigsten erfolgt der Zugriff kurz vor Mitternacht, um an Geldautomaten zweimal den Höchstbetrag vom Konto abheben zu können (vor und nach Mitternacht).

- Halten Sie sich außerhalb sicherer Räume, insbesondere in den Abend- und Nachtstunden, möglichst nicht alleine auf und gehen Sie nicht zu Fuß.

- Führen Sie nur Karten mit, deren PIN Sie kennen. Die Täter werden Ihnen nicht glauben, dass Sie eine PIN nicht kennen.

- Steigen Sie nicht unmittelbar nachdem Sie Geld abgehoben haben in ein Taxi, das „zufällig" vor der Bank steht. Benutzen Sie nur lizensierte Taxis.

- Wenn Sie Opfer geworden sind, verhalten Sie sich kooperativ. Ihr Leben und Ihre Gesundheit sind nicht mit dem möglichen Geldverlust aufzuwiegen.

Hochwasser/Tsunami

- Wenn Sie in ein Risikogebiet reisen, sollten Sie unbedingt die Wettervorhersagen in den Medien verfolgen.
- Einer Tsunamiwelle geht oft ein sehr rascher Abfall des Wasserspiegels voraus. Bringen Sie sich sofort in höher gelegene Gebiete im Hinterland in Sicherheit. Sind natürliche Zufluchtsorte nicht schnell erreichbar, suchen Sie höhere Etagen in modernen, stabilen Gebäuden auf.
- Benutzen Sie nicht das Auto, wenn das Risiko besteht, in einen Stau zu geraten.
- Ein Tsunami besteht aus einer Serie großer Wellen in Abständen von 10 bis 60 Minuten. Die erste Welle ist oft nicht die höchste. Verlassen Sie den Zufluchtstort nicht zu früh.
- Schalten Sie Handy, Radio oder Fernsehen auf Empfang für präzise Meldungen und Hinweise des Katastrophenmanagements.

Erdbeben

- Bitte Ruhe bewahren, keine Panik.
- Rennen Sie bei Beginn eines Bebens rasch ins Freie, wenn Sie direkt und schnell dorthin kommen können. Sonst bleiben Sie im Haus, solange die Erschütterungen anhalten
- Schwere stabile Gegenstände (Küchentisch, Schreibtisch) bieten Schutz. Wenn nicht vorhanden, bieten stabile Türrahmen oder die Nähe von tragenden Innenwänden Schutz.
- Schützen Sie Ihren Kopf und das Gesicht mit den Armen.
- Halten Sie Im Freien großen Abstand zu Gebäuden. Stellen Sie sich nicht unter Straßenlampen, Versorgungsleitungen, Bäume sowie auf oder unter Brücken.
- An der flachen Küste rennen Sie möglichst landeinwärts auf höheres Niveau (Tsunamigefahr).
- Schalten Sie Handy, Radio oder Fernsehen auf Empfang für präzise Meldungen und Hinweise des Katastrophenmanagements.
- Nach dem Beben muss mit Nachbeben gerechnet werden. Betreten Sie keine beschädigten Gebäude.

- Achten Sie in Hotels und Unterkünften auf Rauchmeldeanlagen und machen Sie sich immer zuerst mit den Fluchtwegen vertraut.

- Nehmen Sie Feueralarme stets ernst und bewahren Sie Ruhe.

- Schließen Sie Ihr Zimmer ab und nehmen den Schlüssel mit. Nehmen Sie beim Verlassen ein nasses Handtuch mit, um bei Rauchentwicklung damit Mund und Nase zu bedecken.

- Verlassen Sie das Gebäude über die Fluchttreppen. Benutzen Sie keine Aufzüge.

- Versuchen Sie sich unterhalb des Rauches zu bewegen.

- Wenn Sie das Gebäude nicht verlassen können, füllen Sie Badewanne, Dusche oder Waschbecken mit Wasser und dichten die Tür mit nassen Handtüchern, Bettlaken oder anderen Stoffen ab. Versuchen Sie, sich den Rettungskräften bemerkbar zu machen.

Diese Informationen wurden von den Experten für internationale Sicherheit und Krisenmanagement der **CORPORATE TRUST** Business Risk & Crisis Management GmbH erstellt.

CORPORATE TRUST ist eine Unternehmensberatung für Sicherheitsdienstleistungen. Als strategischer Partner im Risiko- und Krisenmanagement unterstützen wir Unternehmen, Organisationen und Privatpersonen im High-Level-Security-Bereich.

Sicherheitskonzepte sollten so effektiv und diskret sein, dass Sie ihre Existenz am besten gar nicht wahrnehmen. Genau das ist unsere Mission: Wir wollen eine Umgebung schaffen, in der Sie sich absolut sicher und ungestört auf Ihre Ziele und die Ziele Ihres Unternehmens konzentrieren können. Im Mittelpunkt steht dabei immer der Mensch.

Persönliche Integrität und Professionalität ergeben den entscheidenden Mehrwert für Ihre Sicherheit. Absolute Diskretion ist das fundamentale Kriterium für ein vertrauensvolles Verhältnis zu unseren Kunden. Und selbstverständlich profitieren Sie von unserer langjährigen Erfahrung, unserer Expertise und unserer maximalen Einsatzbereitschaft.

CORPORATE TRUST
Business Risk & Crisis Management GmbH

Graf-zu-Castell-Straße 1
D-81829 München

Tel.: +49 89 599 88 75 80
Fax: +49 89 599 88 75 820

info@corporate-trust.de
www.corporate-trust.de

Regelmäßig aktuelle Informationen
von Sicherheitsexperten

Follow us: twitter
www.twitter.com/corporatetrust