Tipps und Ratschläge

Nutzen Sie diese Tipps und Ratschläge und machen Sie sich den sicheren Umgang mit dem Internet zur Gewohnheit. Dieser Abschnitt wurde in Abstimmung mit der Initiative „Get Safe Online“ (Sicher online gehen) aus dem Vereinigten Königreich und dem Department of Homeland Security, der Heimatschutzbehörde der USA, entwickelt.

- Schützen Sie Ihren PC und Ihre mobilen Endgeräte
- Schützen Sie Ihre personenbezogenen Daten und Ihre Identität
- Schützen Sie geschäftliche Informationen außerhalb Ihrer Organisation
- Vorsicht, wenn Sie online gehen
- Achten Sie auf einen vernünftigen und sachkundigen Umgang mit dem Internet

Schützen Sie Ihren PC und Ihre mobilen Endgeräte

PC

- Nutzen Sie eine Firewall: Firewalls schützen Ihr Netzwerk vor Viren und Hackern
- Installieren Sie Antivirensoftware: Durch Antivirensoftware ist Ihr Computer vor Infektionen mit Viren geschützt
- Laden Sie immer die neuesten Sicherheitsupdates herunter: Sorgen Sie dafür, dass Ihre Anwendungen und Ihr Betriebssystem den Anforderungen angepasst, frei von Schadsoftware und auf dem neuesten Stand sind
- Stoppen Sie Spyware: Öffnen Sie keine verdächtigen E-Mails oder Anhänge, damit niemand von außen in Ihren Computer eindringen kann
- Führen Sie regelmäßig eine Datensicherung durch: So schützen Sie sich vor Datenverlust

Laptops

- Unterbrechen Sie drahtlose Verbindungen, wenn Sie diese nicht nutzen oder benötigen
- Schließen Sie Ihren Laptop regelmäßig an ein vertrauenswürdiges Netzwerk an, um Ihre Sicherheitsmechanismen zu aktualisieren
- Erstellen Sie eine Sicherungskopie der auf Ihrem Laptop abgelegten Daten
- Lassen Sie Ihren Laptop nicht unbeaufsichtigt

USB-Speichersticks

- Verwenden Sie einen verschlüsselten USB-Speicherstick
- Nutzen Sie den USB-Speicherstick im Read-only-Modus, um die Übertragung von Viren zu vermeiden: Manche USB-Sticks haben einen Schalter bzw. eine Verriegelung, um das Gerät

im Read-only-Modus zu betreiben, der das Beschreiben des Laufwerks bzw. die Änderung darauf gespeicherter Daten durch den Host-Rechner verhindert
- Unterziehen Sie den USB-Speicherstick einem Anti-Virus-Scan, wenn Sie Dateien von einem nicht vertrauenswürdigen und/oder nicht genehmigten Rechner kopiert haben
- Bevor Sie Ihren USB-Speicherstick an den PC einer anderen Person anstecken, löschen Sie alle Dateien, die Sie für den betreffenden Vorgang nicht benötigen
- Erstellen Sie Sicherheitskopien, um auf USB-Speichersticks abgelegte Daten bei Bedarf wiederherstellen zu können
- Befestigen Ihre USB-Speichersticks an Schlüsselringen oder Tragebändern, damit Sie sie nicht verlieren; aufgrund ihrer geringen Größe gehen sie sehr leicht verloren oder können gestohlen werden. Außerdem erhöhen größere Speicherkapazitäten die potenziell dem Risiko eines unberechtigten Zugriffs ausgesetzte Datenmenge. USB-Speichersticks werden gewöhnlich in Handtaschen, Rucksäcken, Laptop-Taschen, Jackett- und Hosentaschen aufbewahrt oder unbeaufsichtigt am Arbeitsplatz zurückgelassen. In jüngerer Zeit kommt es immer häufiger zu Vorfällen, bei denen USB-Speichersticks verloren gehen, verlegt, ohne Erlaubnis ausgeliehen oder gar gestohlen werden

Mobiltelefone und Handheld-Computer

Handheld-Computer wie Windows Mobile-, Palm-, iPhone-, Android- und Blackberry-Geräte ermöglichen die Verbindung zum Internet und können große Datenmengen speichern. Gerade weil es sich um mobile Geräte handelt, verlangt ihre Handhabung besondere Sorgfalt

- Unterbrechen Sie drahtlose Verbindungen (z. B. Bluetooth und WLAN), wenn Sie die Geräte nicht benutzen. Mithilfe der Bluetooth-Technologie können elektronische Geräte per Funkvernetzung über kurze Distanz miteinander kommunizieren
- Lassen Sie Ihr Mobiltelefon und Ihren Handheld-Computer nicht unbeaufsichtigt. Dies könnte einen Datenverlust zur Folge haben
- Nutzen Sie die Passwort-Funktion, um unbefugte Zugriffe von außen auf Ihr Smartphone zu verhindern

Schützen Sie Ihre personenbezogenen Daten und Ihre Identität

- **Verwenden Sie ein starkes Passwort:** Mit Ihrem Passwort schützen Sie Ihre Daten im Internet vor unberechtigtem Zugriff, so wie Sie Ihr Haus abschließen, um Eindringlinge fernzuhalten. Passwörter sind ein wichtiger Schutzmechanismus, weshalb Ihnen einige bewährte Regeln für den Umgang mit Passwörtern dabei helfen können, Ihre sensiblen persönlichen Daten und Ihre Identität besser zu schützen. Das Passwort zu Ihrem Desktop gewährt Zugriff auf alle persönlichen und Unternehmensdaten, die Sie auf Ihrem Computer gespeichert haben, und auf alle Online-Konten. Wählen Sie ein starkes Passwort, um Ihre Daten zu schützen: Verwenden Sie eine komplexe Zeichenreihe; kombinieren Sie Buchstaben (Klein- und Großschreibung), Ziffern und Symbole. Je größer die Zeichenvielfalt

in Ihrem Passwort, desto schwieriger ist es zu erraten. Verwenden Sie keine personenbezogenen Informationen, wie Ihren eigenen Namen, den Namen Ihres Kindes oder Geburtstage, die jemand bereits kennt oder leicht in Erfahrung bringen kann. Versuchen Sie außerdem, gemeinsprachliche Wörter zu vermeiden, weil einige Hacker Programme einsetzen, die jedes Wort ausprobieren, das im Wörterbuch steht

- **Ändern Sie Ihr Passwort regelmäßig:** Wenn Sie den Eindruck haben, dass ein unrechtmäßiger Zugriff auf Ihr System stattgefunden hat, dann ändern Sie Ihre Passwörter sofort
- **Halten Sie Ihr Passwort geheim:** Ihr Passwort ist nur Ihnen bekannt und darf niemandem mitgeteilt werden. Versuchen Sie nach Möglichkeit, sich Ihre Passwörter einzuprägen. Überlegen Sie sich eine Strategie, mithilfe derer Sie sich die Passwörter merken können. Wenn Sie Ihre Passwörter notieren, bewahren Sie sie sicher auf. Bewahren Sie die Aufzeichnungen über Ihre Passwörter nur dort auf, wo Sie auch die Daten ablegen würden, die durch die Passwörter geschützt werden
- **Ein eigenes Passwort für jedes Online-Konto:** Verwenden Sie für jedes Online-Konto, auf das sie zugreifen, ein eigenes Passwort (oder verwenden Sie zumindest mehrere verschiedene Passwörter). Wenn Sie für mehrere Konten dasselbe Passwort nutzen, hat ein Angreifer, der sich Zugriff auf eines Ihrer Konten verschafft, Zugang zu allen Ihren Konten
- **Erhöhen Sie die Sicherheit Ihrer Online-Konten:** Viele Anbieter stellen zusätzliche Verfahren zur Prüfung Ihrer Identität bereit, bevor Sie über die betreffende Website Geschäfte abschließen
- **Legen Sie das Sicherheitsniveau von Websites selbst fest:** Sofern möglich, passen Sie die Datenschutz- und Sicherheitseinstellungen auf Websites so an, dass ein Datenaustausch nur in dem Ihnen genehmen Maß erfolgen kann. Es ist besser, genau festzulegen und zu beschränken, mit wem Sie Daten austauschen
- **Seien Sie vorsichtig, wenn Sie soziale Netzwerke im Internet nutzen:** Machen Sie sich bewusst, dass in sozialen Netzwerken im Internet viele Risiken von Online-Angeboten in geballter Form auftreten können; Online-Mobbing, die Preisgabe personenbezogener Daten, Cyber-Stalking (Missbrauch des Internets für Belästigung), Zugang zu für bestimmte Altersgruppen ungeeigneten Inhalten und im Extremfall die Vorbereitung des sexuellen Missbrauchs von Kindern (Online-Grooming)

Schützen Sie geschäftliche Informationen außerhalb Ihrer Organisation

- **Sorgen Sie für die Sicherheit sensibler Daten:** Stellen Sie sicher, dass Sie sensible Daten und Geräte jederzeit sicher aufbewahren, wenn Sie sich außerhalb Ihrer Organisation befinden, um deren Diebstahl oder Verlust zu verhindern. Seien Sie vor allem in der Öffentlichkeit vorsichtig im Umgang mit Daten
- **Wahren Sie die Vertraulichkeit geschäftlicher Informationen:** Beachten Sie, dass andere mithören können, was Sie sagen. Machen Sie vertrauliche Informationen Ihrer Organisation nicht für jeden zugänglich

- **Schützen Sie sich vor Shoulder-Surfing:** Wenn Sie unterwegs oder von einem dezentralen Arbeitsplatz aus arbeiten, achten Sie darauf, dass Ihnen niemand über die Schulter schauen kann (Shoulder-Surfing)
- **Nutzen Sie Webmail-Dienste mit Umsicht:** Wenn Sie einen Internet-Browser nutzen, um Ihre E-Mails zu lesen, sollten Sie genauso große Vorsicht walten lassen wie bei einem Desktop-Mailsystem; Webmail-Dienste bergen einige spezielle Sicherheitsrisiken

Vorsicht, wenn Sie online gehen

- **Unterbrechen Sie drahtlose Verbindungen, wenn Sie diese nicht nutzen oder benötigen**
- **Ergreifen Sie Vorsichtsmaßnahmen, wenn Sie WLAN-Hotspots nutzen:** Beschränken Sie die Vorgänge, die Sie über WLAN-Hotspots abwickeln, und passen Sie die Sicherheitseinstellungen an Ihrem Gerät an, damit nicht jeder darauf zugreifen kann
- **Schützen Sie Ihr Geld:** Achten Sie beim Online-Banking und Online-Shopping darauf, dass die betreffenden Seiten über Sicherheitsfunktionen verfügen. Achten Sie auf Web-Adressen mit https:// oder shttp://, die besagen, dass die Website zusätzliche Maßnahmen ergreift, um Ihre Daten zu schützen. Http:// ist nicht sicher
- **Stoppen Sie unerwünschte E-Mails:** Spam-E-Mails sind ein Sicherheitsrisiko. Öffnen Sie keine unbekannten E-Mails und Anhänge
- **Im Zweifelsfall löschen:** Wenn Links in E-Mails, Tweets, Posts und Online-Werbung verdächtig scheinen, so löschen Sie sie am besten oder kennzeichnen Sie gegebenenfalls als Junkmail – und zwar auch dann, wenn Ihnen die Quelle bekannt ist
- **Leiten Sie E-Mails bei Bedarf weiter.** Erwägen Sie jedoch, zuvor die Nachrichtenhistorie zu löschen
- **Seien Sie vorsichtig, wenn Sie im Internet surfen**
- **Laden Sie keine Dokumente und Materialien herunter, die von nicht vertrauenswürdigen Quellen angeboten werden**
- **Seien Sie vorsichtig, wenn Sie öffentliche Computer nutzen:** Gehen Sie mit einem öffentlichen Computer nur online, wenn Sie eine verschlüsselte Verbindung nutzen können (erkennbar an einem Schloss-Symbol in der rechten unteren Ecke Ihres Browserfensters und an den Buchstaben ‚https://' am Anfang der Webadresse.)
- **Nutzen Sie nur Webmail-Dienste von bekannten und vertrauenswürdigen Unternehmen**

Achten Sie auf einen vernünftigen und sachkundigen Umgang mit dem Internet

- **Halten Sie sich auf dem Laufenden:** Informieren Sie sich kontinuierlich, wie man sicher online geht: Suchen Sie auf vertrauenswürdigen Websites nach den aktuellsten Informationen, geben Sie diese an Ihre Familie, Freunde und Kollegen weiter und halten Sie sie zu einem vernünftigen und sachkundigen Umgang mit dem Internet an. Sorgen Sie dafür, dass Ihr Browser sicher ist

- **Denken Sie nach, bevor Sie handeln:** Seien Sie vorsichtig, wenn Sie im Internet zu sofortigem Handeln gedrängt werden, auf allzu verlockende Angebote stoßen und nach personenbezogenen Daten gefragt werden
- **Sichern Sie Ihre Daten:** Schützen Sie Ihre Arbeit, Musik, Fotos und andere digitale Daten, indem Sie eine elektronische Kopie erstellen und diese an einem sicheren Ort verwahren