Anleitung

Sicher am Computer arbeiten – auch unterwegs und im Home Office

Sicherheitsempfehlungen für das mobile Arbeiten

Ziel dieser Anleitung

Diese Empfehlungen dienen dazu, zu verhindern, dass

- Daten verlorengehen
- Unbefugte Zugriff auf dienstliche Daten erhalten
- Schadsoftware ins Netz der PH Ludwigsburg gelangt

Generell

Datenträger müssen sicher entsorgt werden. Dies betrifft vornehmlich Dokumente in Papierform, die Geschäftsgeheimnisse oder personenbezogene Angaben enthalten. Diese dürfen nicht im Papierkorb landen, sondern müssen im Aktenvernichter geschreddert werden. Aber auch nicht mehr benötigte Mobiltelephone, CDs oder nur scheinbar defekte USB-Sticks dürfen nicht einfach in den Müll geworfen oder per Elektronikschrott entsorgt werden. Diese sind entweder selbst gründlich zu zerstören oder im Sekretariat des MIT (Raum 4.319) abzugeben, wo sie mittels eines professionellen Schredders entsorgt werden.

Erhalten Sie von Lieferanten, Herstellern, Kunden, Geschäftspartnern, Kollegen anderer Hochschulen etc. CDs oder USB-Sticks als Geschenk oder zur Kenntnisnahme der darauf enthaltenen Informationen, bedenken Sie bitte, dass sich auf diesen Datenträgern Schadsoftware befinden kann. Bevor Sie eine Datei öffnen, sollte der gesamte Inhalt zunächst mit dem auf jedem Laptop installierten Virenscanner (Trend Micro Office Scan Agent) geprüft werden.

Ausdrucke und Kopien nicht im Drucker/Kopierer liegenlassen!

Benutzen Sie sichere Paßwörter: je länger, desto besser – zwölf Zeichen sind ein guter Schutz. Verwenden Sie nicht das gleiche Paßwort für mehrere Konten.

Auf Ressourcen der Hochschul-IT kann remote nur im abgesicherten Verbindungsmodus über VPN zugegriffen werden.
Beschreibung hier: https://www.ph-ludwigsburg.de/9075.html

Schützen Sie Ihre Technik mit regelmäßigen Updates. Aktualisieren Sie Virenscanner, damit dieser gegen die neusten Virenversionen gewappnet ist, und installierte Anwendungen, denn durch aktuelle Patches werden u.a. Sicherheits-Schwachstellen in den Anwendungen beseitigt. Der Standard-Virenscanner der PH, Trend Micro Office Scan Agent, aktualisiert sich regelmäßig selbst. Dennoch kann es nicht schaden, gelegentlich zu überprüfen, ob die Aktualisierung auch tatsächlich erfolgt ist (Liste aller Anwendungen kann mit der Windowstaste aufgerufen werden).

Auf der lokalen Festplatte des Laptops dürfen dauerhaft keine sensitiven Daten aufbewahrt werden. Diese sollten ausschließlich im Home- und Gruppenverzeichnis der Hochschulserver liegen. Temporäre Speicherung auf der lokalen Festplatte ist nur ausnahmsweise gestattet, etwa wenn die Daten für eine Präsentation benötigt werden oder wenn man unterwegs arbeiten möchte.
Übertragen Sie die erarbeiteten Daten regelmäßig auf das zentrale Firmensystem!

Wenn Informationen, IT-Systeme oder Datenträger verlorengegangen sind oder gestohlen wurden, ist dieser Vorfall umgehend sowohl bei den Vorgesetzten als auch beim MIT (Dr. Winfried Knörzer, Tel.: -449; winfried.knoerzer@ph-ludwigsburg.de) zu melden.

Verschlüsselung: Die Daten auf USB-Sticks und externen Festplatten müssen mit dem Programm Bitlocker verschlüsselt werden. Eine Beschreibung finden Sie unter: https://www.ph-ludwigsburg.de/21313.html. Die interne Laptopfestplatte ist ebenfalls mit Bitlocker verschlüsselt zu betreiben.

Im Home-Office

Ihr häuslicher Arbeitsplatz muß so sicher sein wie Ihr Büro. Niemand (auch nicht Familienangehörige oder Freunde) darf Einblick in Ihre Daten erhalten. Beim Verlassen des Arbeitsplatzes ist die Bildschirmsperre zu aktivieren und bei längerer Abwesenheit bzw. nach Feierabend sind alle Unterlagen in einem sicheren Behältnis (Schrank, Rollcontainer) abzuschließen. Es dürfen keine dienstlichen Dokumente am Arbeitsplatz liegenbleiben.

Der Arbeitsplatz sollte so gut wie möglich vor Einbrüchen geschützt werden, z.B. durch Verschließen von Türen und Fenstern nach Feierabend. Besondere Sorgfalt sollte auf die Einbruchssicherung vor Urlaubsbeginn aufgewandt werden.

Schützen Sie Ihren WLAN-Router vor unerlaubtem Zugriff. Sofern Sie das Paßwort noch nie geändert haben: Stellen Sie sicher, dass es sich hierbei nicht um Standard-Zugangsdaten handelt, die von Angreifern z.B. in der Bedienungsanleitung auf der Herstellerwebseite recherchiert werden können. Aufgrund des besonders hohen Schutzbedarfs eines WLANs sollte das Paßwort mindestens 18 Zeichen lang sein.

Unterwegs

Beim Verlassen von öffentlichen Verkehrsmitteln, Gaststätten, Hotelzimmern usw. immer zuerst die Tasche mit dem Laptop in die Hand nehmen, bzw. die Mappe mit den schriftlichen Unterlagen verstauen.

USB-Sticks sicher aufbewahren, z.B. in der Laptoptasche oder besser noch im Geldbeutel.

Da trotz aller Vorsicht immer etwas verlorengehen kann, dürfen niemals Unikate transportiert werden. Dies gilt natürlich besonders für schriftliche Dokumente wie Urkunden, Zeugnisse o. dgl. Es muß immer eine Kopie vorhanden sein.

Verhindern Sie, wenn Sie unterwegs sind, dass Unbefugte Ihren Bildschirminhalt oder die Kennworteingabe beobachten können.

Für Personen, die häufig unterwegs sind, empfiehlt sich als Diebstahlsicherung die Anschaffung eines Kabelschlosses (z.B. von Kensington)

Bei Besprechungen: Wenn ein Besprechungszimmer für längere Zeit verlassen wird (z.B. wegen des Mittagessens) darf der Laptop nicht ungesichert zurückbleiben. Das Besprechungszimmer muß entweder abgeschlossen, der Laptop mitgenommen oder mittels eines Kabelschlosses in geeigneter Weise fixiert werden

Wenn man im Zug seinen Sitzplatz verläßt, um auf die Toilette oder ins Bordrestaurant zu gehen, wäre es sicherheitsmäßig wünschenswert, den Laptop mitzunehmen. Das ist aber nicht immer praktikabel, weshalb man zumindest sicherstellen sollte, dass in der Zeit der Abwesenheit keine datenanzeigenden Programme aktiv sind und vor allem keine Daten auf der lokalen Festplatte gespeichert sind. Vor Verlassen des Platzes muß mindestens die Bildschirmsperre aktiviert werden, besser noch ist es, das Gerät komplett auszuschalten.
Sinngemäß gilt diese Empfehlung auch für Flugzeuge, Bahnhöfe, Flughäfen, Gaststätten, usw.

Sprechen Sie in der Öffentlichkeit, d.h. wenn Fremde zuhören können, nicht über vertrauliche Hochschulinterna.

Besondere Vorsicht sollte man bei der Arbeit auf Fremd-Computern (Internet-Café, PCs in Büros, wo Sie zu Gast sind) walten lassen, weil es sich kaum vermeiden läßt, daß Reste der eigenen Aktivität (temporäre Dateien, Profileinträge) irgendwo zurückbleiben. Auf keinen Fall sollten Browser-Funktionen zur Auto-Vervollständigung von Benutzernamen und Passwörtern genutzt werden, damit nachfolgende Benutzer sich nicht einfach unter diesem Benutzernamen anmelden können.

Zusammenfassung:

Behandeln Sie Ihre Daten und Datenträger genau so, wie Sie ein Ihnen gehörendes, sehr empfindliches und sehr teures Schmuckstück behandeln würden!