Informationssicherheit im Homeoffice

Home Office wird uns auch weiterhin im Arbeitsalltag begleiten.

Darum finden Sie hier Handlungsanleitungen und Anwendungsempfehlungen, die das Arbeiten von Zuhause so sicher wie nötig und so praktikabel wie möglich machen.

Diese Infos finden Sie hier

Noch Fragen?

Sollten Sie bei der Umsetzung der einzelnen Anleitungen Fragen oder Probleme haben, wenden Sie sich bitte an help@it.tuwien.ac.at oder an den_die IT-Beauftragte_n und/oder IT-Admin Ihres Instituts. Ergänzungswünsche und Anregungen werden unter infosec@tuwien.ac.at oder datenschutz@tuwien.ac.at gerne entgegengenommen und an die entsprechenden Stellen weitergeleitet. Eine laufend aktualisierte Liste an Anwendungen für das Homeoffice finden Sie im coLab der TU Wien unter: https://colab.tuwien.ac.at/display/HOT

Das könnte Sie auch interessieren

IT Security Empfehlungen für Anwender_innen

IT Security Empfehlungen für Administrator_innen

Datenzugang und Anwendungen

VPN

Sicheren Zugang zu Daten, die an der TU Wien gespeichert sind, erhalten Sie über eine **VPN-Verbindung**. Dabei handelt es sich um eine gesicherte Verbindung aus einem beliebigen Netzwerk zu einem Netzwerk einer Organisation der TU Wien.

Details zu Beantragung und Installation finden Sie unter https://colab.tuwien.ac.at/pages/viewpage.action?pageId=9439634

Ist die VPN-Verbindung aktiv, haben Sie Zugang zu den Laufwerken, Daten und Anwendungen an der TU Wien, für die Sie eine Berechtigung haben.

Es ist nicht gestattet, ohne VPN oder SSH Tunnel per Remotedesktop von außerhalb der TU Wien auf Rechner der Institute zuzugreifen.

Befindet sich Ihre Organisationseinheit hinter einer eigenen Firewall, benötigen Sie für VPN eine statische IP-Adresse, um auf die Ressourcen zugreifen zu können. Diese beantragen Sie im Online Account Management unter https://www.it.tuwien.ac.at/rechte-und-rollen/online-account-management/. Ihr lokaler Firewall-Admin wird Ihnen dann für diese IP die Firewall öffnen.

E-Mail

Zugang zu Ihren **E-Mails** erhalten Sie über https://upTUdate.tuwien.ac.at.

Daten speichern und teilen

Wollen Sie Daten mit Kolleg_innen anderer Abteilungen austauschen, tun Sie dies am besten über die **owncloud** der TU Wien (TUownCloud) unter https://owncloud.tuwien.ac.at/.

Ist es erforderlich, Daten mit TU-externen Personen auszutauschen, verwenden Sie die proCloud der TU Wien. Details zu Beantragung und Anwendung finden Sie unter https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/collaboration/tuprocloud-sync-und-share-fuer-projekte/.

Dokumente gemeinsam bearbeiten

Wollen Sie Dokumente gemeinsam mit Kolleg_innen bearbeiten, verwenden Sie die Anwendung **TUdocs** : https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/datenspeicherung/tuowncloud-sync-und-share/tudocs/

Dokumente in der TUowncloud bzw. TUprocloud können mit ONLYOFFICE gemeinsam bearbeitet werden.

Telefonieren und Chatten

Mithilfe der Anwendung **Cisco Jabber** können Sie wie mit dem **Standtelefon** im Büro via PC telefonieren. Die Anleitung zur Einrichtung der Anwendung finden Sie hier: https://colab.tuwien.ac.at/display/HOT/Softphone+Cisco+Jabber

Mit Hilfe von TISS können außerdem Merkmale des TUphone-Profils sowie das TUphone-Passwort geändert werden. Eine Anleitung dazu finden Sie unter https://www.it.tuwien.ac.at/fileadmin/TUit/BILDERPOOL/service/TUphone_Festnetz/Anleitungen/Endanwender.pdf.

Mittels TUchat können Sie sich über eine einfache, intuitiv bedienbare Plattform in Gruppen (Kanälen) oder einzeln miteinander austauschen sowie Dateien, Bilder oder Videos versenden.

Informationen zum Zugriff auf diese Anwendungen finden Sie unter https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/collaboration/tuchat/zugriff/.

Webkonferenzen und Terminfindung

Benötigen Sie ein Abstimmungstool zur Terminfindung, werden die Anwendungen https://terminplaner4.dfn.de/ oder https://www.termino.gv.at/meet/de empfohlen.

Die TU Wien empfiehlt für interne Meetings und Besprechungen MS Teams oder ZOOM.

In manchen Besprechungsräumen können Cisco Jabber Installationen genutzt werden.
Durch die hohe Akzeptanz und leichten Bedienbarkeit ist das Tool der Wahl im Bereich der Lehre ZOOM.

MS Teams: https://colab.tuwien.ac.at/pages/viewpage.action?pageId=9439683
Cisco Jabber: https://colab.tuwien.ac.at/display/CORONA/Cisco+Jabber
ZOOM: https://colab.tuwien.ac.at/display/DLGP/ZOOM

INFOSEC Hinweis - Webkonferenzen

Aktuell wird für die Durchführung von Lehrveranstaltungen primär das Konferenztool ZOOM verwendet, deshalb wurden kommerzielle Lizenzen gekauft. Die freie Version von ZOOM ist in der derzeitigen Ausführung nicht DSGVO konform und darf an der TU Wien nicht verwendet werden. Weitere Informationen zu ZOOM finden sich unter Distance Learning Good Practice - Tools.

Werden Sie zu einer Videokonferenz eingeladen, müssen Sie als Teilnehmer_in keine personen bezogenen Daten bekannt geben und sie können ihre IP-Adresse anonymisieren indem sie sich zuvor über ein VPN verbinden. Weitere Vorkehrungen zur Datensicherheit sind von den Veranstalter_innen zu setzen. Die notwendigsten Sicherheitseinstellungen werden vom Administrator des ZOOM-Mandanten der TU Wien (beim TSC) zwingend eingestellt, erkennbar durch eine ausgegraute Schaltfläche, diese können durch einen Organisator eines Meetings nicht verändert werden. Andere Einstellungen sind datenschutzfreundlich voreingestellt, diese können aber verändert werden.

GoToMeeting kann als Alternative dazu verwendet werden, allerdings ist zu beachten, dass GoToMeeting nicht barrierefrei ist und keine datenschutzfreundlichen Voreinstellungen durch das TSC oder TU.it vorgenommen werden können. Beide Tools sind in der momentanen Version nicht für die Übertragung von sensiblen Daten geeignet, hierfür eignet sich das Tool MS Teams. Nähere Informationen zu MS Teams finden sich unter Microsoft Teams (Skype for Business).

Generell gilt für diese Anwendungen Folgendes:

- Erstellen Sie keine öffentlichen Veranstaltungen ohne Passwortsperre, sondern nutzen Sie die Möglichkeit Ihr Meeting mittels Passwort zu schützen.
- Bei manchen Anwendungen gibt es auch die Möglichkeit einen Warteraum einzurichten und den Zutritt von Teilnehmer_innen zu kontrollieren.
- Teilen Sie den Link zu einem Meeting nicht an öffentlich zugänglichen Orten (beispielsweise in Social Media Accounts), sondern schicken Sie den Link direkt an die eingeladenen Personen.
- Stellen Sie Unterlagen für Meetings oder Lehrmaterial nach Möglichkeit nur über TU-Plattformen wie TUWEL, TISS, ownCloud und coLab zur Verfügung (in TISS und TUWEL wurde die zulässige Dateigröße auf 250 MB hinaufgesetzt). Wenn Sie die Daten auf institutseigenen Webservern zur Verfügung stellen, sind die Zugangsdaten über TISS/TUWEL zu übermitteln.
- Stellen Sie sicher, dass nur Sie als Organisator_in den Bildschirm teilen können.
- Stellen Sie sicher, dass alle Teilnehmer_innen die aktuellste Version der Anwendung nutzen.

Datensicherheit im Homeoffice

Allgemeines

Wie auch am Arbeitsplatz an der TU Wien der Rechner bei Verlassen des Arbeitsplatzes zu versperren ist, ist dieser auch im Homeoffice zu versperren, wenn man Pause macht. Aktivieren Sie dazu auch am besten einen Bildschirmschoner mit Passwort. Wenn Sie an einem privaten Rechner arbeiten müssen, der auch von anderen Familienmitgliedern benutzt wird, ist es ratsam einen passwortgeschützten Firmenaccount anzulegen. Eine Anleitung dazu finden Sie beispielsweise hier: https://support.microsoft.com/de-de/help/4026923/windows-10-create-a-local-user-or-administrator-account oder unter https://www.heise.de/tipps-tricks/Windows-10-Neuen-Benutzer-anlegen-4058638.html.

Arbeiten Sie in Ihrem Bereich mit der TUownCloud oder TUproCloud, sollten Sie nicht automatisch alle Daten auf Ihrem Rechner synchronisieren, sondern nur diejenigen, die Sie für die tägliche Arbeit benötigen.

Werden Daten zur Bearbeitung aus TUfiles am lokalen Rechner abgelegt, sind diese nach Beendigung der Arbeit wieder in TUfiles zu speichern und am lokalen Rechner zu löschen.

Verwenden Sie zur Speicherung von Daten nach Möglichkeit keine externen Datenträger. Sollte es doch notwendig sein, solche zu verwenden, sind diese zu verschlüsseln und sicher zu verwahren, um zu verhindern, dass Daten verloren gehen oder versehentlich gelöscht werden.

Cyberkriminalität und "Social Engineering" (Quelle: https://www.dsb.gv.at/documents/22758/23115/Informationsblatt_der_Datenschutzbehoerde_Datensicherheit_und_Home-Office.pdf/ zuletzt abgerufen am 14.04.2020)

Die aktuelle Ausnahmesituation und die Verunsicherung wird von Kriminellen missbraucht. Insbesondere ist ein Anstieg von Phishing-Attacken zu beobachten, mittels welcher Kriminelle versuchen über gefälschte Webseiten, E-Mails oder Kurznachrichten an Nutzer_innendaten zu gelangen.

Rechnen Sie damit, dass Kriminelle versuchen, sich als vertrauenswürdige Quellen (etwa als Gesundheitsbehörde) auszugeben. Geben Sie unter keinen Umständen Benutzer_innendaten oder Passwörter weiter, wenn Sie dazu aufgefordert werden. Überprüfen Sie vor der Eingabe von Nutzer_innendaten auf einer Webseite die URL („die Webadresse“) und rufen Sie Login-Seiten lieber durch manuelle Eingabe auf, anstatt einem Link aus einem E-Mail zu folgen. Installieren Sie auch nicht eigenmächtig Software auf ihrem (Dienst-) Laptop.

Hinterfragen Sie stets Anweisungen, die Sie zu ungewöhnlichen Handlungen oder der Installation von diversen Programmen auffordern. Bitte berücksichtigen Sie, dass eine Identität gefälscht werden kann. Überprüfen Sie bei ungewöhnlichen E-Mails daher stets die Identität der Absendeadresse und vergleichen diese mit der Absendeadresse von vertrauenswürdigen E-Mails Ihrer Kolleg_innen.

Besondere Vorsicht ist auch geboten, wenn Sie in einer E-Mail zu dringenden Handlungen aufgefordert werden. Kriminelle versuchen oftmals unter Vorspielung besonderer Dringlichkeit zu bestimmten Handlungen zu verleiten („Falls Sie nicht innerhalb der nächsten 2 Tage eine Verifikation durchführen, wird ihr Konto/Zugang gesperrt.“)
Bitte halten Sie im Zweifel Rücksprache mit der Ansprechperson für IT-Angelegenheiten oder mit der TU.it (unter help@it.tuwien.ac.at).

Beispiele:

- Sie erhalten eine E-Mail mit der Aufforderung, eine Home-Office-Software zu installieren.
- Sie erhalten eine E-Mail mit der dringlichen Aufforderung ihren E-Mail-Account für den Home-Office-Einsatz zu verifizieren.
- Sie erhalten eine E-Mail mit der Aufforderung, Ihre Benutzer_innendaten oder Passwörter einzugeben, damit Sie aktuelle Informationen über das Coronavirus (COVID-19) erhalten.
- Es öffnet sich ein Pop-Up. Ein angebliches Sicherheitsteam informiert Sie über die neueste Anzahl von Infektionsfällen und fordert Sie auf, eine „Nachrichtensoftware“ zu installieren.
- Sie erhalten einen Anruf. Die unbekannte Person gibt sich als Mitarbeiterin einer Gesundheitsbehörde aus und fordert Sie auf, Ihre Kreditkartendaten bekannt zu geben, damit Ihnen ein Impfstoff zugeschickt werden kann.

Wie Sie Betrug im Internet erkennen und sich davor schützen, erfahren Sie in diesem Video.

Quelle: https://alexanderlehmann.net/#Impressum

Erste Ansprechpartnerin für IT-Sicherheitsfragestellungen hinsichtlich Firewalls, Netzsicherheit für Server, Anwendungssicherheit bei Arbeitsplätzen und verschiedene Bedrohungsszenarien, wie Spam, Phishing und Schadprogramme (Viren) ist die Abteilung IT-Security der TU.it (https://www.it.tuwien.ac.at/services/beratung-und-servicedesk/beratung/it-security/).

Passwörter

Geben Sie Passwörter auch innerhalb Ihrer Familie nicht weiter und verwenden Sie möglichst komplexe Passwörter.

Wenn Sie passwortgeschützte TUownCloud-Links verschicken, um wichtige Informationen zu teilen, verschicken Sie das Passwort per SMS oder zumindest in einer gesonderten E-Mail. Gleiches gilt für passwortgeschützte Meetings oder andere Anwendungen, deren Zugriff mittels Passwort geschützt ist und mit anderen Personen geteilt wird. Wenn Sie heikle Daten an TU-Mitarbeiter_innen übermitteln wollen, verwenden Sie dafür am besten die TUownCloud. Für den Datenaustausch mit externen Personen können Sie die TUproCloud benutzen.

Stellen Sie sicher, dass Sie für unterschiedliche Anwendungen unterschiedliche Passwörter verwenden. Das Passwort für die Anmeldung zum Firmenaccount oder am TU-Laptop sollte sich vom Passwort für jegliche private Dienste unterscheiden. Gleiches gilt für das Passwort für den upTUdate-E-Mail-Zugang. Dieses soll keinesfalls mit dem Passwort für andere E-Mail-Dienste ident sein.

Speichern Sie Passwörter nicht in zugänglichen Textfiles, z.B. auf dem Desktop oder in gemeinsamen Fileshares, und schreiben Sie diese auch nicht auf Post-its und dergleichen. Passwörter sollten auch nicht in Webbrowsern gespeichert werden, auch wenn dies als sehr komfortabel erscheint. Optimal ist die die Verwendung eines Passwortmanagers. Die TU Wien stellt den Passwortmanager 1password im Testbetrieb zur Verfügung. Bei Fragen dazu wenden Sie sich derzeit bitte noch an infosec@tuwien.ac.at. Die TU.it ist bemüht, das Service sobald wie möglich über ihre Website zur Verfügung zu stellen.

Eine Anleitung wie Sie Ihr TU-Passwort ändern können finden Sie hier: https://www.it.tuwien.ac.at/rechte-und-rollen/accounts-an-der-tuw/accounts-fuer-mitarbeiter-innen/

Wann ein Passwort sicher ist und wie Sie ein sicheres Passwort erstellen, erfahren Sie in diesem kurzen Video:

Geräte

TU Laptop

Bei diesen Laptops handelt es sich in der Regel um administrativ betreute Geräte, sei es bei einem TUclient durch die TU.it oder bei dezentral servicierten Geräten durch den_die IT-Admin der jeweiligen Organisationseinheit.

Primär sollten diese Betreuer_innen für Fragen oder Hilfe kontaktiert werden, da sie im Regelfall die Möglichkeit eines Remote-Zugriffs (beispielsweise via Teamviewer) auf Ihren Client haben und so direkte Unterstützung leisten können.

Fragen an die TU.it können per E-Mail an help@it.tuwien.ac.at gerichtet werden. Es gibt außerdem die Möglichkeit, unter https://support.tuwien.ac.at/assystnet/ direkt ein Ticket anzulegen.

Sicherheits-Anwendungen wie Antivirenschutz, Firewalls, Endpointsecurity usw. sollten auf einem aktuellen Updatestand sein. Gleiches gilt auch für dein Betriebssystem und die verwendete Software.

Beachten Sie, dass nur Sie auf Ihrem TU-Laptop arbeiten dürfen! Es ist nicht gestattet, andere Familienangehörige an diesem Rechner arbeiten zu lassen.

Privater PC oder Laptop

Verwenden Sie einen privaten Laptop oder PC, legen Sie nach Möglichkeit ein separates, passwortgeschütztes „Firmenkonto“ an. Eine Anleitung für Windowsrechner finden Sie beispielsweise hier: https://support.microsoft.com/de-de/help/4026923/windows-10-create-a-local-user-or-administrator-account oder unter https://www.heise.de/tipps-tricks/Windows-10-Neuen-Benutzer-anlegen-4058638.html.

Ist es nicht möglich, ein separates Konto anzulegen, ist darauf zu achten, dass Sie sich nach getaner Arbeit von allen Services der TU Wien wieder aktiv abmelden. Speichern Sie heikle Daten nach Möglichkeit nur in Ordnern, auf die nur Sie Zugriff haben. Wie Sie auf einem Windows-Rechner einen Ordner mittels Passwort schützen können, erfahren Sie beispielsweise hier: https://www.heise.de/tipps-tricks/Ordner-mit-Passwort-schuetzen-unter-Windows-3703169.html. Sollte dies nicht möglich sein, speichern Sie Dokumente, die Sie lokal bearbeitet haben, in der TUowncloud oder in Ihrem TUfiles-Ordner und löschen Sie alle lokal, direkt auf Ihrem Rechner gespeicherten Daten, sobald Sie Ihre Arbeit beendet haben.

Verwenden Sie das Betriebssystem Windows, muss es sich dabei jedenfalls um die Version 8.1 oder höher handeln, da es für Windows 7 und 8 seit über einem Jahr keine Sicherheitsupdates mehr gibt. Das Upgrade von Windows 7 und 8 auf die Version 10 ist nach wie vor gratis möglich (https://www.microsoft.com/de-de/software-download/windows10). Achten Sie auch darauf, dass die Anti-Viren-Software aktuell gehalten wird. Bei Windows 10 passiert dies automatisch.

Ähnlich wie bei Microsoft Windows gibt es bei Apple-Produkten onboard Möglichkeiten zur Festplatten Verschlüsselung. Näheres dazu finden Sie hier: https://support.apple.com/de-at/HT204837.

Bitte stellen Sie sicher, dass das Gerät auf dem Sie arbeiten verschlüsselt ist.

Achtung, wenn sie externe Datenträger mit den onboard Programmen verschlüsseln, können die Daten meist nicht auf anderen Betriebssystemen gelesen werden, da meistens über das Filesystem auf den Datenträgern verschlüsselt wird.

Will man betriebssystemübergreifend arbeiten, dann empfiehlt sich das Programm Vera-Crypt, es kann auf Windows, MacOS und Linux installiert werden und auch für alle lesbare verschlüsselte externe Datenträger erstellen.

https://www.veracrypt.fr/en/Home.html oder https://www.heise.de/download/product/veracrypt-95747

Um Daten über „unsichere“ und meist freie Cloud-Fileshares zu synchronisieren, empfiehlt sich das Programm Cryptomator, das ein virtuelles Laufwerk generiert und im Hintergrund die Daten verschlüsselt in der Cloud ablegt, auch dieses Programm ist für Windows, MacOS und Linux verfügbar.

https://cryptomator.org/de/

Detaillierte Tipps und Anleitungen, wie Sie Ihren privaten PC oder Laptop sicherer machen können, finden Sie hier im coLab unter folgendem Link: Für Anwender_innen.

Handy

Laden Sie nach Möglichkeit nur zertifizierte Apps auf Ihr Telefon. Verfügen Sie über ein Firmenhandy darf dies ausschließlich von Ihnen genutzt werden. Wenn Sie Firmen-E-Mails über Ihr privates Telefon abrufen oder Sie das TU Adressbuch dorthin synchronisieren, gehen Sie sicher, dass Ihr Handy von anderen Personen nicht unbeaufsichtigt benutzt wird. Auf vielen Handys und Tablets gibt es die Möglichkeit, eigene Profile (beispielsweise für Kinder) anzulegen. Bitte prüfen Sie, ob dies auf Ihren Geräten möglich ist, und richten Sie separate Konten ein, sofern Ihr Gerät auch von anderen Personen benutzt wird. Stellen Sie sicher, dass Ihre Geräte verschlüsselt sind. Eine Anleitung zum Verschlüsseln von Android-Geräten finden Sie beispielsweise hier: https://www.heise.de/tipps-tricks/Android-Daten-verschluesseln-so-geht-s-4049575.html.