Verhaltensregeln zur Informationssicherheit

—

ETAT DE FRIBOURG
STAAT FREIBURG

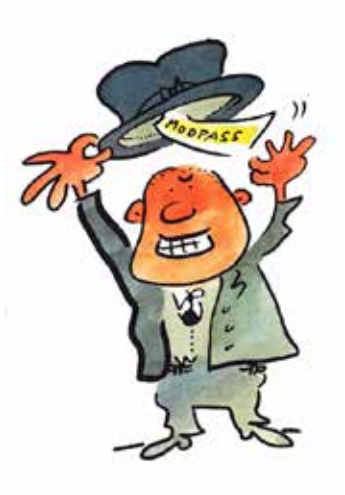
Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

EC 916

Passwörter

Behandeln Sie Ihr Passwort wie Ihre Zahnbürste!

- Nie mit jemandem teilen.
- Sorgfältig auswählen.
- Regelmässig wechseln.



Verwenden Sie für Ihre Passwörter eine Kombination aus Ziffern, Buchstaben und Sonderzeichen.

- Ein sicheres Passwort besteht aus mindestens 10 Zeichen.
- Es setzt sich zusammen aus **Ziffern, Buchstaben** und **Symbolen** (Sonderzeichen, Interpunktionen).
- Es darf keine auf Ihre Person bezogenen Daten enthalten (Vorname, Geburtsdatum usw.).
- Es darf nicht in einem Wörterbuch vorkommen (auch nicht in einem fremdsprachigen). Es kann dagegen aus einem Satz mit mindestens 4 Wörtern (ohne Abstand) bestehen, aber immer aus Ziffern, Buchstaben oder Zeichen zusammengesetzt (sog. **Geheimsatz** oder **passphrase**).

Passwörter NIE weitergeben und nicht irgendwo notieren.

- Geben Sie Ihr Passwort NIE weiter, **weder an Kollegen** (auch nicht bei Ferienvertretung), **noch an Vorgesetzte, und auch nicht an Ihren Ehepartner.**
- Ein Passwort darf nicht von mehreren Personen gemeinsam verwendet werden.
- Ein Passwort darf unter keinen Umständen weitergegeben werden.

Benutzen Sie unterschiedliche Passwörter für unterschiedliche Anwendungen, vor allem für Online-Dienste.

—

- Verwenden Sie für **jede** Online-Dienst-Anmeldung **ein anderes** Passwort.
- Verwenden Sie vor allem nie ein Passwort, das Sie schon für eine **andere Anwendung** benützen (wie zum Beispiel das Passwort für Windows oder Ihre Mailbox).
- Je mehr **Anwendungen mit Zugriffsbeschränkung** Sie nutzen, desto mehr verschiedene Passwörter brauchen Sie!

Die Mehrfachverwendung eines Passworts erhöht die Gefahr von Daten- und Identitätsdiebstahl.

Passwörter in regelmässigen Abständen ändern.

—

- Die maximale Lebensdauer eines Passworts hängt von der zu schützenden Anwendung ab und sollte nicht mehr als **90 Tage** betragen.
- Wenn Ihr Passwort einen weniger wichtigen Zugang schützt, brauchen Sie es nicht so oft zu ändern.
- Schützt Ihr Passwort hingegen einen wichtigen Zugang wie beispielsweise zu Ihrem Computer oder Ihrem E-Banking-Account, ändern Sie es regelmässig.

Wenn Sie vermuten, dass jemand anderes Ihr Passwort kennt, ändern Sie es sofort!

Voreingestellte Passwörter so schnell wie möglich ändern.

—

- Wird Ihnen ein standardmässiges Passwort zugewiesen, **so müssen Sie es unbedingt ändern.**
- **Ein neues Passwort muss immer zweimal eingegeben werden,** um Tippfehler auszuschliessen.

Besondere Vorsicht ist geboten, wenn Sie einen öffentlichen Computer nutzen. Man kann nie wissen, ob die eingegebenen Passwörter von Schadprogrammen ausgespäht werden!

Wenn Sie sich in einem Internetforum oder einer Plattform anmelden, müssen Sie eine Mail-Adresse und ein Passwort als Zugangsschutz für dieses Forum eingeben:

- **Geben Sie NIE das Passwort Ihres Windows- oder E-Mail-Accounts an.**
- **Der Administrator des Forums** kann nämlich auf die Informationen zugreifen, die Sie ihm gegeben haben, vor allem wenn die Website, auf der Sie Ihr Benutzername und Ihr Passwort (login) speichern, schlecht gesichert ist.

Wenn Sie mehrere Passwörter verwenden, wählen Sie einen Passwort-Manager oder Passwort-Safe.

Wie erinnern Sie sich an ein gutes Passwort?

–

- **Schreiben Sie** das Passwort **nicht auf Papier** auf, um es in Ihrem Büropult oder in Ihrer Brieftasche aufzubewahren.
- Wählen Sie einen **Geheimsatz,** wie oben erwähnt.
- Sie können auch einen Satz wählen wie «Es waren einmal 3 kleine Hündchen: Pim Pam Pum.» Nehmen Sie die Anfangsbuchstaben und die Interpunktionen, was ergibt: Ewe3kH :PPP.
- Falls nötig, ergänzen Sie Ihr Passwort mit Spezialzeichen, wie zum Beispiel @ anstelle von a.

E-Mail

Gehen Sie mit Ihrer E-Mail-Adresse gleich um wie mit Ihrer Telefonnummer!

- Nicht jedem x-Beliebigen geben.
- Kritisch sein.
- Aufpassen, mit wem man sich austauscht.

Vorsicht bei der E-Mail-Bearbeitung.

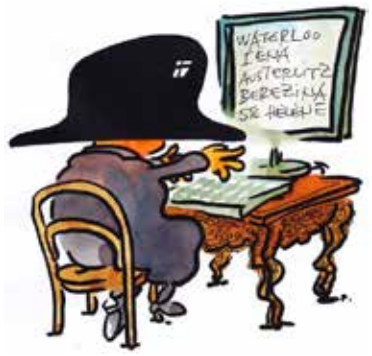
- Wenn Sie eine E-Mail von ausserhalb Ihrer Organisation erhalten, trauen Sie auch keinem bekannten Absender, wenn Ihnen der Inhalt der Nachricht verdächtig erscheint.
- Bevor Sie eine Aktion ausführen, zu der Sie in einer E-Mail aufgefordert werden, und Sie Zweifel in Bezug auf den Absender oder die verlangte Aktion haben, klären Sie zuerst ab, woher diese E-Mail kommt, indem Sie zum Beispiel den Absender anrufen.

Wenn Sie eine wichtige E-Mail erhalten, sollten Sie immer eine Bestätigung verlangen.

Beim Mailverkehr ist es wie am Telefon wichtig, den Grund für den Anruf bzw. das Mailing zu kennen und zu wissen, worum es geht und mit wem man es zu tun hat.

Eine E-Mail-Adresse ist kein effektives Identifikationsmittel.

Denken Sie daran, dass E-Mail-Adressen «gekapert» und von Personen verwendet werden können, denen sie gar nicht gehören.



*Verwenden Sie für die E-Mail-Angabe auf einer «nicht beruflichen» Website **eine anonyme Adresse** mit einem Pseudonym und einem anderen Namen als dem Ihrer Organisation, z. B. bill@bluewin.ch.*

Geben Sie Ihre E-Mail-Adresse nicht öffentlich bekannt.

–

- **Geben Sie** Ihre beruflichen und privaten E-Mail-Adressen **nicht leichtfertig bekannt.**
- Nutzen Sie Ihre berufliche E-Mail-Adresse ausschliesslich für berufliche Zwecke.
- Geben Sie Ihre private E-Mail-Adresse nur **vertrauenswürdigen Personen** bekannt.

***Bemerkung:** In gewissen Fällen ist es allerdings unumgänglich, auf einen Link mit E-Mail-Adresse zu klicken (z.B. wenn das Passwort vergessen ging). Dies geschieht allerdings auf Ihre Anforderung hin.*

Vorsicht vor E-Mails mit Links auf Websites, es könnte ein Virenangriff oder ein Phishingversuch dahinterstecken.

–

- Klicken Sie keine in einer E-Mail enthaltenen **externen Links** an.
- **Geben Sie die normale Internetadresse** der Website selber ein und nicht unbedingt die in der E-Mail angegebene.
- Der Absender dieser Adresse kann nämlich versuchen, Sie **auszutricksen** und auf eine **gefälschte Website** zu locken.

Öffnen Sie keine angehängten Dateien mit zwei Erweiterungen wie beispielsweise «picture.bmp.vb».

Vorsicht mit Fotos, PowerPoint-Präsentationen, Animationen und sonstigen eingefügten Dateien, denn die E-Mail kann auch ohne das Wissen des Absenders infiziert sein.

Vorsicht vor angehängten Dateien, sie können Viren enthalten.

–

- An eine E-Mail mit unbekanntem **Absender** angehängte Dateien möglichst **nicht öffnen.**
- Müssen Sie Dateien öffnen, die Sie von **Unbekannten** erhalten haben, vergewissern Sie sich, dass diese Dateien mit einem **Virenscanner** überprüft worden sind. Sie können die Dateien auch selber mit Ihrem Antivirusprogramm auf Viren überprüfen.

Vorsicht bei beruflichen Informationen mit vertraulichem Charakter.

—

› Verschicken Sie keine beruflichen E-Mails an Dritte, die nicht geschäftlich mit Ihrer Organisation zu tun haben, und halten Sie sich an das **Berufsgeheimnis**, dem Sie unterstehen.
› Bewahren Sie keine auf Ihre beruflichen Projekte bezogenen Dokumente in Ihrer Mailbox auf. Speichern Sie sie auf **dem Netzwerklaufwerk.**

Versenden Sie vertrauliche Daten nur verschlüsselt per E-Mail.

Beantworten Sie keine E-Mails, in denen persönliche Informationen verlangt werden.

—

› Seriöse Organisationen verlangen niemals die Bekanntgabe von **persönlichen** Informationen oder **Zugangsdaten per E-Mail** (Login, Bankkontennummer usw.).
› Sind Sie über die Herkunft einer Nachricht im Zweifel, kontaktieren Sie direkt die Organisation, von der sie gesendet wurde, um deren **Identität** zu überprüfen.

Füllen Sie keine per E-Mail gesendeten Formulare unbekannter Herkunft aus.

Verschicken Sie keine Ketten-E-Mails.

—

› Leiten Sie NIE eine E-Mail an **Ihr ganzes Adressverzeichnis** weiter, Sie können so selber zum Spammer werden.
› Reagieren Sie nicht auf Kettenbriefe!

*Wenn Sie eine Nachricht weiterschicken, ohne die **Quelle** zu überprüfen, lassen Sie sie aufgrund Ihrer guten Reputation als Versender vertrauenswürdig erscheinen, auch wenn sie es gar nicht ist!*

Internet

Surfen im Internet ist wie Segeln auf hoher See!

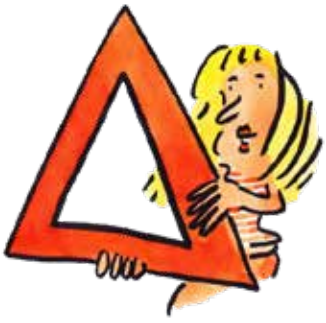
- Nie unbedacht auf allen möglichen Websites surfen.
- Netiquette einhalten.
- Vorsicht mit Privatem.

Verwenden Sie im Internet für den Zugang zu sensiblen Anwendungen (E-Commerce / E-Banking) immer starke Passwörter.

- Führen Sie Ihre Transaktionen auf **vertrauenswürdigen** und **sicheren** Websites durch **https:\\www…** Mit dem Protokoll «https://...» (sicheres http) lässt sich der Datenverkehr verschlüsseln. Damit wird es fast unmöglich, dass ein Dritter, der gesicherte Webverbindungen hackt, auf den Inhalt der Internetseiten und den darüber laufenden Datentransfer zugreifen kann.
- In der Regel erscheint das Schloss-Symbol für sichere Sites im Browserfenster und zeigt an, dass die Verbindung mit der besuchten Website gesichert ist.

Verlassen Sie sensible Webapplikationen immer über das Logout.

- Webbrowser löschen Cookies nur dann, wenn Sie Ihre Sitzung ganz geschlossen haben.
- Mit Cookies werden Optionen gespeichert, die Sie angekreuzt haben, um sie bei Ihrem nächsten Besuch nicht nochmals eingeben zu müssen; diese Informationen können aber schädlich sein, wenn sie personenbezogen sind.



Verwenden Sie nie die Option «Sich an mich erinnern» (oder «angemeldet bleiben»).

- Die Option «angemeldet bleiben» erlaubt, Ihre Benutzeridentifizierung im Browser zu speichern, damit Sie beim nächsten Besuch der Webseite mit Zugriffsbeschränkung automatisch verbunden werden. **Verwenden Sie diese Option nie auf einem anderen PC als auf Ihrem eigenen** (und dies nur, wenn sie den PC mit niemandem teilen).
- Diese Option verwendet ein Cookie, das jedem Nutzer, der sich auf Ihrem PC einloggt, erlaubt, auf die entsprechenden Accounts zuzugreifen.

Bemerkung: *Diese Option setzt voraus, dass Sie den Browser schliessen oder den PC ausschalten, ohne sich aus der geschützten Webseite auszuloggen.*

Nie vorschnell einen in einer E-Mail oder einer angehängten Datei eingefügten Weblink anklicken.

—

› Solche Adressen können gefälscht sein! Statt sie anzuklicken, **tippen Sie sie lieber selber in der Adresszeile Ihres Browser ein.**
› Das klassische Vorgehen zur Täuschung der Internetnutzer zwecks Datendiebstahls besteht darin, sie dazu zu bringen, eine Internetadresse in einer E-Mail anzuklicken.

Seien Sie zurückhaltend bei der Weitergabe persönlicher Informationen.

—

› Machen Sie niemals **persönliche Angaben** auf nicht gesicherten Websites.
› Geben Sie niemals sensible Informationen wie **Bankdaten** auf Websites preis, die nicht alle erforderlichen Schutzgarantien bieten.
› Geben Sie keine **unangebrachten Kommentare** in **öffentlichen Foren** ab. Seien Sie sich bewusst, dass solche Beiträge für immer archiviert bleiben!

Um im Internet zu surfen, sollte Ihre Software regelmässig aktualisiert sein, vor allem Ihre Sicherheitssoftware.

—

› In der Regel haben es Hacker auf Computer mit nicht aktualisierter **Software** abgesehen und nutzen die nicht behobenen **Sicherheitslücken**, um sich Zugang zu verschaffen.
› Deshalb ist es ganz wichtig, dass Sie Ihr **System** und alle Ihre **Programme** aktualisieren, um solche Lücken zu schliessen, und dass Sie ein Antivirenprogramm verwenden.

Die neuen Browser besitzen eine Aktualisierungsfunktion.

Loggen Sie sich nicht über einen auch anderen Nutzern zugänglichen Computer auf eine Bankwebsite ein.

—

› Ein fremder oder frei zugänglicher Computer bietet **keinerlei Gewähr** punkto Sicherheit.
› Man kann nie wissen, ob er mit Spyware infiziert ist und so Ihre Tastatureingaben aufgezeichnet werden, um Ihr **Passwort** und Ihren Zugangscode auszuspähen.

Vorsicht bei der Nutzung eines allgemein zugänglichen Computers im öffentlichen Raum.

Datenschutz

Hüten Sie Ihre Daten wie Ihren Augapfel!

- Nicht jeden x-Beliebigen auf Ihre Daten zugreifen lassen.
- Sorge zu Ihren Daten tragen, sie sind sehr wertvoll.
- An einem sicheren Ort aufbewahren.

Um jeglichen Missbrauch Ihrer Identität zu vermeiden, sperren Sie Arbeitsplatz, wenn Sie ihn verlassen, auch wenn es nur für wenige Minuten ist.

Respektieren Sie die allgemeinen Verhaltensregeln beim Gebrauch der Informationssysteme im Berufsumfeld.

- Sie sind für alle Operationen und Aktionen, die unter Ihrem Namen ausgeführt werden, **verantwortlich** (login und Passwort).
- Achten Sie auf strenge Einhaltung der Verhaltensregeln in risikoreichen Situationen.

Nicht unbedingt alles, was möglich ist, ist auch legal oder erlaubt!

- Die **Schweizer Gesetze**, namentlich das **kantonale Gesetz über den Datenschutz (DSchG)**, das Bundesgesetz über den Datenschutz (DSG) sowie die **internationalen Gesetze** müssen eingehalten werden.
- Ausserdem müssen Sie **die internen Reglemente Ihrer Organisation befolgen und sich an vertragliche Auflagen** sowie an die Vorgaben der Kunden halten, für die Sie arbeiten.

Halten Sie die Regeln zum Schutz des geistigen Eigentums ein

- Dies gilt sowohl für Software als auch für jegliche Art von **geistiger Schöpfung** im Internet.
- Innerhalb Ihrer Organisation darf nur Software verwendet werden, für die **Lizenzen** erworben wurden.
- Besonders darauf zu achten ist, dass die **Autorenrechte** eingehalten werden, wenn Sie Informationen (Texte, Bilder, Sonstiges) aus dem Internet kopieren.

Speichern Sie keine unrechtmässigen Inhalte auf einer Festplatte des IT-Systems Ihrer Organisation oder auf anderen Speichermedien.

—

Sie dürfen **keine** Nachrichten, Bilder oder Informationen **hochladen, verbreiten** oder **speichern**:

- die beleidigend, verleumderisch, diffamierend, ehrverletzend, rufschädigend oder menschenverachtend sind
- die andere Benutzer oder Dritte dazu verleiten oder es ihnen ermöglichen, **Rechte an geistigem Eigentum** zu verletzen
- und damit das Briefgeheimnis verletzen.

Sollten Sie Unregelmässigkeiten feststellen oder Nachrichten mit unrechtmässigen Inhalten erhalten, so müssen Sie dies Ihrem Vorgesetzten oder der Direktion Ihrer Organisation melden.

Nutzen Sie die IT-Ressourcen im legitimen Rahmen Ihrer Tätigkeit.

—

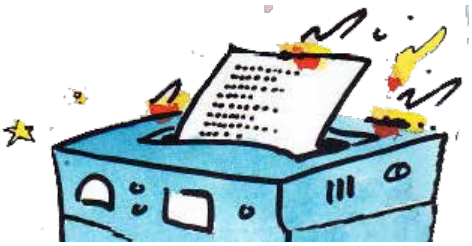
- Die Nutzung der IT-Ressourcen Ihrer Organisation muss sich auf Ihre **beruflichen Aufgaben** beschränken.
- Die Daten Ihrer Organisation dürfen **nicht** von **Unbefugten** verwendet werden.

*Es ist verboten, sich Kenntnis von **vertraulichen Informationen** im Besitz anderer Nutzer zu verschaffen, auch wenn diese sie nicht explizit geschützt haben.*

Lassen Sie Ihre Ausdrucke nie unbeaufsichtigt.

—

- **Vertrauliche Dokumente**, die Sie auf einem Gerät ausdrucken oder kopieren, das sich nicht in Ihrer unmittelbaren Nähe befindet, **nicht liegen lassen.**
- Löschen Sie bei einer Druckerpanne die Dokumente in der Warteschlange.

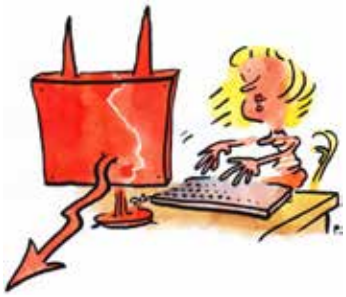


*Vorsicht bei **Multifunktionsgeräten**! Ohne Authentisierungsfunktion und/oder Verschlüsselung der Datenübertragung sind Ihre **vertraulichen** Dokumente nicht vor unbefugtem Zugriff geschützt. Vorsicht auch bei Standarddruckern.*

Sie sind für den Umgang mit jeglichen digitalen Speichermedien verantwortlich.

—

› Bevor ein persönliches digitales Speichermedium auf dem IT-System Ihrer Organisation **eingesetzt** werden darf, muss die Zustimmung der Direktion Ihrer Organisation eingeholt werden.
› Die Verwendung von digitalen Speichermedien ist **streng reglementiert.**



Vorsicht bei der Weitergabe von Informationen.

—

› Prüfen Sie, mit **wem Sie es zu tun haben,** bevor Sie Informationen herausgeben.
› Achten Sie **an öffentlichen Orten** darauf, wer sich in Ihrer **Nähe** aufhält.
› Achten Sie am **Telefon** oder in der **Öffentlichkeit** darauf, **nicht zu laut** zu sprechen!

Wenn Sie vertrauliche Informationen beispielsweise per E-Mail versenden müssen, verwenden Sie ein Verschlüsselungsprogramm (siehe «E-Mail»).

—

› Sie können Ihre E-Mails mit einem Krypto-programm wie beispielsweise PGP **verschlüsseln**.
› Zum Schutz von besonders schützenswerten Personendaten empfiehlt auch der Eidgenössische Datenschutzbeauftragte eine solche Verschlüsselung.

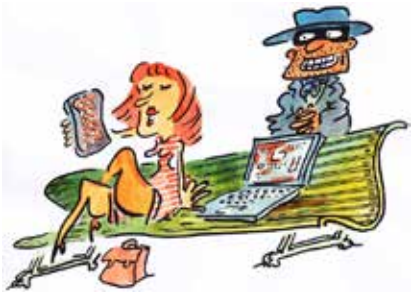
Einige Begriffe:

—

› Unter **Personendaten** (Daten) sind alle Angaben zu verstehen, die sich auf eine bestimmte oder bestimmbare Person beziehen.
› Als **besonders schützenswerte Personendaten** gelten Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe sowie über strafrechtliche oder administrative Sanktionen.
› Unter **Bearbeiten** ist jeder Umgang mit Personendaten zu verstehen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.
› Als **Datensammlung** wird jeder Bestand von Personendaten bezeichnet, der so aufgebaut ist, dass die Daten nach den betroffenen Personen erschliessbar sind.
› Der Begriff **Verantwortlicher der Datensammlung** steht für das öffentliche Organ, das über den Zweck und den Inhalt einer Datensammlung entscheidet.
› Der **Datenschutzverantwortliche** ist die Kontaktperson für alle Fragen zum Datenschutz.

Mobilität

Lassen Sie Ihre mobilen Geräte nicht aus den Augen!



- Keine allzu wichtigen Daten auf Mobilgeräten speichern.
- Nicht jedem x-Beliebigen ausleihen.
- Nicht herumliegen lassen.

Sie tragen die Verantwortung für die von Ihnen mitgenommenen Informationen.

- Lassen Sie Ihre **Mobilgeräte nie unbeaufsichtigt.** Stecken Sie sie wenn möglich weg oder halten Sie sie **unter Verschluss!**
- Lassen Sie sich beispielsweise in der **Öffentlichkeit nicht über die Schulter blicken.** Schützen Sie Ihren Bildschirm vor neugierigen Blicken.
- Melden Sie einen **Verlust oder Diebstahl** von Mobilgeräten mit beruflichen Daten umgehend Ihrem Vorgesetzen.

Schützen Sie den Zugang zu den Informationen auf Ihren Mobilgeräten mit einem Passwort.

- Ein gutes Passwort muss **schwer zu erraten** sein, auch von Personen, die Sie sehr gut kennen!
- Ein gutes Passwort sollten Sie **sich leicht merken** können, ohne es irgendwo **notieren** zu müssen!

Speichern Sie nie vertrauliche Daten unverschlüsselt auf Ihren Mobilgeräten.

- Halten Sie sich an die **Verschlüsselungsvorschriften Ihrer Organisation.**

Schützen Sie Ihre mobilen Datenträger vor Schadprogrammen.

–

› Überprüfen Sie den Inhalt der von Ihnen verwendeten mobilen Datenträger mit einer **Antivirensoftware**.
› Es gibt sehr gute kostenlose Antivirenprogramme für Ihre persönlichen Geräte. Regelmässige Updates nicht vergessen!

Schliessen Sie keine USB-Speichersticks an, wenn Sie mit erweiterten Zugriffsrechten arbeiten (z. B. als Administrator)!

–

› Um die **Aktionen einzuschränken**, die ein Stick auf dem IT-System ausführen kann, schliessen Sie USB-Sticks nur dann an, wenn Sie mit **eingeschränkten Rechten** arbeiten.
› Verfügen Sie über erweiterte Benutzerrechte für einen Computer oder das IT-System Ihrer Organisation, seien Sie vorsichtig bei der Verwendung von USB-Medien. **Idealerweise öffnen Sie eine andere Sitzung (mit einem anderen Login) mit sehr eingeschränkten Rechten.**

USB-Stick gründlich «säubern».

–

› USB-Sticks können **sensible Daten** enthalten.
› Bevor Sie einen USB-Stick **ausleihen** oder entsorgen, «säubern» Sie den Speicher und entfernen Sie alle vertraulichen Daten vollständig.

Sperren Sie wenn möglich den Zugriff auf Ihren USB-Stick.

—

- Manche USB-Sticks haben einen **physischen Schreibschutzschalter**, mit dem Sie den Schreibzugriff **sperren** können. Vergessen Sie nicht, ihn zu aktivieren.
- Das **bewahrt Sie nicht vor Datendiebstahl,** bietet also keine absolute Gewähr für die Vertraulichkeit, hindert aber **Aussenstehende** daran, den Inhalt des Sticks **ohne Ihr Wissen** zu **verändern** oder zu löschen!

Internetzugang aus einem öffentlichen WLAN ist nicht sicher und garantiert nicht, dass die Vertraulichkeit der heruntergeladenen Daten gewahrt bleibt.

—

- Beim Herunterladen aus einem öffentlichen WLAN, sind die Daten einsehbar.
- Es ist nicht auszuschliessen, dass unbefugte Personen den Datenfluss überwachen, um an Ihre **Passwörter** oder **vertrauliche Dokumente** zu gelangen.
- Laden Sie keine vertraulichen Daten herunter, wenn Sie ein **öffentliches WLAN** benützen. Müssen Sie es trotzdem tun, verwenden Sie eine verschlüsselte Verbindung **(VPN)** oder den **mobilen Hotspot** Ihres Smartphones.

Bring Your Own Device (BYOD) ist im beruflichen Umfeld immer mehr verbreitet.

—

- Von BYOD spricht man, wenn Mitarbeitende ihre privaten Smartphones oder Tablets für berufliche Zwecke verwenden.
- Verwenden Sie ein **sicheres Passwort** auf Ihrem Smartphone, wenn Sie es für berufliche Zwecke benützen.

Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB
Chorherrengasse 2, CH-1700 Freiburg
T +41 26 322 50 08
-
www.fr.ch/de/oedsmb
-
Dezember 2023
-
Illustrationen
Pécub, Pier Paolo Pugnale
Experte für Unternehmenskommunikation
http://www.pecub.ch/