**Vorlage: Merkblatt für Mitarbeitende im Homeoffice**

**So ist Ihre Arbeit im Homeoffice sicher**

|  |  |
| --- | --- |
| **Gefahr** | **Massnahmen dagegen** |
| Ungesperrte Computer | Sperren Sie Ihren Computer! Dies gilt nicht nur im Homeoffice, sondern auch im Büro und auf Geschäftsreisen. Wenn Sie nicht in Reichweite sind, muss Ihr PC gesperrt sein.  Im Homeoffice geht es nicht einmal so sehr um böswillige Personen, die an Ihre Daten gelangen wollen, sondern auch um neugierige Kinder, die beim Herumspielen ungewollt Dateien löschen oder anderen Schaden anrichten können. |
| Offen herumliegende Datenträger | Schliessen Sie Datenträger wie USB-Sticks oder externe Festplatten weg, wenn Sie sie nicht benutzen. Ideal ist, wenn die Daten darauf verschlüsselt sind. |
| Fremde Leute im Haus | Lassen Sie sich nicht über die Schulter schauen. Der Sanitär repariert den Abfluss, die Nachbarin bringt einen Kuchen vorbei – achten Sie darauf, dass keine wichtigen Dokumente offen herumliegen und dass niemand auf Ihren Bildschirm schauen kann.  Vor allem, wenn Sie mit sensiblen Daten arbeiten, besteht das Risiko, dass sich Personen unter falscher Identität Zutritt zu Ihrem Haus verschaffen, um so einen Blick auf Ihre Unterlagen und in Ihre Arbeitstätigkeit zu erhaschen. |
| Mitgehörte Gespräche | Nutzen Sie Kopfhörer – vor allem auch wenn Sie unterwegs arbeiten.  Vertrauliche Gespräche am Telefon oder im Videocall sollte niemand mithören können – mit einem Kopfhörer sind immerhin die Worte Ihrer Gesprächspartner geschützt. Schliessen Sie bei vertraulichen Gesprächen Türen und Fenster. |
| Einsehbare Bildschirme | Achten Sie auf die Position Ihres Bildschirms: Kann der Nachbar durch das Fenster darauf sehen? Dann stellen Sie das Gerät um. Oder benutzen Sie Schutzfolien, die gegen Blicke aus der Ferne schützen. |
| Einblick in die Privatsphäre | Achten Sie auf den Hintergrund – vor allem wenn Sie kein separates Arbeitszimmer zur Verfügung haben. Sonst sind durch die Kamera viele Dinge sichtbar, die Sie besser nicht zeigen sollten: etwa Bilder Ihrer Familie oder Ihre Einrichtung.  Das ist nicht nur ein Eingriff in Ihre Privatsphäre, sondern kann auch ein Risiko für Social-Engineering-Angriffe darstellen. Ein Angreifer kann beispielsweise die Anzahl, Namen oder Bilder Ihrer Familienmitglieder benutzen, um Ihre Identität zu missbrauchen. Nutzen Sie daher einen Hintergrundfilter; viele Videokonferenz-Tools bieten diese Möglichkeit standardmässig. |