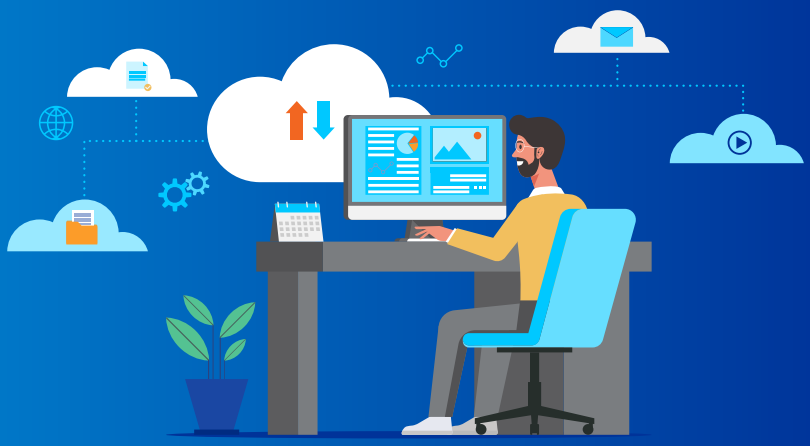
Sicherheit im Home Office: diese 15 Tipps müssen Sie beachten

Machen Sie Ihren Home Office-Arbeitsplatz sicher und schützen Sie sich und Ihr Unternehmen vor Cyberkriminellen



Sperren Sie Ihren Rechner, wenn sie abwesend sind

Auch wenn Sie Ihren Arbeitsplatz nur kurz verlassen, sollten Sie Ihren Rechner sperren. Ein sicheres und nur Ihnen bekanntes Passwort verhindert, dass Unbefugte (dazu gehören auch Familienmitglieder oder Mitbewohner) Einsicht in die Unternehmensdaten haben.

Schützen Sie Ihren Bildschirm vor Einblick durch Andere

Stellen Sie sicher, dass niemand Ihren Monitor einsehen kann. Richten Sie ihn dazu so aus, dass keine Fenster oder Türen hinter Ihnen sind. Arbeiten Sie außerdem nicht in videoüberwachten Bereichen. Am besten verwenden Sie eine Blickschutzfolie.

Achten Sie darauf, dass niemand Videokonferenzen oder Telefonate mithört

Wenn Sie telefonieren oder an einer Videokonferenz teilnehmen, sollten sie sicherstellen, dass niemand dabei zuhören kann. Wenn das nicht möglich ist, vermeiden Sie es unbedingt, sensible Daten (wie zum Beispiel die Namen von Kunden) zu nennen.

Sorgen Sie für sichere Ausdrucke an gemeinsam genutzten Druckern

Wenn sie geschäftliche Unterlagen an gemeinsam genutzten Netzwerkdruckern ausdrucken, sollten Sie darauf achten, dass niemand sonst Einsicht in diese Dokumente hat. Stellen Sie außerdem sicher, dass die Daten nicht auf dem Drucker gespeichert werden.

Vernichten Sie betriebliche Unterlagen auf sichere Art

Werfen Sie Unternehmensunterlagen nicht einfach in den Papiermüll, denn dann könnten Sie unter Umständen von Dritten eingesehen werden. Verwenden Sie stattdessen einen Schredder, damit keine Daten rekonstruiert werden können.

Bewahren Sie Ihre Arbeitsmittel sicher auf

Wenn Sie sich nicht an Ihrem Arbeitsplatz befinden, schließen Sie Firmenunterlagen sowie Rechner und mobile Endgeräte am besten in einem Schrank oder einer Schublade ein. So kann diese niemand unberechtigt an sich nehmen. Hinterlassen Sie Ihren Arbeitsplatz am besten vollständig aufgeräumt.

Verwenden Sie betriebliche Endgeräte nicht für private Zwecke

Ihren geschäftlichen Rechner sollten Sie auch wirklich nur zum Arbeiten verwenden. Wenn Sie privat im Internet surfen, könnten Sie unwissentlich auf schadhafte Seiten gelangen und dadurch nicht nur Ihren Rechner, sondern auch das Firmennetzwerk gefährden. Achten Sie deshalb auch während der Arbeit darauf, nur vertrauenswürdige Seiten zu besuchen.

Führen Sie geschäftliche Gespräche nicht über private Kommunikationsmittel

Bei Daten, die über private Messenger oder Mail-Server verarbeitet werden, können Sie nicht sicher sein, dass Ihre Informationen vor dem Zugriff durch Dritte geschützt sind. Nutzen Sie daher nur die Kommunikationswege, die für die geschäftliche Korrespondenz vorgesehen sind.

Nutzen Sie nur zugelassene Speichermedien und -dienste

Um Unternehmensdaten zu sichern, sollten Sie nur Speichermedien verwenden, die im Unternehmen gestattet sind. Private USB-Sticks, SD-Karten oder externe Festplatten sowie private Cloud-Speicher sind kein sicherer Ort für geschäftliche Daten. Schließen Sie zudem auch keine fremden Speichermedien an Ihren Rechner an, denn darauf könnte sich Schadsoftware befinden.

Arbeiten Sie nur mit Software, die Ihr Arbeitgeber gestattet

Wenn Sie ungeprüfte Software installieren, laufen Sie Gefahr, dass dadurch versehentlich Viren oder Trojaner ins Unternehmensnetzwerk gelangen. Nutzen Sie daher nur Programme, die Ihr Arbeitgeber auch offiziell vorgibt oder erlaubt.

Verwenden Sie eine sichere Internetverbindung und ein VPN

Nutzen Sie die höchsten Sicherheitseinstellungen für Ihr WLAN und verbinden Sie sich über ein VPN (Virtuelles Privates Netzwerk) mit dem Firmennetzwerk. Dadurch wird die Kommunikation verschlüsselt. Vermeiden Sie es, öffentliches WLAN zu benutzen.

Richten Sie sichere Passwörter und 2-Faktor-Authentifizierung ein

Starke Passwörter, die nur Ihnen bekannt sind, schützen Ihre Konten vor unbefugtem Zugriff. Wenn möglich, sollten Sie beim Login in Ihre geschäftlichen Accounts auch eine 2-Faktor-Authentifizierung nutzen. Geraten Passwörter in falsche Hände, sind Ihre Accounts auf diese Weise trotzdem vor unerlaubtem Zugriff geschützt, sodass Sie die Passwörter schnell ändern können.

Seien Sie wachsam gegenüber Spam und Phishing-Angriffen

Wenn Sie eine E-Mail erhalten, die Ihnen fragwürdig vorkommt, öffnen Sie diese sicherheitshalber nicht und wenden sich an Ihre IT-Abteilung. Sollte der Absender ein Kollege oder Vorgesetzter sein, fragen Sie lieber persönlich per Telefon nach. Klicken Sie keine enthaltenen Links oder Dateianhänge an und antworten Sie auch nicht direkt auf die E-Mail – es könnte sich um einen Betrugsversuch handeln.

Halten Sie Ihr Betriebssystem und Ihre Software auf dem neuesten Stand

Durch regelmäßige Updates Ihres OS und Ihrer Software werden kritische Sicherheitslücken geschlossen, durch die Hacker Ihr System infizieren könnten. Installieren Sie deshalb immer möglichst sofort neue Updates. Besonders wichtig ist hier auch die Antivirensoftware. Um Updates des Betriebssystems kümmert sich in der Regel Ihre IT-Abteilung.

Melden Sie Vorfälle an den IT-Support

Wenn ein Firmengerät beschädigt wurde, es zum Datenverlust kam oder Ihr Rechner von Malware befallen ist, wenden Sie sich umgehend an Ihre IT-Abteilung. So können weitere Folgen im besten Fall direkt verhindert werden und Sie erhalten eine Lösung für Ihr Problem.

👍 Alles befolgt? Prima, Sie sind bereit für die sichere Arbeit im Home Office!