Verhalten am Arbeitsplatz

Es kommt auf Sie an!

Durch ein Versehen oder technische Lücken könnte auch der Zugriff auf andere Datenbestände möglich werden. Daher sollten Sie – auch zu Ihrer persönlichen Absicherung - einige grundsätzliche Verhaltensregeln berücksichtigen.

+ Passwörter nicht weitergeben

Passwörter nicht weitergeben

Ihnen anvertraute oder von Ihnen erzeugte Passwörter dürfen Sie keinesfalls weitergeben. Es ist auch verboten, sie aufzuschreiben, in Schubladen, unter Schreibtischunterlagen o.ä. – also letztlich für Dritte zugänglich – aufzubewahren!

Passwörter sind personengebunden. Das heißt: Alle berechtigten Personen haben ein eigenes Passwort erhalten. Sie benötigen nicht das Ihrige!

Falls Sie Schwierigkeiten mit der Bedienung passwortgeschützter Daten oder Anwendungen haben, kann die zuständige Einheit auch ohne Kenntnis Ihres persönlichen Passworts Hilfe leisten.

Falls Sie befürchten, dass eine andere Person Ihr Passwort kennt, ändern Sie es unverzüglich ab.

+ Zugang sichern

Zugang sichern

Der Computer an Ihrem Arbeitsplatz ist das Tor zu den auf diesem Rechner gespeicherten Daten, aber auch zu Daten auf anderen Computern Ihrer Verwaltung und oft auch zum Internet.

Wenn Sie Ihr Büro verlassen, sollten Sie immer den Zugang zum Computersystem sperren. Dies geschieht mit einem einfachen Handgriff und verhindert, dass Dritte Zugriff auf Daten haben oder in Ihrem Namen Nachrichten schreiben.

Unter Windows sperrt z.B. die Tastenkombination „Windows-Taste + L“ das System so, dass es nur durch Eingabe Ihres Passwortes oder durch eine Person mit Administratorrechten wieder benutzt werden kann.

Es reicht nicht aus, Ihr Zimmer abzuschließen. Ein geübter Dieb schafft es innerhalb von Sekunden, ein normales Schloss zu öffnen.

+ Social Engineering-Angriffe abwehren

Social Engineering-Angriffe abwehren

Seien Sie misstrauisch, wenn jemand Ihre Zugangsdaten, insbesondere Passwörter erfragt. Dies gilt gerade bei Ihnen Unbekannten, die auf Auskunft drängen und sich auf ihre Autorität (hoher Funktionsträger etc.) oder eine hohe Dringlichkeit („Die Zeit drängt...“, „Sie behindern...“) berufen.

Häufig werden gezielt Personen für Angriffe ausgewählt, die keine sicherheitsrelevanten Aufgaben haben. Über deren Zugänge zu Anwendungen und Netzwerken versuchen die Angreifer und Angreiferinnen als Sprungbrett dann weiter in die Systeme einzudringen.

Wie verhalten Sie sich, wenn Sie Zweifel haben?

- Lassen Sie sich im Zweifelfsfall eine Rückrufnummer geben, die Sie überprüfen.
- Erkundigen Sie sich bei Vorgesetzten, Kollegen ob die anfragende Person vertrauenswürdig und "echt" ist.

+ Vorsicht bei mobilen Datenträgern

Vorsicht bei mobilen Datenträgern

Durch USB-Speichersticks, Smartphones und andere mobile Datenträger können leicht Daten auf und von Computern kopiert werden. Dies birgt erhebliche Gefahren.

Zum einen ist oft nicht nachvollziehbar, welche Daten vom Computer herunterkopiert werden. Somit sind ein „Diebstahl“ und die unberechtigte Verwendung von Daten möglich. Auch lassen sich kleine Geräte leichter verlieren oder stehlen.

Zum anderen besteht die Gefahr, dass auf den mobilen Geräten enthaltene Viren auf den Computer und damit in das Verwaltungsnetz gelangen.

Verwenden Sie daher mobile Datenträger an Ihrem Arbeitsplatz nur, wenn Ihnen dies gestattet ist und Sie einen aktuellen Virenscanner im Einsatz haben.

+ Verhalten im Schadensfall

Verhalten im Schadensfall

Verdächtige Vorfälle melden! Auf keinen Fall Gefahren ignorieren! Behalten Sie die Ruhe!

Sollten Sie den Eindruck haben, dass jemand durch vorsätzliches Einwirken auf Sie versucht, Passwörter, Zugangsdaten oder konkrete Inhaltsdaten zu erkunden, weisen Sie dieses Ansinnen höflich, aber bestimmt zurück und informieren Sie die Ihnen vorgesetzte Person und die Campus IT.

Schalten Sie Ihren Computer beim Verdacht auf einen Virus nicht eigenmächtig aus. Falls Ihnen die Kabel des Rechners vertraut sind, empfiehlt es sich, die Netzwerkverbindung durch Ziehen des entsprechenden Steckers oder Abschalten von WLAN- bzw. Mobilfunkverbindungen zu unterbrechen. Dadurch wird z.B. die Verbreitung eines Virus im Netzwerk verhindert.

Tauchen trotz des Befolgen aller hier vorgestellten Regeln Probleme auf, informieren Sie unverzüglich

die Campus IT.