Kontakt

Porsche Informatik Service Desk
+43 662 4670 2222
https://support.porscheinformatik.com

IT-Sicherheitsbeauftragter
Marcus Michalek, +43 662 4670 6488

INFORMATIONSSICHERHEIT
geht auch Sie an!

Herausgeber
Porsche Informatik - Informationssicherheit

Porsche Informatik GmbH
Handelszentrum 7 | 5101 Bergheim | Österreich
T +43 662 4670 0 | www.porscheinformatik.at

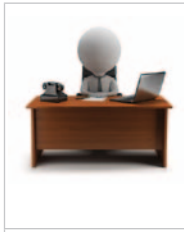
PORSCHE
INFORMATIK GMBH

Am Telefon meldet sich eine unbekannte Person und bittet Sie um sensible Informationen. Werden Sie ihr die Informationen geben? Sie wollen ihr ja gerne helfen.

Leider kann Ihre Hilfsbereitschaft von Kriminellen ausgenutzt werden.
Lösung: Geben Sie Informationen nur an berechtigte und bekannte Personen weiter. Überprüfen Sie die Person im Zweifelsfall mit Hilfe des Telefonbuchs oder im Internet.

Jemand meldet sich bei Ihnen z. B. als „Administrator". Unter einem Vorwand bittet er Sie um Ihr Passwort. Werden Sie es ihm nennen?

Immer noch werden mehr Passwörter am Telefon verraten als von Hackertools geknackt.
Lösung: Eine solche Frage ist immer unzulässig. Geben Sie Passwörter niemals weiter. Wenn Sie nach Passwörtern gefragt werden, melden Sie das bitte unverzüglich. Falls Sie den Verdacht haben, dass Ihr Passwort Dritten bekannt geworden ist, ändern Sie es unverzüglich.



Sie verlassen Ihr Büro. Ihr Rechner ist nicht gesperrt. Wissen Sie, wer sich an Ihrem Arbeitsplatz zu schaffen machen könnte?

Unversperrte PCs laden zum Zugriff auf sensible Daten ein.
Lösung: Sperren Sie beim Verlassen Ihres Arbeitsplatzes den Computer. Benutzen Sie hierfür den „Affengriff" [Strg]+[Alt]+[Entf] und klicken Sie „Computer sperren" an. Oder drücken Sie einfach gleichzeitig [Windows-Taste] und [L].

Sie erhalten ein E-Mail mit Anhang von einem unbekannten Absender. Öffnen Sie den Anhang? Er könnte ja interessant sein.

Viren, Würmer und Trojaner werden meist als Anhang versendet.
Lösung: Öffnen Sie keine Anhänge und klicken Sie bei E-Mails von Unbekannten nicht auf Links. Geben Sie niemals sensible Daten an Unbekannte weiter. Lassen Sie verdächtige E-Mails überprüfen. Kontaktieren Sie hierfür den Service Desk.

Sind Ihre Dokumente sicher aufbewahrt?

Die unsichere Aufbewahrung von Daten ist indirekt eine Einladung zum Datenmissbrauch.
Lösung: Lassen Sie keine sensiblen Daten offen auf Ihrem Schreibtisch liegen. Sensible Daten gehören nicht in den normalen Papierkorb, sondern in den Aktenvernichter. Vermeiden Sie die Verwendung von USB-Sticks sowie CDs/DVDs bei sensiblen Daten.

Im Internet haben Sie ein interessantes Programm gefunden. Es könnte Ihnen bei Ihren Aufgaben helfen. Installieren Sie es? Es reicht ja ein Doppelklick.

Diese angebotenen „Helfer" enthalten oft Schadsoftware und spionieren Daten aus.
Lösung: Lassen Sie nur freigegebene Software vom Benutzerservice installieren. Auch Bilder, harmlos aussehende Dokumente oder Videos können Schadsoftware enthalten. Nutzen Sie nur vertrauenswürdige Quellen.

Auf einer Messe bekommen Sie einen USB-Stick oder eine CD überreicht. Produktinformationen sollen darauf sein. Trauen Sie dem Inhalt?

Auf solchen Datenträgern kann Schadsoftware enthalten sein.
Lösung: Benutzen Sie solche Datenträger nicht ohne vorherige Prüfung. Verbinden Sie keine privaten Geräte (auch keine Telefone oder MP3-Player) mit dem Firmennetzwerk - Infektionsgefahr!

Sie kennen das: Hitzige Diskussionen mit Kollegen. Oder Sie sitzen im Zug, arbeiten an einem Dokument und telefonieren nebenbei. Wissen Sie immer genau, wer mithört oder mitliest?

Durch unvorsichtiges Verhalten können Unbefugte Informationen mithören oder mitlesen.
Lösung: Interne Informationen (Daten, Namen, Sachverhalte) gehören nicht in die Öffentlichkeit. Lassen Sie Unbefugte nicht mithören oder mitlesen, weder im Zug oder Flugzeug noch im Hotel oder im Restaurant.

Verwenden Sie sichere Passwörter?

Unsichere Passwörter können leicht von Unbefugten erraten werden, die dadurch Zugang zu Systemen erlangen können.
Lösung: Je länger ein Passwort, umso besser. Verwenden Sie auch Ziffern, Großbuchstaben und Sonderzeichen. Schreiben Sie Passwörter nie für andere sichtbar auf. Ändern Sie Ihre Passwörter regelmäßig.