Tipps und Tricks zum sicheren Umgang mit E-Mail und Internet

Die digitale Revolution und neue Technologien halten auch allerlei Gefahren bereit, deren Tragweite vielen Usern gar nicht bewusst sind. Folgende Richtlinien helfen dir, dich zu Hause oder im Betrieb vor Phishingattacken, Viren, dem Diebstahl sensibler Daten oder Mutwilligkeiten zu schützen:

1. E-Mail-Nutzung:

- Fülle die Betreffangabe (Subject) immer aus entsprechend der Betreffangabe in einem «normalen» Schreiben.
- Leite keine Dateien ungeprüft weiter (Forwarding).
- Verwende für externe E-Mails eine Signatur/Fussnote.
- Vertraue nicht auf Absenderangaben. E-Mail-Adressen können leicht gefälscht werden.
- Vorsicht vor Fehlmanipulationen: Überprufe vor dem Absenden immer noch einmal den bzw. die Adressaten. Sehr oft wird anstelle des «Reply»-Buttons (antworten) der «Reply all»-Button (allen antworten) gedrückt und so die Nachricht an viele Personen versendet, welche diese Nachricht vielleicht gar nicht erhalten sollten. Überprüfe zudem, ob der Anhang auch wirklich die gewünschte Datei enthält.
- Um Bedrohungen wie E-Mail-Bomben oder Spam-Mails entgegenzuwirken, solltest du genau überlegen, wann und wem du deine E-Mail-Adresse weitergibst.

2. Virenproblematik:

- Prüfe alle erstmals verwendeten externen Datenträger mit einem entsprechenden Programm auf mögliche Viren, bevor du mit diesen arbeitest (Viren können auch auf USB-Sticks, Flashkarten, CD-ROMs oder externen Harddiscs versteckt sein). Als Tipp für zu Hause. Im Geschäft geschieht dies durch ein automatisches Antivirenprogramm.
- Sei vorsichtig bei auffälligen Subject- oder Betreff-Angaben, auch wenn die E-Mail von dir bekannten Absendern stammt. Der gesunde Menschenverstand ist noch immer ein sehr wichtiger Aspekt beim Schutz vor Viren. Lösche verdächtige E-Mails sofort aus deinem Posteingang, ohne diese vorher zuöffnen!

3. «Clear Desk»-Richtlinien

- Bei längerer Abwesenheit ist der Computer ordnungsgemäss herunterzufahren.
- Türen zu Nebenräumen mit sensiblen Daten oder wertvollem Inhalten sind abzuschliessen.
- Aktiviere auch den automatischen Start des Bildschirmschoners mit Passwortschutz nach Ablauf einer bestimmten Inaktivitätsdauer, z.B. nach 15 Minuten.

4. Passwörter

Notiere niemals deine Passwörter auf irgendwelche Notizzettel. Klebe keine diesbezüglichen Informationen an den Monitor oder unter die Tastatur. Auch die «bequeme» fixe Speicherung von persönlichen Passwörtern in automatischen Prozeduren ist gefährlich.

Tipps für sichere Passwörter:

- Verwende keine Passwörter mit persönlichen Informationen, wie z.B. deiner Telefonnummer, dem Vornamen deiner Frau/deines Mannes, dem Geburtsdatum des ersten Kindes, deinem Autokennzeichen usw.
- Verwende mindestens 8 Zeichen: Ein sicheres Passwort besteht mindestens aus 8 Zeichen. Darin sollten Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen vorkommen.
- Verwende Zahlen in Passwörtern: Wenn im Passwort Zahlen verwendet werden, kann die Zahl systematisch ändern. Beispielsweisedie Monatsnummer: niemand kommt auf die Idee, dass die Zahl 21 den Monat August meint, weil nur du weisst, dass du deine Lieblingszahl 13 immer dazu addierst.
- Abgekürzte Sätze: Nimm von einem Satz, den du dir gut merken kannst, jeweils den ersten Buchstaben, und du erhältst ein Passwort mit einer sehr hohen Sicherheitsstufe. Beispiel:
  «**M**eine **1.** **K**atze **h**iess **F**ritz **u**nd **w**urde **8** **J**ahre **a**lt» ergibt als Passwort: **M1KhFuw8Ja**