01 Sperrbild-schirm aktivieren

02 Sichere Passwörter wählen

03 Betriebssystem und Antiviren-software aktuell halten

04 Erst denken, dann klicken

05 Sichere WLAN-Netze nutzen

06 Geschäfts-identität nicht privat nutzen

07 Unbekannte Personen überprüfen

08 Sensible Daten korrekt ablegen

09 Geprüfte Software nutzen

10 Verdacht melden

Die 10 goldenen Regeln der IT-Sicherheit

01 Sperrbildschirm aktivieren

Aktiviere den Sperrbildschirm immer, wenn du deinen Arbeitsplatz verlässt und lass mobile Geräte nie unbeaufsichtigt.

Windows: + L
Mac: ⌘ + Ctrl + Q
Mobil: Minimum ein PIN

02 Sichere Passwörter wählen

Gib niemals ein Passwort weiter. Verwende nur starke Passwörter und benutze für jedes Login ein anderes Passwort. Ein Passwortmanager kann dir bei der Generierung und Verwaltung von Passwörtern helfen.
Wenn du die Möglichkeit hast, benutze Zwei-Faktor-Authentifizierung, damit auch im Falle eines Passwort-Leaks deine Logins sicher sind.

03 Betriebssystem und Antivirensoftware aktuell halten

Update regelmässig das Betriebssystem deines Computers und halte deine Anti-Virensoftware auf dem neusten Stand. Nur so kannst du aktuelle Sicherheitslücken schliessen und bist vor den neusten Viren geschützt.

04 Erst denken, dann klicken

Bevor du auf einen Link klickst oder einen Anhang öffnest, stelle sicher, dass sie aus vertrauenswürdiger Quelle stammen.
So lädst du dir nicht aus Versehen Schadsoftware auf deinen Rechner.

05 Sichere WLAN-Netze nutzen

Wenn du unterwegs bist, vermeide die Nutzung öffentlicher und ungesicherter WLAN-Netze. Du kannst nie wissen, wer noch in diesem Netz unterwegs ist.

06 Geschäftsidentität nicht privat nutzen

Benutze deine UZH-Mailadresse und deinen UZH-Benutzernamen nicht für private Zwecke wie zum Beispiel für Social Media-Logins.
So sind deine Arbeitslogin auch bei einem Datenleak sicher.

07 Unbekannte Personen überprüfen

Überprüfe die Identität dir unbekannter Personen, bevor du ihnen unternehmensbezogene Informationen aushändigst oder Transaktionen tätigst. Andernfalls könnten wichtige Informationen in die falschen Hände geraten.

08 Sensible Daten korrekt ablegen

Verschlüssle sensible oder vertrauliche Dokumente oder speichere sie in geschützten Ordnern ab. Physische Dokumente solltest du in abschliessbaren Schränken aufbewahren und ausschliesslich in die dafür vorgesehenen Behälter entsorgen, denn normale Abfallcontainer können nach verkäuflichen Informationen durchsucht werden.

09 Geprüfte Software nutzen

Verwende ausschliesslich Software, die von der IT vorinstalliert oder im Software Center der UZH zum Download bereitgestellt wurde. Installiere keine Software, die nicht durch die IT geprüft und als sicher eingestuft wurde. Auch in seriös wirkender Software können Hintertüren oder Abhörvorrichtungen eingebaut sein.

10 Verdacht melden

Halt dich an die Regeln und Vorgaben der IT-Security und wenn du dir unsicher bist oder dir eine E-Mail verdächtig erscheint, melde dich beim Helpdesk oder der IT-Security.
Jeder Hinweis kann nützlich sein.

security@uzh.ch oder **044 634 3333**

Universität Zürich[UZH]