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

Aktivieren Sie den Sperrbildschirm immer, wenn Sie Ihren Arbeitsplatz verlassen und lassen Sie mobile Geräte nie unbeaufsichtigt.

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

02 Sichere Passwörter wählen

Geben Sie niemals ein Passwort weiter. Verwenden Sie nur starke Passwörter und benutzen Sie für jedes Login ein anderes Passwort. Ein Passwortmanager kann Ihnen bei der Generierung und Verwaltung von Passwörtern helfen. Wenn Sie die Möglichkeit haben, benutzen Sie Zwei-Faktor-Authentifizierung, damit auch im Falle eines Passwort-Leaks Ihre Logins sicher sind.

03 Betriebssystem und Antivirensoftware aktuell halten

Updaten Sie regelmässig das Betriebssystem Ihres Computers und halten Sie Ihre Anti-Virensoftware auf dem neusten Stand. Nur so können Sie aktuelle Sicherheitslücken schliessen und sind vor den neusten Viren geschützt.

04 Erst denken, dann klicken

Bevor Sie auf einen Link klicken oder einen Anhang öffnen, stellen Sie sicher, dass sie aus vertrauenswürdiger Quelle stammen. So laden Sie sich nicht aus Versehen Schadsoftware auf Ihren Rechner.

05 Sichere WLAN-Netze nutzen

Wenn Sie unterwegs sind, vermeiden Sie die Nutzung öffentlicher und ungesicherter WLAN-Netze. Sie können nie wissen, wer noch in diesem Netz unterwegs ist.

06 Geschäftsidentität nicht privat nutzen

Benutzen Sie Ihre UZH-Mailadresse und Ihren UZH-Benutzernamen nicht für private Zwecke wie zum Beispiel für Social Media-Logins. So sind Ihre Arbeitslogin auch bei einem Datenleak sicher.

07 Unbekannte Personen überprüfen

Überprüfen Sie die Identität Ihnen unbekannter Personen, bevor Sie ihnen unternehmensbezogene Informationen aushändigen oder Transaktionen tätigen. Andernfalls könnten wichtige Informationen in die falschen Hände geraten.

08 Sensible Daten korrekt ablegen

Verschlüsseln Sie sensible oder vertrauliche Dokumente oder speichern Sie diese in geschützten Ordnern ab. Physische Dokumente sollten Sie 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

Verwenden Sie ausschliesslich Software, die von der IT vorinstalliert oder im Software Center der UZH zum Download bereitgestellt wurde. Installieren Sie 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

Halten Sie sich an die Regeln und Vorgaben der IT-Security und wenn Sie sich unsicher sind oder Ihnen eine E-Mail verdächtig erscheint, melden Sie sich beim Helpdesk oder der IT-Security. Jeder Hinweis kann nützlich sein.

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

Universität Zürich[UZH]