Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Kontakt: Roland Brunner, Austellungsstrasse 80, 8090 Zürich
roland.brunner@edu.zh.ch

D5.6-12A
Erstellung 08.12.2022
Revision .....

1. Juli 2022

Ein Dutzend Verhaltensregeln, um sich sicher im digitalen Raum zu bewegen - Einhaltung von Datenschutz und Datensicherheit

Das Wichtigste: Ich nutze in jeder Situation *meinen gesunden Menschenverstand*. Ich bin mir auch bewusst, dass nichts gratis ist *(im Internet werden Gratisangebote meist mit «Daten bezahlt»)*.

1. Ich nutze unterschiedliche und starke Passwörter

Für verschiedene Dienste verwende ich unterschiedliche Passwörter. Die Länge der Passwörter ist mindestens 8 Zeichen und besteht aus einer Kombination aus Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen. Längere Passwörter (Bsp. 10 – 12 Zeichen) sind sicherer. Meine Passwörter speichere ich nicht im Browser, idealerweise verwende ich ein Passwortmanager.

Und – logisch – mein Passwort gehört mir allein.

Wenn möglich, nutze ich die Zwei-Faktor-Authentifizierung.

Ein Passwort mit weniger als 8 Zeichen (auch mit Sonderzeichen, Gross- und Kleinschrift) wird von einem Profi in wenigen Minuten gehackt. Jedes Zeichen mehr benötigt exponentiell mehr Aufwand.

2. Ich verwende E-Mail bewusst

Ich schreibe nicht in eine E-Mail, was ich nicht auch auf eine Postkarte schreiben würde. Vertrauliche Informationen versende ich nur mit einer verschlüsselten E-Mail.

E-Mail-Verkehr wird ungesichert übertragen. Der «Postbote» kann jederzeit mitlesen, die Informationen lesen, auswerten, kombinieren und ggf. verkaufen.

3. Ich klicke nicht blindlings auf Links

Ich hinterfrage, bevor ich einen Link in einer E-Mail anklicke, nicht nur von unbekannten Absendern. Auch auf Webseiten bin ich aufmerksam und klicke nicht einfach auf Links, Downloads und «OK».

Schadsoftware wird häufig über E-Mail, unseriöse Webseiten oder Downloads verbreitet.

4. Ich surfe nicht mit Administratorenrechten

Für meine Arbeit verwende ich ein Windowskonto mit normalen Benutzerrechten.

Verschafft sich jemand Zugang zu meinem Benutzer, verfügt er / sie über alle Rechte. Wenn ich mit einem Windowskonto mit Administratorenrechten am Surfen bin, können im Hintergrund ohne mein Wissen Programme installiert oder Code ausgeführt werden. Verwende ich zwei unterschiedliche Konten, muss ich jeweils eine Installation oder Codeausführung bestätigen und sie geschieht nicht ohne mein Wissen.

5. Ich halte meine Programme und mein Betriebssystem aktuell

Ich führe die vom System vorgeschlagenen Updates zeitnah durch. Ich nutze die Auto-Update-Funktion von Windows / Mac / Linux.

Angreifer nutzen gezielt bekannte Schwachstellen aus. Wenn ich die von den Herstellern bereitgestellten Updates rasch installiere, reduziere ich das Risiko massiv.

6. Mein System schütze ich mit einem aktuellen Viren-/Malwarescanner

Ich verwende einen Viren-/Malwareschutz und halte diesen aktuell.

Mit einem Viren-/Malwareschutz können verdächtige Dateien und Mails automatisch

erkannt und isoliert werden. Ein vertrauenswürdiger Virenscanner aktualisiert im Hintergrund automatisch die Virendefinitionen.

7. Wechselmedien schliesse ich nicht ungeprüft an mein System an

Ich verwende nur genehmigte Wechselmedien. Diese versehe ich mit einem Passwortschutz. Ich achte auch auf eine fachgerechte Entsorgung (dies gilt auch für meinen Desktop/Laptop bzw. meine externe Festplatte und mein NAS).

USB-Sticks sind nicht geeignet, um Daten längerfristig und sicher zu speichern. Schon gar nicht wichtige oder sensible Daten (z.B. Maturaarbeit).
Wechselmedien wie USB-Sticks können einfach verloren oder verlegt werden. Deshalb sind die Informationen darauf zu schützen (verschlüsseln).
«Herrenlose» USB-Sticks werden häufig für Malware-Attacken missbraucht.

8. Ich sichere meine Daten

In regelmässigen Abständen sichere ich meine Daten. Idealerweise richte ich ein dafür spezialisiertes Programm ein, welches die Daten automatisch sichert. Die Datensicherung bewahre ich nicht am selben Ort auf wie die Originaldaten.

Daten können durch Malware verschlüsselt und so für mich unbrauchbar gemacht werden. Auch Fehlmanipulationen können zu Datenverlust führen. Eine Datensicherung kann mich hier vor den Folgen retten.

9. Ich sperre meinen Bildschirm, wenn ich nicht davorsitze

Wenn ich vom Bildschirm weggehe, schalte ich die Bildschirmsperre ein (unter Windows mit «Win + L»).

Ein frei zugänglicher Arbeitsplatz ermöglicht es einem «Kollegen», in meinem Namen Dinge auszuführen. Dies kann ein Mailversand oder auch die Ausführung von Programmcode über einen USB-Stick sein.

10. Ich behandle vertrauliche Informationen vertraulich

Ich versende vertrauliche oder geheime Informationen nur verschlüsselt per E-Mail. Ich speichere sie in separaten, nur den berechtigten Personen einsehbaren Verzeichnissen ab.

Vertrauliche Informationen müssen unter Verschluss gehalten werden, ansonsten besteht die Gefahr von Missbrauch. Zudem handelt es sich um eine Datenschutzverletzung.

11. Ich lasse keine Dokumente liegen

Ich räume meinen Arbeitsplatz beim Verlassen immer sauber auf und schliesse sensible Dokumente weg. Dasselbe gilt auch für Klassenräume, Sitzungszimmer, etc.

Personen, die mein Büro / Klassenzimmer betreten können Einsicht in Dokumente erhalten, welche sie nichts angehen.

12. Ich verhalte mich in der Öffentlichkeit bewusst

An öffentlichen Orten wie Restaurants, öffentlicher Verkehr, etc. spreche ich nur indirekt über meine Arbeit, nenne keine Namen und vertraulichen Informationen. Das gilt auch für Telefongespräche (auch im Homeoffice bei offenem Fenster) und meine Äusserungen in sozialen Medien. *Andere Personen können Dinge mithören / -lesen, die sie nichts angehen. Dies kann mich oder andere Personen wie auch meinen Arbeitgeber in Misskredit bringen.*