Sicherheitscheck (siehe auch material.digidaktik.de - Version: 1.2017)

Vorsicht! Jede Veränderung gründlich notieren und vorher (besonders beim „löschen“) jemanden fragen, der sich damit auskennt!

1. WLAN / WiFi kein WEP, WPA,WPS => mind. WPA2, ungewöhnlicher Name, SEHR gutes Passwort (s.u.)

2. Computer

a) neue Programme oder Dateien (Word, Excel, DOCs, PDFs, Bilder, ...) aus dem Internet (z.B. aus e-mails - wenn **nicht private / vertrauliche**!) vor dem Öffnen / Installieren bei https://www.virustotal.com/ überprüfen

b) neue Programme/Software/Apps nur aus vertrauenswürdiger Quelle und wenn unbedingt nötig installieren. Nach dem Herunterladen und vor dem Ausführen eine Woche warten und dann erneut auf Viren scannen. (evtl. freie Alternativen bevorzugen z.B. http://www.documentfoundation.org/ statt Microsoft-Office-Kopie)

c) Makrofunktionen möglichst deaktivieren (und auch auf Aufforderung möglichst nicht aktivieren)

d) OpenSource-Software aus seriöser Quelle nutzen, z.B. statt Adobe-PDF: http://www.pdfreaders.org/

e) überflüssige Software (Zweck überprüfen!) deinstallieren (z.B. Adobe-PDF?, Java? - s.o.!)

f) bereits bei der Installation die Optionen jeder Software überprüfen und evtl. bewusst Haken entfernen (Toolbars? Bing / Google ...? Autostart? Datenschutz? „Testversion“? ...) Anschließend alle Einstellungen überprüfen

g) an einem vertrauenswürdigen Netz (**nicht** an öffentlichen (W)LANs) und über die System-Funktionen: zügig alle Sicherheitsupdates einspielen (besonders von: PDF-Reader, „flash“, Office und System)

h) integrierte Firewall aktivieren und Ausnahmen überprüfen, evtl. Blacklist / Kinderschutz am Router nutzen (z.B. in Windows Verbindungen immer als öffentliches Netzwerk kennzeichnen, Remotezugriff deaktivieren, ...)

i) Internet besser **mit „Click-to-Play“** z.B. mit (aktuellem!) Firefox http://www.mozilla.org/ **und** installiertem, restriktiv aktiviertem **NoScript-AddOn** (https://addons.mozilla.org/de/firefox/addon/noscript/ - Whitelist nur vorsichtig erweitern und nur gezielte Ausnahmen temporär erlauben => sinnvollen Umgang lernen) oder „bequemer“=„unsicherer“: (aktueller!) Chromium mit ClickToPlay und **ohne** Java- und Silverlight-Plugin („chrome://plugins/“) benutzen.

j) „Eingebauten“ Browser (z.B. Internet Explorer) eher einschränken. System-Internet- und Intranet-Optionen möglichst restriktiv (auf höchste Stufe) einstellen.

k) „Verschlüsselt“ surfen (z.B. StartTLS, SSL „https:“, VPN)?, Datenschutz? (Cookies? Like-Buttons? ...)

l) hosts-Datei / DNS-Einstellungen überprüfen + Zugriff durch fremde Personen erschweren

m) Online-Banking besser nur gezielt über Live-Linux-CD/DVDs (neu gestartet und gleich beendet), das Gleiche gilt für „wildes“ bzw. „neugieriges“ bzw. „gefährliches“ „surfen“: besser über spezielle Surf-CDs, („Tor“: erhöhte Gefahr)

n) Win: Virenschutz mit Verhaltenserkennung (eher ohne weitere Firewall) regelmäßig auf seine Funktion überprüfen

o) (...und Unterschied zwischen Systembenachrichtigungen und internen Texten bzw. Programmfenstern beachten; verschiedene e-mail-Adressen und gute/verschiedene Passwörter (ohne Umlaute/Sonderzeichen) nutzen, die in keiner Form im Netz o.Ä. vorkommen z.B. (ehemals ;-) AdL5adM9snkW - evtl. auf Zettel schreiben; und grundsätzlich möglichst wenige und/oder stimmige falsche Daten angeben.)

p) Möglichst keine online Benutzerkonten anlegen bzw. falls nicht unbedingt benötigt löschen, auf Anonymisierung bzw. Datensparsamkeit achten, Einstellungen bzgl. „privacy“, Datenschutz und evtl. Datensammlung für Konten / Accounts und diverse Systeme (Windows, Android, iOS) und Apps und Web-Services (Google, facebook …) überprüfen und einschränken, online vorliegende nicht unbedingt nötige Daten und ältere „Posts“, Mitteilungen, Bilder, … löschen (vorab lokales Backup?). Lokale Backups statt Cloud bevorzugen, evtl. automatische Synchronisierungen deaktivieren. Verschlüsselung bevorzugen.
Am Beispiel von Windows: http://www.spiegel.de/netzwelt/web/windows-10-so-bekommen-sie-mehr-privatsphaere-a-1138075.html

3. Handy / Smartphone

siehe: http://www.digidaktik.de/research/IT-Sicherheit/Smartphone-Checkliste.pdf

Siehe auch:

http://www.digidaktik.de/research/IT-Sicherheit/

http://www.digidaktik.de/medien-links.shtml

https://twitter.com/digidaktik