Arbeitszeit: 10 Minuten

Seitenrand links 2,5 cm, Seitenrand rechts 2,5 cm

**Internet - Handy - Smartphone**

**Achte unbedingt auf die Sicherheit!**

Wie du deinen PC richtig schützt, dafür gibt es viele Tipps im Netz. Aber wie sieht das mit deinem *Smartphone* aus? Das Smartphone hat ähnliche Funktionen wie ein PC und sollte daher auch von dir geschützt werden. Alle Sicherheitstipps für PCs und die Nutzung von drahtlosen Verbindungen (WLAN) gelten grundsätzlich auch für Smartphones. Darüber hinaus können dir Apps helfen, dein Smartphone sicherer zu machen. Da gibt es z. B. Apps, die vor Viren und Trojanern schützen. Oder Apps, die dabei helfen, andere Apps zu kontrollieren und deren Aktivitäten und Rechte bei Bedarf einzuschränken. Denn nicht jede App benötigt für ihre Funktionalität zwangsläufig Informationen über deinen Standort oder Zugriff auf dein Telefonbuch. Auf den folgenden Seiten kannst du dich informieren, wie du deinen PC und dein Smartphone am besten schützen kannst.

Ausspähen - Verändern von Daten

Beim Surfen im Internet besteht die Gefahr, dass Kriminelle versuchen, Daten auszuspähen, denn Smartphones, Tablets, Notebooks etc. sind auf verschiedene Arten angreifbar.

Zum Beispiel können **Hacker** versuchen, über dein WLAN Zugriff auf deinen PC zu bekommen oder deine Passwörter auszuspionieren. Mit ein paar einfachen WLAN-Einstellungen und sicheren Passwörtern kannst du das verhindern. Darüber hinaus gibt es im Internet viele manipulierte Internetseiten sowie manipulierte E-Mails. Über die manipulierten Links soll man auf scheinbar echte Seiten geführt werden. Auf diese „Fake-Seiten“ wollen Kriminelle dich dazu bringen, vertrauliche Daten einzugeben. Diese Daten fangen sie dann ab und kaufen online ein oder tätigen illegal Bankgeschäfte in deinem Namen.

*Ausspähen und Abfangen von Daten*

Wenn ein Computer gehackt wurde, indem beispielsweise ein **Trojaner** darauf installiert wurde, haben Kriminelle Zugriff auf die persönlichen Daten des Besitzers, wie z. B. Passwörter, und können diese missbrauchen. Man spricht in diesem Zusammenhang juristisch vom „Ausspähen von Daten“ bzw. vom „Abfangen von Daten“. Gemäß der §§ 202a und 202b des Strafgesetzbuches ist das strafbar.

Schütze dich vor aktuellen Phishing-Maschen

Betrüger nutzen das Informationsbedürfnis der Bevölkerung in der aktuellen Lage aus, um über Phishing an sensible Daten zu kommen. Dabei tarnen sich die Kriminellen als offizielle Stellen.

Die Polizei rät: Sei vorsichtig beim Öffnen von E-Mail-Anhängen!

Potentielle schädliche Anhänge in den Formaten .docx oder .exe werden zurzeit vermehrt in gefälschten E-Mails scheinbar im Namen von Gesundheitsämtern, der Weltgesundheitsorganisation sowie anderen Behörden, Institutionen und Firmen, verschickt. Wenn du diese öffnest, installiert sich eine *Spyware* oder der Computer wird komplett verschlüsselt.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI), kursiert momentan zudem eine sogenannte „Corona-Karte“, die angeblich in Echtzeit angeben soll, wo Coronainfektionen registriert worden sind. Diese „Corona-Karte“ wird von Kriminellen als Lockmittel genutzt. Öffnest du diese Karte, lädt sich im Hintergrund eine *Schadsoftware*, die Passwörter und Zugangsdaten am PC ausliest.

Drei Tipps der Polizei gegen die neuen Maschen beim Phishing:

* Öffne **keine** Dateien, Anhänge oder Links von unbekannten Adressaten. Sei auch misstrauisch, wenn es sich um Anhänge in E-Mails von scheinbar offiziellen Stellen handelt.
* Folge den Aufforderungen in E-Mails, Programme herunterzuladen, nur dann, wenn du die entsprechende Datei auch auf der Internet-Seite des Unternehmens findest. (Starte keinen Download über den direkten Link.)
* Gehe **nicht** auf mögliche Geldforderungen ein, wenn dein PC gesperrt wird.

Wenn du deine Daten eingegeben hast: Die Checkliste von Polizei und BSI vermittelt wichtige Empfehlungen für den Ernstfall.

Onlinespielen kann teuer werden!

Wusstest du, dass vermeintlich kostenlose Spiele-Apps auch zur Kostenfalle werden können, wenn so genannte *In-App-Käufe* für zusätzliche Funktionen nicht deaktiviert sind?

Darauf solltest du als Gamer oder älterer Bruder oder Schwester achten!

Bei einem In-App-Kauf, z. B. bei kostenlosen Spiele-Apps, können **bestimmte Funktionen nur gegen Geld** erworben werden. Bei einigen Spiele-Apps kann das Spiel nur gegen eine Zahlung fortgesetzt werden. So kommst du in eine Kostenfalle, denn die **Zusatzkosten** für ein „neues Leben“ oder eine „Wunderwaffe“ werden **oft nicht klar gekennzeichnet**. Darum sei vorsichtig oder frage deinen älteren Bruder oder deine Schwester, dass sie noch mal genauer auf Sicherheit und Kosten bei deinem Spiel schauen.

Altersfreigabe von Spiele-Apps

Sei ehrlich, hast auch du schon Spiele-Apps genutzt, für die du eigentlich noch zu jung bist? Nur, damit du mit deinen Freunden mithalten kannst? Die **Altersbeschränkung** ist aber wichtig, denn es kommt vor, dass Spiele-Apps, die zunächst keiner Altersbeschränkung unterlagen, im Nachhinein eine Ein­stufung erhalten, weil sie für Kinder **ungeeignet** sind. Deswe­gen solltest du dich mit deinen **Eltern** zusammensetzen und festlegen, welche Spiele für dich geeignet sind und für wel­ches Alter sie freigegeben sind.

So vermeidest du einen In-App-Kauf

Aktiviere die Drittanbieter-Sperre für dein Smartphone. Dies kannst du oder jemand aus deiner Familie über den Netzbetreiber einrichten lassen.

Ändere die Einstelllungen im Betriebssystem. Unter Einstellungen kann man je nach Betriebssystem In-App-Käufe deaktivieren oder ein Passwort zur Beschränkung von Käufen einrichten.

Achte auch grundsätzlich auf die Alterskennzeichnung von Spiele-Apps: Lass jemanden aus deiner Familie unter www.usk.de prüfen, ob das gewünschte Spiel für deine Gruppe freigegeben ist.

Soziale Netzwerke

Weit **mehr** **als die Hälfte** der Kinder und Jugendlichen ist in einem Sozialen Netzwerk angemeldet und nutzt es mehrmals in der Woche. In den Netzwerken werden Fotos und Videos ausgetauscht, man unterhält sich mit anderen und verabredet sich. Um ein Soziales Netzwerk nutzen zu können, muss jeder zunächst ein eigenes Profil von sich erstellen. Das *persönliche* Profil beinhaltet dabei oft viele ganz private Angaben wie zum Beispiel das Alter und den Wohnort sowie Interessen und Fotos. Je nach Einstellung des Profils sind diese Informationen für viele andere Nutzer sichtbar - auch für deine Lehrer oder einen zukünftigen Arbeitgeber. Daher ist die Nutzung der Privacy-Option wichtig. Nicht alles, was man in Sozialen Netzwerken machen kann, darf man auch. So darfst du die Persönlichkeitsrechte von anderen nicht verletzen oder gegen das Urheberrecht verstoßen.

*Mögliche Straftaten*

In Sozialen Netzwerken treten viele Menschen, die sich zum Teil vielleicht nicht einmal kennen, miteinander in Kontakt und man bekommt viele Informationen von anderen Personen, im besten Fall nur von Freunden. Das kann Spaß machen, aber es birgt auch gewisse Gefahren. In Sozialen Netzwerken können, wie im richtigen Leben auch, Straftaten begangen werden. Häufige Rechtsverletzungen sind Verstöße gegen das **Recht am eigenen Bild** und das **Urheberrecht**. Aber auch Cybergrooming und Cybermobbing beinhalten Straftaten, die in Sozialen Netzwerken immer wieder auftreten.

Recht am eigenen Bild

Fast jeder Jugendliche kennt die Situation: Mit ein paar Freunden ist man in der Disko oder auf einer privaten Party gewesen, hatte Spaß und hat sich dabei gegenseitig fotografiert. Soweit ist das ok. Doch es ist ja nur halb so lustig, wenn man diese Fotos nicht auch ins Internet hochlädt. Aber damit kann der Ärger schnell anfangen. Denn wer die Fotos der Freunde - ohne dass sie damit einverstanden sind - ins Internet hochlädt, macht sich strafbar. Vorher sollte man also checken, ob alle damit einverstanden sind, dass die Fotos veröffentlicht werden. Denn einmal ins Internet hochgeladen, sind die Fotos nicht mehr so einfach zu löschen.

*Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen*

Nicht jede Situation darf fotografiert, nicht jedes Foto veröffentlicht werden. Das Gesetz verbietet es, von Personen dort **unbefugt** Fotos zu machen, wo jemand ganz privat ist, nämlich in seinem „höchstpersönlichen Lebensbereich“, wie z. B. in seiner Wohnung. Ebenfalls nicht fotografiert oder gefilmt werden darf an Orten wie Toiletten oder Umkleideräumen. Diese Orte sind **bewusst** vor den Blicken vieler Leute geschützt, sind privat und sollen das auch bleiben. Weiterhin kommt hinzu, dass Personen nicht in peinlichen oder hilflosen Situationen fotografiert oder gefilmt werden dürfen. Um Menschen vor solchen Aufnahmen und möglichen Veröffentlichungen zu schützen, gibt es den § 201a Strafgesetzbuch (StGB). **Er stellt das unbefugte Gebrauchen, Herstellen, Übertragen oder Weitergeben** solcher Aufnahmen unter Strafe. Grundsätzlich muss der oder die Fotografierte immer mit der Aufnahme einverstanden sein!