Schule Online –
Lernen in der Digitalen Welt

Tipps zur sichereren Nutzung des Internets

Ob mit dem Smartphone, dem Tablet oder dem Computer – täglich surfen Kinder und Jugendliche wie du durch das Internet. Dabei nutzt du es wahrscheinlich sowohl in der Schule als auch privat: Du kommunizierst mit Freunden online über Messenger, informierst dich auf sozialen Netzwerken, schaust Videos und Tutorials und suchst Informationen, um die Hausaufgaben zu erledigen. Vielleicht spielst du auch online, um etwas Spaß zu haben? Dass das Internet neben den ganzen positiven Aspekten auch viele Gefahren birgt, weißt du bestimmt schon.

Private Daten, wie Adressen und Fotos werden geteilt, Passwörter geknackt, Viren landen auf dem PC. Ob aus Unwissenheit oder Unachtsamkeit – du kannst sicherlich nicht alle diese Gefahren vermeiden, aber du kannst dich davor schützen.

Hier findest du 10 Tipps um das Risiko, Opfer von Internetkriminalität zu werden, zu verringern:

- Tipp 1: Erstelle sichere Kennwörter
- Tipp 2: Nutze aktuelle Virenscanner & Firewall
- Tipp 3: Ignoriere verdächtige E-Mail-Anhänge
- Tipp 4: Nutze Downloads aus sicheren Quellen
- Tipp 5: Verwende unterschiedliche Benutzerkonten
- Tipp 6: Erstelle regelmäßige Sicherungen durch Backups
- Tipp 7: Benutze die Sicherheitsfunktionen des Browsers
- Tipp 8: Surfe in sicherem WLAN
- Tipp 9: Bestimme die Einstellungen der Cookies
- Tipp 10: Sichere Daten mithilfe von Updates

Schule Online –
Lernen in der Digitalen Welt

Tipp 1: Erstelle sichere Kennwörter

Für jedes Benutzerkonto, ganz gleich ob in einer App oder online, solltest du **ein eigenes** Kennwort nutzen! Dieses Kennwort sollte

- aus mindestens 10 Zeichen,
- sowie aus Groß- und Kleinbuchstaben,
- als auch aus Zahlen und Sonderzeichen bestehen.

Einfache Wörter, die in Wörterbüchern stehen und leicht mit dir in Verbindung gebracht werden können oder Zahlenfolgen (eigenes Geburtsdatum, Postleitzahl, etc.), solltest du **nicht** verwenden.

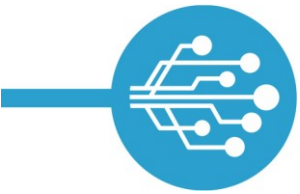
Beachte, dass ein neues Passwort, das du vergeben sollst, nicht wie das alte Passwort lauten darf. Eine Idee wäre, von einem Satz immer nur die Anfangsbuchstaben zu nehmen: Ich denke oft an meine 2 Lieblingstiere, die Katzen Max und Paule. Das Kennwort wäre dann: Idoam2L,dKMuP

Da du dir wahrscheinlich mehrere Passwörter gleichzeitig merken musst, ist es eine gute Idee, einen so genannten Password-Manager zu verwenden. Dieses Programm speichert Anmeldedaten verschlüsselt entweder in einer App, einer Cloud oder auf einem Speichermedium, wie beispielsweise einem USB-Stick. Statt vieler unterschiedlicher Kennwörter musst du dir dann nur noch ein Master-Password merken. Dieses Kennwort sollte dann natürlich besonders „kompliziert" sein, so dass niemand es erraten kann, allerdings so „logisch" für dich, damit du es gut behalten kannst. Weitere Informationen und Tipps zur Erstellung sicherer Kennwörter findest du hier.

Tipp 2: Nutze aktuelle Virenscanner & Firewall

Virenscanner sind Programme, die dein Gerät vor Schadsoftware schützen. Sie erkennen, blockieren und beseitigen viele Gefahren automatisch. In den gängigen Betriebssystemen sind Virenscanner bereits enthalten. Da diese nur bereits bekannte Schadsoftware bekämpfen können, ist es wichtig, sie immer auf dem neuesten Stand zu halten, da sie sonst die „neuen Viren" nicht als solche erkennen. Die Option „automatische Updates" solltest du daher unbedingt aktivieren.

Firewalls sind in den gängigen Betriebssystemen ebenfalls integriert. Sie sollten auf jeden Fall aktiviert sein, damit der Rechner auch gegen unerwünschte Netzwerkzugriffe geschützt wird.



Schule Online – Lernen in der Digitalen Welt

Tipp 3: Ignoriere verdächtige E-Mail-Anhänge

Unerwünschte und massenhaft versendete E-Mails werden als **Spam- oder Junk-Mails** bezeichnet. Auch wenn die Spamfilter einen Großteil dieser lästigen Mails blockieren, klappt das nicht immer vollständig. Du kannst unerwünschte E-Mails als Spam markieren und so mithelfen, die Spamfilter zu verbessern.

Phishing-E-Mails sind E-Mails, die versuchen an deine persönlichen Daten, z. B. Kennwörter zu gelangen. Dafür versenden Kriminelle E-Mails, die vorgeben von einem bekannten und vertrauenswürdigen Unternehmen zu stammen. Häufig enthalten diese E-Mails aber gefährliche Links, Dateianhänge oder die Aufforderung, deine persönlichen Daten einzugeben. Phishing-Mails solltest du immer sofort löschen, damit du sie nicht versehentlich doch noch öffnest. Als allgemeine Regel gilt: Unternehmen werden **niemals** Nutzerdaten per Mail von dir verlangen! Im Zweifel solltest du über einen anderen Kommunikationsweg (z. B. Anruf) mit dem angeblichen Absender Kontakt aufnehmen.

Besondere Vorsicht ist bei **Mail-Anhängen** geboten. Wenn du den Absender nicht kennst bzw. von einem bekannten Absender keine Mail mit Anhang erwartest, solltest du keinerlei Anhänge öffnen. Auch hier kannst du im Zweifel beim Absender noch mal persönlich nachfragen.

Tipp 4: Nutze Downloads aus sicheren Quellen

Ob kostenlos oder nicht - Downloads werden im Internet überall angeboten. Beim Download kannst du jedoch auch zusätzliche, eventuell gefährliche Programme mit herunterladen, ohne dass du es selbst merkst und ohne, dass das Virenschutzprogramme dies anzeigt. Kostenfreie Software, sogenannte Freeware, solltest du daher immer direkt beim Hersteller selbst herunterladen.

Tipp 5: Verwende unterschiedliche Benutzerkonten

Wenn verschiedene Personen an einem Computer arbeiten, ist das Einrichten von unterschiedlichen Benutzerkonten sinnvoll. Du kannst dein Benutzerkonto dann nicht nur deinen persönlichen Vorlieben entsprechend anpassen, sondern auch sicher verwalten. Dateien, die du abgelegt hast, liegen dann in einem Verzeichnis, auf das niemand außer dir Zugriff hat. Oft können so in Schulen mehrere Schülerinnen und Schüler an einem Computer arbeiten. Deine Zugangsdaten solltest du auch hier niemals weitergeben.

Schule Online –
Lernen in der Digitalen Welt

Tipp 6: Erstelle regelmäßige Sicherung durch Backups

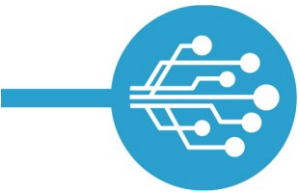
Vielleicht hast du schon von Mitschülerinnen oder Mitschülern gehört, dass sie selbst auf ihre eigenen Dateien nicht mehr zugreifen konnten. Dies kann an einer kaputten Festplatte oder auch an einem Angriff mit Schadsoftware liegen. So oder so, seine eigenen Dateien komplett zu verlieren, ist mehr als ärgerlich und das Wiederherstellen nahezu unmöglich.
Daher solltest du in regelmäßigen Abständen eine Sicherungskopie (engl. Backup) aller relevanten Daten auf einem externen Speichermedium oder in einer Cloud anfertigen. Da das allerdings sehr lange dauern würde, gibt es eine einfache Lösung: Backup-Software. Diese Software vergleicht die ursprüngliche Datenquelle mit der Sicherungskopie und ergänzt nur die Änderungen. Sowohl die Quelldaten als auch die Backups sollten immer verschlüsselt werden, damit Fremde keinen Zugriff auf deine Dateien haben. Verschlüsselungsprogramme sind in den gängigen Betriebssystemen bereits integriert, müssen aber aktiv eingerichtet werden. Selbstverständlich solltest du auch hier sichere Kennwörter wählen.

Tipp 7: Benutze die Sicherheitsfunktionen des Browsers

Lesezeichen: Gehst du häufig auf die gleichen Internetseiten wie beispielsweise LOGINEO NRW oder ein soziales Netzwerk, so ist es sinnvoll, Lesezeichen im Browser zu setzen. Das ist nicht nur bequem, sondern minimiert auch das Risiko, dass du beispielsweise durch Buchstabendreher oder betrügerische Links auf Internetseiten mit Schadsoftware weitergeleitet wirst.

Passwortmanager: Die meisten Browser bieten die Funktion an, deine Zugangsdaten auf Webseiten zu speichern und beim Einloggen automatisch einzutragen. Diese Funktion hat Vor- und Nachteile: Einerseits musst du die Kennwörter nicht ständig neu eingeben und sparst somit Zeit, andererseits stehen die gespeicherten Passwörter auch den anderen Personen zur Verfügung, die an dem PC den gleichen Browser nutzen. Besser ist es, einen separaten Password-Manager (siehe Tipp 1 Kennwörter) zu verwenden, der als App oder verschlüsselte Datei in der Cloud oder auf einem (mobilen) Speichermedium zur Verfügung steht.

Internet-Verbindungen: Grundsätzlich solltest du sparsam mit der Übermittlung eigener Daten im Internet sein. Überprüfe ob die Seiten, auf denen du deine persönlichen Daten eingeben musst, deine Daten verschlüsselt übertragen. Nutzt du eine gesicherte Internetverbindung, findest du das Präfix **https://** als auch das geschlossene Vorhängeschloss in der Browseradresszeile.



Schule Online –
Lernen in der Digitalen Welt

Überprüfen der Link-URL: Bevor du einem zugesandten Link folgst, kannst du den hinterlegten Linktext überprüfen. Bewege dafür die Maus bzw. den Cursor über das als Link gekennzeichnete Wort. Fallen dir dabei verdächtige Begriffe auf, die mit der Seite bzw. dem Link rein gar nichts zu tun haben, solltest du den Link besser nicht anklicken.

Tipp 8: Surfe in sicherem WLAN

Daheim bewegst du dich sicherlich im sicheren WLAN. Wenn du aber unterwegs surfen willst, ist das heutzutage an vielen Stellen durch sogenannte öffentliche Hotspots möglich. Auch wenn der Betreiber eine verschlüsselte Verbindung anbietet (siehe Tipp 6 Browser) ist es möglich, dass Personen auf die Daten deines Endgeräts zugreifen und Passwörter abfangen. Um dich möglichst gut zu schützen, solltest du die Dateifreigabe in den Systemeinstellungen vorab deaktivieren und nach dem Surfen in den Datenschutzeinstellungen des verwendeten Browsers die gesamte Chronik löschen.

Tipp 9: Bestimme die Einstellungen von Cookies

Wenn du online surfst und Internetseiten aufrufst, werden auf deinem Endgerät Cookies erstellt. Das sind kleine Textdateien, die auf deinem Rechner gespeichert werden. Teilweise sind sie notwendig, damit die Seite funktioniert, teilweise werden darüber aber auch Daten gesammelt, die dich identifizierbar machen und beispielsweise für Werbezwecke verwendet werden können. Besuchst du eine Seite, wirst du aufgefordert, die Cookie-Einstellungen anzunehmen. Hier solltest du alle nicht notwendigen Cookies ablehnen.
Auch Drittanbietercookies, das heißt Cookies, die von einer anderen Website angelegt werden als von der, die du gerade besuchst, sollten in den Browsereinstellungen grundsätzlich immer abgelehnt werden. Werden Cookies automatisch beim Schließen des Browsers gelöscht, gibst du weniger Daten preis, musst aber ggf. bei einem späteren Besuch von Webseiten die Eingaben deiner Daten wiederholen.

Tipp 10: Sichere Daten mithilfe von Updates

Die Hersteller von Computer-Software schließen bekannt gewordene Sicherheitslücken in ihren Produkten. Daher ist es wichtig, die Software durch die Aktivierung automatischer Updates auf dem aktuellen Stand zu halten. Je nach Einstellungen der Software wirst du über Updates regelmäßig informiert und solltest sie sobald wie möglich durchführen.

Schule Online –
Lernen in der Digitalen Welt

Glossar

- Backup: Sicherungskopie von persönlichen Daten
- Browser: Programm bzw. App, mit der Internetseiten angezeigt werden können.
- Cookie: Textdatei, die während des Besuchs einer Webseite auf einem Computer platziert wird und verschiedene Informationen sammelt. Firewall: ein Teil des Sicherungssystems des Computers, das ihn vor Angriffen zumeist aus dem Internet schützt.
- Phishing-E-Mail: Kunstwort aus *Passwort* und *fishing*. E-Mails, die Anhänge oder Links enthalten und versuchen, sensible Daten abzugreifen.
- Schadware: jegliche Form von Software, deren Ziel es ist, dem Computer zu schaden oder an private Daten zu gelangen (Virus / Trojaner / Spähprogramme)
- Software: Oberbegriff für alle Programme wie dem Betriebssystem, Virenschutzprogramm oder auch dem Internetbrowser.
- Spam- / Junk-E-Mail: Bezeichnung für unerwünschte und massenhaft zugestellte E-Mails, die meistens Werbung enthalten.
- Virenscanner: Programm, das den Computer auf Schadsoftware durchsucht, um ihn zu schützen.
- Virus: eine Form von Schadsoftware.
- WLAN / Wi-Fi: englische Abkürzung, bedeutet auf Deutsch Lokales Drahtlosnetzwerk

Herausgeber: Medienberatung NRW