Name: …….. **Klasse: ….** **Datum: ……**

Gefahr	Gegenmaßnahmen
Viren Kleine Programme, die sich an Dateien anhängen. Immer wenn dieses Programm aufgerufen wird, kopiert sich das Virusprogramm weiter. Die Viren können Daten zerstören und z. B. die Festplatte löschen. **Trojaner** Sie tarnen sich als scheinbar praktische Programme, beinhalten aber Schadprogramme, z. B. Viren.	▪ Verwende nie geliehene, getauschte, von irgendjemandem „geschenkte“ Raubkopien! ▪ Fertige Sicherungskopien von deinen Originalen (Programme und Dateien) an und besorge dir zusätzlich eine externe Festplatte! ▪ Installiere ein Anti-Viren-Programm, das die Speicher nach Viren untersucht, dich auf Viren aufmerksam macht und sie beseitigt! ▪ Firewall und Virenscanner regelmäßig updaten! ▪ Öffne keine unbekannten Links und Emails!
Würmer Programme, die sich selbstständig über Netzwerke verbreiten und in ungeschützte Rechner eindringen. Sie können Einstellungen am Betriebssystem oder an der Software ändern und den Zugang für Dialer, Hackerprogramme usw. ermöglichen.	▪ Verwende zwei Rechner, von welchen nur einer Internetanschluss hat!
Dialer Dialer bewirken, dass sich der Computer unbemerkt über sehr teure 0190er- oder 0900er-Nummern ins Internet einwählt (nur bei Modem oder ISDN-Karte).	▪ Sperre bestimmte Vorwahlen (in Haustelefonanlage oder bei Telefondienstleister)! ▪ Installiere keine Programme, die aus unsicheren Quellen stammen! ▪ Breche einen automatisch gestarteten Download sofort ab! ▪ Richte keinen automatischen Internet-Zugang ein! ▪ Speichere dein Zugangspasswort nicht ab! ▪ Installiere ein Dialer-Schutzprogramm! ▪ Vermeide zur Vergabe eines Passwortes die Eingabe persönlicher Daten!

Spyware – Phising Passwort-Fishing Programme, die Daten eines Computers ausspionieren (z. B. Zugangsdaten) und Informationen unbemerkt an Dritte versenden, z. B. Passwörter.	▪ Öffne keine Anlagen oder Mails mit verdächtigem Betreff! ▪ Installiere eine Anti-Spyware-Software!
Spam und Popups Bombardement mit Werbung und weiteren unerwünschten Mails	▪ Klicke nicht auf Links in Werbe-Mails oder auf den beworbenen Web-Seiten! ▪ Aktiviere einen Spam-Schutz beim Provider (Spam-Blocker)! ▪ Leite keine Kettenbriefe weiter! ▪ Deaktiviere die Antwortfunktion des Mailprogrammes! ▪ Öffne Dateianhänge nur bei bekanntem Absender! ▪ Öffne keine E-Mails mit unbekanntem Absender! ▪ Verwende zwei Mailadressen (für Freunde und für Gästebücher, Chat usw.)
Hacker Zugriff und Manipulation der Daten auf deinem PC	▪ Sicher deinen WLAN-Anschluss! ▪ Hybride Kriegsführung; Organisationen, die es nicht gut mit uns meinen, greifen Firmennetzwerke oder unsere empfindliche Infrastruktur an und versuchen den Wahlkampf in demokratischen Ländern mit Fehlinformationen zu unterwandern ▪ Durch Anrufe mit Schocknachrichten bei dir zuhause versuchen angebliche Mitarbeiter einer Firma (z. B. Telekom, Microsoft, Polizei, Staatsanwalt, …) Zugang zu deinem PC zu bekommen, um z. B. Gelder von deinem Konto abzubuchen. Es können am Telefon auch gefakte Stimmen von dir bekannten Personen verwendet werden!
Hoaxes „Scherzhafte“ Falschmeldungen, die irrtümlich für wahr gehalten und an viele Personen weitergeleitet werden.	▪ Verwende immer verschiedene Informationsquellen! ▪ Gib trotz Aufforderung keine persönlichen Daten an (z. B. Bankdaten)!
Gefälschte E-Mails, Webseiten und Bildbearbeitung, Falschmeldungen und Fake-News	▪ Erkenne gefälschte Emails (fehlerhafte Rechtschreibung)! ▪ Schalte deinen gesunden Menschenverstand ein! ▪ Auch internationale und nationale Politiker verbreiten Falschmeldungen – informiere dich immer bei verschiedenen Quellen, um nicht in einer falschen „Informationsblase“ zu landen! ▪ KI kann als Brandbeschleuniger für Falschmeldungen wirken – jede(s) Bild, Video, Geschichte, … kann gefakt sein!

Verschwörungstheorien und Sekten	▪ Glaube nicht alles, was im Internet steht und sei misstrauisch!
Chat Chatten ist, wenn jemand einem anderen per einem Online-Chat eine Nachricht schreibt und diese in wenigen Minuten beantwortet wird.	▪ Gib keine persönlichen Daten von dir preis! ▪ Verwende „Spitznamen“, die man nicht zuordnen kann! ▪ Verwende keine Namen, die Verlockungen vortäuschen können („Sexy Hexy“)! ▪ Chatte nur mit wirklichen Bekannten und lass Unbekanntes unbeantwortet! ▪ Traue niemandem, den du nicht persönlich kennst (auch Fotos sind kein Beweis)! ▪ Triff dich nie mit Chatpartnern! ▪ Fertige einen „Screenshot-Beweisausdruck“ (Alt + Druck) mit Datum und Uhrzeit von einem negativen Chatverlauf an! ▪ Melde Auffälligkeiten bei deinen Eltern, beim Chatbetreiber und bei der Polizei! ▪ Achtung: auch Chatforen diverser Spiele werden von „vermeintlich Gleichaltrigen“ genutzt, um an Kinder- und Jugendliche heranzukommen!
Tauschbörsen (Filesharing) Es werden viele legale und illegale Daten angeboten **Kostenfallen** **Betrug in Handelsbörsen**	▪ Verletze nicht das Urheberrecht! ▪ Gegen eine kleine Gebühr können legale Daten erworben werden – nichts ist umsonst und niemand hat etwas zu verschenken! ▪ Richte sichere Passwörter ein! ▪ Prüfe die Seriösität eines Anbieters! ▪ Beachte die Versand- und Lieferbedingungen! ▪ Wähle sichere Zahlungsmethoden!
Bluetooth ist eine drahtlose Funkverbindung, über die sowohl mobile Kleingeräte wie Mobiltelefone als auch Computer und Peripheriegeräte miteinander kommunizieren können.	▪ Verwende Bluetooth nicht dazu, Musik und Videos aller Art illegal von Handy zu Handy weiterzugeben!
Soziale Netzwerke **Kommunikationsplattformen**	▪ Nur deine Freunde sollen Zugang zu deinem Profil haben (Persönlichkeitseinstellungen)! ▪ Keine Partybilder veröffentlichen – das Netz vergisst nie (Bewerbung)! ▪ Gib nie deine vollständige Adresse an! ▪ Poste nie deinen aktuellen Aufenthaltsort (Einbruchgefahr)!

Cybermobbing **Cyberbullying** **Beleidigung** **Bedrohung**	▪ Die Weitergabe von pornografischen und Gewalt verherrlichenden Darstellungen über Handys sind keine „visualisierte“ Mutprobe, sondern Jugendliche können hierbei Straftaten mit beträchtlichen strafrechtlichen Folgen begehen. ▪ Wer Körperverletzung, sexuelle Nötigung oder andere Straftaten mit dem Handy filmt, kann wegen unterlassener Hilfeleistung belangt werden. ▪ Fertige einen „Screenshot-Beweisausdruck“ (Alt + Druck) mit Datum und Uhrzeit von einem negativen Chatverlauf an! Prävention: ▪ „Zeit für uns“ (regelmäßige Klassenkonferenzen zu Problemen aller Art) ▪ Projekte (Externe Experten, Film „BenX“, …)
Verletzung der Menschenwürde	Lass deine Finger von Webseiten, die sich mit folgenden Themen beschäftigen: ▪ Pornografie (Kinder- und Tierpornografie) ▪ „Snuff“-Videos (z. B. Hinrichtungen) ▪ „Tasteless“ (Bilder von Unfallopfern) ▪ „Happy Slapping“ (Fröhliches Schlagen) ▪ Darstellung von Kriegsopfern ▪ Links- und rechtsextremistische Seiten von Neonazis (Gegen Minderheiten, z. B. Sinti; Verherrlichung des Naziregimes; Leugnen des Holocaust; …) ▪ Suizid- und Magersucht-Foren (suche dringend reale ärztliche Hilfe!) ▪ Kannibalismus, Bombenbau, Terrorismus und Gewaltdarstellungen
Suchtgefahr durch Computerspiele, Internet- und Handynutzung	▪ Verwende den Computer als gezieltes Werkzeug und nicht zum Zeitvertreib – das Leben hat Dir z. B. im Musik- oder Sportverein viel mehr zu bieten! ▪ Teile dir klare Zeiten ein, in welchen du den Rechner nutzt! ▪ Beachte die Güteprüfung und die altersgerechte Zulassung von Computerspielen! **Unsere drei Lieblingstipps zur maßvollen Handynutzung zuhause:** 1. Geräte während des gemeinsamen Essens nicht auf dem Tisch lassen! 2. Geräte nachts nicht im Kinder- bzw. Jugendzimmer belassen, sondern z. B. in der Küche lagern! 3. Vorbildfunktion der Eltern beachten!