10 Tipps zum Schutz gegen Angriffe aus dem Internet und Schad-Software:

(diese Möglichkeiten sind natürlich keine Garantie zum Schutz vor Gefahren im oder aus dem Internet)

1. Windows aktuell halten
   Sicherheitslücken im System sind eine willkommene Zugriffschance für Hacker.
   Durch Einschalten der automatischen Updates in der Systemsteuerung bleibt Windows auf dem aktuellen Stand.

2. Aktualisierung der Software
   Wie Windows kann auch andere Software Sicherheitslücken haben, die gegen Angriffe aus dem Internet nicht gefeit sind. Installieren Sie nur das Nötigste und halten Sie es aktuell. Zum Notwendigsten gehört auch eine Antiviren-Software, die **täglich** aktualisiert wird.

3. Nicht ins Internet mit Administrator-Rechten
   Dieser Benutzer (Administrator) hat Vollzugriff auf das System und somit auch Schädlinge, die man sich einfängt. Im Internet genügt oft ein falscher Klick oder der Besuch einer gehackten oder einschlägigen Internet-Seite. Mit einem eingeschränkten Benutzerkonto (als Hauptbenutzer, noch besser nur als Benutzer) haben auch Schädlinge weniger Chancen. Bei lokalen Arbeiten als Administrator sollte die Internetverbindung getrennt sein.

4. Nur vertrauenswürdige Mails öffnen
   Mails mit HTML-Inhalten oder Mailanhänge können Schädlinge bzw. Schadcode enthalten (Malware). Öffnen Sie nur Mails mit sicherem Inhalt / sicherer Quelle. Zusätzlich sollte der Anhang mittels einer Antivirensoftware gescannt werden.

5. Sichere Software downloaden
   Nicht alles, was im Internet feilgeboten wird (kostenpflichtige Software wie auch Freeware nicht !), hält das, was es verspricht. Absichtlich manipulierte oder mit Programmierfehlern behaftete Software machen das System unsicher und können bereits Schädlinge enthalten. Installieren Sie nur sichere (und durch Virenscanner geprüfte) Software, die Sie wirklich brauchen.

6. DNS-Einstellungen optimieren
   Ungeschützte oder nur mit einem Standardpasswort versehene DSL-Router können Zum Ziel von Malware werden, die die DNS-Einstellungen verändern. So könnten Eingebene URL's (Internetadressen) auf ungewünschte Webseiten umgeleitet werden (z.B. Phishing-Seiten). Ändern Sie auf jeden Fall Ihr Router-Kennwort !

7. Schutz gegen gehackte Webseiten
   Absolute Sicherheit gegen manipulierte Internetseiten gibt es nicht. Auf gehackten Seiten werden Downloads oft ohne ihr Wissen ausgelöst, heruntergeladen und installiert. Wirkungsvoll ist hier ebenfalls ein eingeschränktes Benutzerkonto (siehe 3.)

8. Peer-to-Peer-Netze (Tauschbörsen) meiden
   Tauschbörsen (die meisten davon sind sowieso illegal und können rechtliche Konsequenzen nach sich ziehen) sind ideale Nester für allerlei Schädlinge. Ein populärer Filmtitel als oder im Dateinamen, und die Datei wird tausendfach heruntergeladen. Finger weg von Tausch-börsen und P2P-Netzwerken !

9. Keine unnötigen Ports öffnen
   Auf jedem PC sind Ports die Schnittstellen vom System zur Aussenwelt, jeder offene Port erhöht das Risiko. Mit einer Hardware- bzw. Software-Firewall schirmt man die meisten Angriffe wirkungsvoll ab.

10. Malware vom Messenger abwehren
    Ähnlich wir per Mail kann auch per Messenger oder mit Chat-Programmen Malware verteilt werden. Hier ist genauso zu verfahren wie bei Punkt 3.