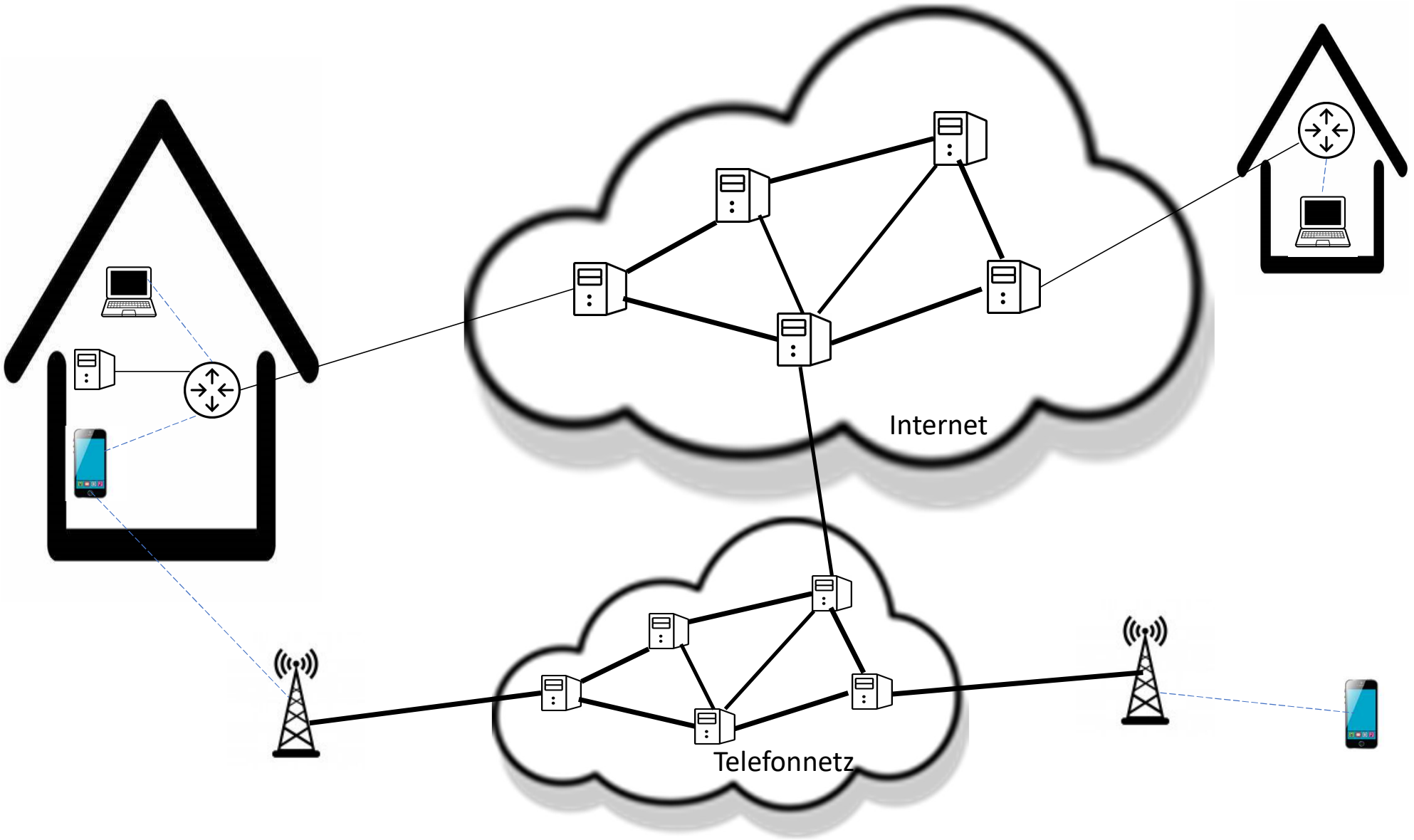
Internet
Telefonnetz

10 Tipps zur sicheren Nutzung des Internets

1. **Passen Sie Ihren Webbrowser an und halten Sie ihn aktuell**
2. **Halten Sie Ihr Betriebssystem und andere Software aktuell**
3. **Nutzen Sie Anwendungen zum Virenschutz und eine Firewall**
4. **Legen Sie unterschiedliche Benutzerkonten an**
5. **Schützen Sie Ihre Online- und Benutzerkonten mit sicheren Passwörtern**
6. **Seien Sie vorsichtig bei E-Mails und deren Anhängen**
7. **Seien Sie vorsichtig bei Downloads, insbesondere von Programmen**
8. **Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten**
9. **Schützen Sie Ihre Daten durch Verschlüsselung**
10. **Fertigen Sie regelmäßig Sicherheitskopien an**

1. Passen Sie Ihren Webbrowser an und halten Sie ihn aktuell

Was ist ein Browser

Ein Browser ist eine meist kostenlose Software zur grafischen Darstellung des World Wide Webs. Mit Hilfe eines Browsers werden Texte, Bilder, Videos aber auch Links und andere Funktionen einer Website angezeigt.
Die Bezeichnung Browser leitet sich vom englischen „to browse“ ab und bedeutet so viel wie „stöbern“ oder „blättern“.

Grundfunktionen

- Adressleiste zur Eingabe der URL / Schlagwortsuche
- Schaltflächen zum vorwärts und rückwärts Navigieren, zum Aktualisieren bzw. Neuladen und Anhalten eines Ladevorgangs
- Button zur Startseite des Browsers
- Funktion zum Setzen von Lesezeichen

Beispiele für Browser

Chrome (Google), Firefox (Mozilla), Edge (Microsoft), Safari (Apple), Opera, Brave ..

2. Halten Sie Ihr Betriebssystem und andere Software aktuell

Häufigste Betriebssysteme
PC: Windows, Linux, MacOS
Smartphones: IOS, Android

Häufig genutzte andere Programme
Browser, Office-Pakete, Medienplayer, Virenschutzprogramm,

- Verschaffen Sie sich einen Überblick über die von Ihnen eingesetzten Programme
- Prüfen Sie, zu welchen Produkten Sie automatische Update-Services erhalten
- Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken
- Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen
- Installieren Sie Updates möglichst rasch, sobald diese verfügbar sind

aber:
- Lassen Sie sich durch gefälschte Updates nicht aufs Glatteis führen!

3. Nutzen Sie Anwendungen zum Virenschutz und eine Firewall

Firewall
Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht.
Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.

Virenschutz
Antivirensoftware überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Anzeichen einer Infektion. Dazu vergleicht sie in erster Linie die Daten auf Ihrem Rechner mit den "Fingerabdrücken" bekannter Schadprogramme.
Diese "Signaturen" müssen aber immer auf dem aktuellen Stand sein, weil täglich neue Varianten von Schädlingen auftreten. Deshalb müssen Sie die Software regelmäßig aktualisieren (updaten).
Das geht entweder über die automatische Update-Funktion Ihres Programms. Oder Sie laden die Updates direkt von der Herstellerseite herunter.

4. Legen Sie unterschiedliche Benutzerkonten an

Schadprogramme haben die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind.

Als Administrator haben Sie vollen Zugriff auf fast alle Bereiche Ihres PCs.
Daher sollten Sie nur dann mit Administratorrechten arbeiten, wenn es unbedingt erforderlich ist.

Richten Sie für alle Nutzerinnen oder Nutzer des PCs unterschiedliche, passwortgeschützte Benutzerkonten ein.
Je nach Betriebssystem ist dies über die (System-)Einstellungen oder die Systemsteuerung möglich.

Vergeben Sie für diese Konten nur die Berechtigungen, die die jeweilige Nutzerin oder der jeweilige Nutzer benötigt.
So werden auch private Dateien vor dem Zugriff anderer geschützt.

Surfen Sie im Internet mit einem eingeschränkten Benutzerkonto und nicht in der Rolle des Administrators

5. Schützen Sie Ihre Online- und Benutzerkonten mit sicheren Passwörtern

Vergeben Sie für jedes Online- und Benutzerkonto ein eigenes, sicheres Passwort.
Ändern Sie schnellstmöglich alle Passwörter, wenn diese in falsche Hände geraten sein könnten.
Ändern Sie auch die von den Herstellern oder Diensteanbietern voreingestellten Passwörter bei der ersten Nutzung.

Diese Kriterien gelten für ein sicheres Passwort:

- Sie müssen sich ein Passwort gut merken können.
- Je länger das Passwort ist, desto besser.
  Ein komplexes Passwort sollte mindestens 8 Zeichen lang sein, ein einfaches mindestens 20 Zeichen lang.
- Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Umlaute können problematisch sein.
- Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster, Namen oder Geburtstage kommen ebenfalls als sicheres Passwort nicht in Frage.
- Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert.
- Nutzen Sie, wenn angeboten, die „Zwei-Faktor-Authorisierung“

Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern.
Geben Sie Ihre Passwörter niemals an Dritte weiter!

6. Seien Sie vorsichtig bei E-Mails und deren Anhängen

Verzichten Sie, wenn möglich, auf die Darstellung und Erstellung von E-Mails im HTML-Format und verwenden Sie stattdessen ein reines Textformat. (Einstellung im Mailprogramms)

Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen oder beim Klick auf einen Link. Schadprogramme werden oft über in E-Mails integrierte Bilder, Dateianhänge oder Links verbreitet .

Besonders zu beachten ist das bei E-Mails, deren Absenderin oder Absender Ihnen nicht bekannt ist.
Kommt Ihnen eine E-Mail von einem bekannten Absender seltsam vor, fragen Sie beim Absender nach, ob die E-Mail tatsächlich von ihm stammt. Nutzen Sie dabei aber nicht die in der E-Mail angegebenen Kontaktmöglichkeiten. Sie könnten gefälscht sein.

<u>Unerwünschte oder gefährliche E-Mails identifizieren:</u>
Indem Sie mit der Maus über den Absender fahren oder auf diesen klicken, können Sie erkennen, ob der Absender gefälscht ist. Achten Sie dabei auf wirre Buchstabenfolgen, optisch ähnliche Buchstaben oder eine ausländische Domain. Überprüfen Sie auch die Betreffzeile und den Text der E-Mail auf Sinnhaftigkeit und Rechtschreibung. Betrüger machen hier oft Fehler.

Seien Sie skeptisch, wenn eine schnelle Reaktion von Ihnen eingefordert wird.

7. Seien Sie vorsichtig bei Downloads, insbesondere von Programmen

Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen, insbesondere bei Programmen.

Meiden Sie Quellen, bei denen Sie Zweifel an der Seriosität haben.

Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist.
Nutzen Sie dafür Suchmaschinen, um gegebenenfalls mehr Informationen über den Hersteller zu erhalten oder Erfahrungsberichte von anderen Benutzerinnen oder Benutzern einzuholen.

Nutzen Sie nach Möglichkeit die Webseite des jeweiligen Herstellers zum Download und verschlüsselte Seiten, die Sie an der Abkürzung „https“ in der Adresszeile Ihres Browsers erkennen.

8. Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten

Kriminelle im Internet steigern ihre Erfolgsraten, indem sie ihre Opfer individuell ansprechen.
Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld
werden dazu genutzt, Vertrauen zu erwecken.

Persönliche Daten gelten heute als Währung im Netz und so werden sie auch gehandelt.

Überlegen Sie, welchen Onlinediensten Sie Ihre persönlichen Daten anvertrauen möchten.

Auch die ungeschützte Weitergabe persönlicher Daten in offenen ungesicherten Netzen sollte vermieden werden.

„need to know“ Prinzip anwenden: Welche Daten werden wirklich unbedingt benötigt

9. Schützen Sie Ihre Daten durch Verschlüsselung

Nutzen Sie möglichst nur Internetseiten, die eine verschlüsselte Verbindung anbieten.
Diese Internetadressen beginnen stets mit **https** und haben in der Adresszeile ein kleines geschlossenes Schlosssymbol.

Wenn Sie ein WLAN nutzen, achten Sie hier besonders auf die Verschlüsselung des Funknetzes. Wählen Sie in Ihrem Router den Verschlüsselungsstandard WPA2 oder WPA3 und ein komplexes, mindestens 20 Zeichen langes Passwort. Zugriff auf den Router erhalten Sie über eine festgelegte Internetadresse, die im Handbuch Ihres Routers vermerkt ist.

Wenn Sie die Möglichkeit haben, sich über ein Virtuelles Privates Netzwerk (VPN) mit Ihrem Heimnetz bzw. dessen Router zu verbinden, können Sie auch in öffentlichen WLAN-Hotspots genauso sicher unterwegs sein, wie Sie es von zu Hause gewohnt sind.
Moderne Router bieten oft die Möglichkeit, ein VPN einzurichten.

10. Fertigen Sie regelmäßig Sicherheitskopien an

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion eines Ihrer Geräte, können wichtige Daten verloren gehen.
Dies gilt ebenso bei dem Verlust eines Geräts oder einem anderweitigen Defekt.

Um den Schaden möglichst gering zu halten, ist es wichtig, regelmäßig Sicherungskopien, sogenannte Backups,
Ihrer Dateien auf externen Festplatten oder USB-Sticks zu erstellen.
Diese Datenträger sollten nur bei Bedarf mit dem PC verbunden sein.

Cloud-Dienste können für Sicherungskopien von verschlüsselten Daten herangezogen werden.

Stellen Sie aus der Sicherungskopie nur Ihre Daten wieder her.
Bei einem Neuaufsetzen des Geräts sollten keine Programme aus einer Sicherungskopie genommen werden,
da diese bereits infiziert sein könnten.