Daten und Geräte schützen

PCs, Smartphones, Tablets speichern und haben Zugriff auf wertvolle Daten. Damit diese Daten nicht verloren gehen, ausspioniert oder unbefugt verändert werden, sollten Sicherheitsmaßnahmen ergriffen werden.

Gute Passwörter/Kennwörter verwenden

Benutzername und Passwort ermöglichen nur befugten Benutzern den Zugang.
Ein gutes Passwort sollte

- aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen bestehen
- eine Mindestlänge von 8 Zeichen haben
- nicht in einem Wörterbuch stehen
- keinen persönlichen Bezug haben wie Geburtsdatum, Namensteile etc.
- regelmäßig geändert werden

Gutes Passwort: mVi1963g! (Merkhilfe: **m**ein **V**ater **i**st **1963 g**eboren**!**)
Schlechte Passwörter: 12345 qwertz geheim hallo boss passwort…

Firewall

Die Firewall kontrolliert den Datenverkehr zwischen den Computern. Sie schützt Computer vor unerwünschten Zugriffen über das Netzwerk. Moderne Betriebssysteme wie Linux oder Windows haben eine Firewall als Software dabei.

Backup

Der Computer ist kaputt – wo sind meine Daten?

Wenn eine Festplatte defekt wird oder ein Brand ausbricht, können Computerdaten zerstört werden. Man erstellt daher **Sicherheitskopien** (Backups) auf externe Datenträger (Festplatten, DVDs, etc.) mit denen man die Daten im Unglücksfall wiederherstellen kann.

Die Sicherheitskopien sollten unbedingt an einem anderen Ort aufbewahrt werden, damit sie im Schadensfall nicht auch zerstört werden!

Malware und Antivirensoftware

Malware ist ein Überbegriff für verschiedene Typen von unerwünschten Programmen. Wenn der Computer langsamer als sonst reagiert oder nicht mehr wie gewohnt funktioniert, kann Malware die Ursache sein.

Grundlegende Typen von Malware

Computerviren sind die älteste Art der Malware. Sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.

Ein **Computerwurm** ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie das Internet und versucht in Computer einzudringen.

Ein **Trojanisches Pferd** (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Spyware und Adware (zusammengesetzt aus **ad**vertisement und Soft**ware**) forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese

entweder zu verkaufen oder um gezielt Werbung zu platzieren. Diese Form von Malware wird häufig unbemerkt zusammen mit einer nützlichen Software installiert.

Wie kommt ein Virus auf meinen PC?

Infizierte Dateien können als E-Mailanhang oder durch Download aus dem Internet auf den PC kopiert werden. Wenn ein infiziertes Programm aufgerufen wird, verbreitet sich der Virus.

Auch USB-Sticks können Malware enthalten!

Wie schütze ich mich vor Malware?

- Keine Programme aus unsicheren Quellen installieren
- Keine unbekannte E-Mail-Anhänge öffnen
- Anti-Viren-Software installieren: Für Privatanwender ist das in Windows 10 enthaltene Antivirenprogramm Windows Defender ausreichend.
- Antiviren-Programme aktualisieren sich automatisch, damit auch die neuesten Viren erkannt werden.
- Das Betriebssystem und die Programme müssen die aktuellsten Sicherheitsupdates installiert haben.

Beantworte folgende Fragen:

Wie könnte ein gutes Passwort aussehen? Erstelle ein Passwort!

A - Gutes Passwort: _____

Wodurch wird der Datenverkehr zwischen Computer oder im Netzwerk überwacht?

A: _____

Wie heißt der Überbegriff für unerwünschte Programme?

A: _____

Wie kann man eine Sicherheitskopie auch nennen?

A: _____

Was macht eine Spyware?

A: _____

Fotografiere den QR-Code und löse das Quiz:

Erreichte Punkte: _____