

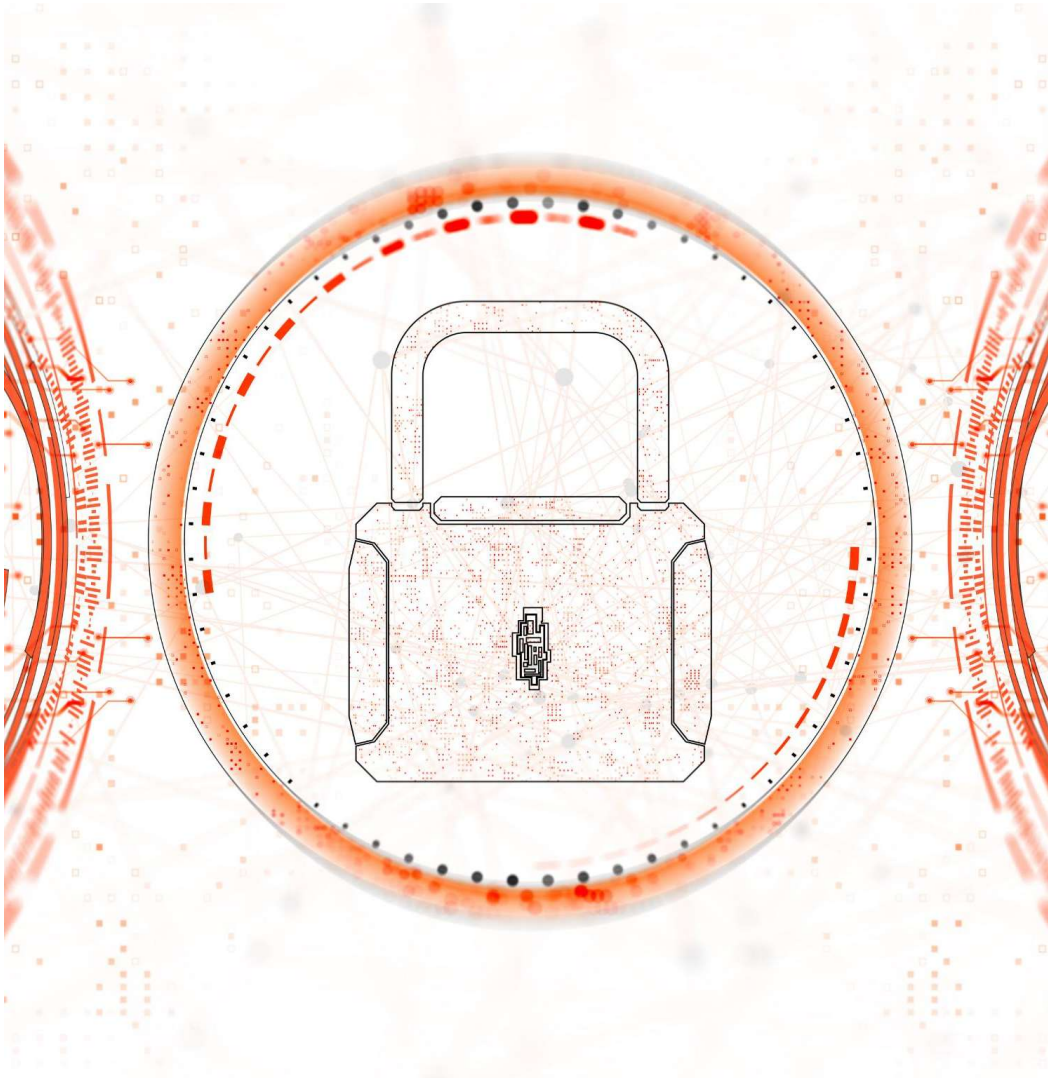


So bleibt Ihr Computer sicher – Tipps für den Alltag

Referent

Stefan Kammermann

Techniker bei DM Informatik



Unsere Themen heute

1. Software aktuell halten und Systempflege
2. Antivirenschutz – Schutz vor digitalen Bedrohungen
3. Sichere Passwörter und Passwort-Manager
4. Backup – Schutz vor Datenverlust
5. Die wichtigste Verteidigungslinie



Warum regelmässige Updates und Wartung wichtig sind

Betriebssystem aktuell halten

Durch Updates werden Sicherheitslücken geschlossen, die potenziellen Angreifern sonst Zugriff ermöglichen könnten.

Softwarewartung

Veraltete Software stellt eine grosse Schwachstelle dar und erleichtert Angreifern den Zugriff.

Es ist entscheidend dass System immer auf dem neuesten Stand zu halten.

Support-Ende von Windows 10

Ende des Supports

Der Support für Windows 10 endet im **Oktober 2025**, danach gibt es keine Sicherheitsupdates mehr.

Sicherheitsrisiken veralteter Systeme

Veraltete Systeme sind anfälliger für Angriffe, da keine Sicherheitsupdates mehr zur Verfügung stehen.



Was können Sie tun?



Betriebssystem prüfen

Überprüfen Sie welche Version von Betriebssystem Sie auf Ihrem Gerät haben.

System aktualisieren

Halten Sie Ihr Betriebssystem stets auf dem neuesten Stand für bessere Sicherheit und Leistung.

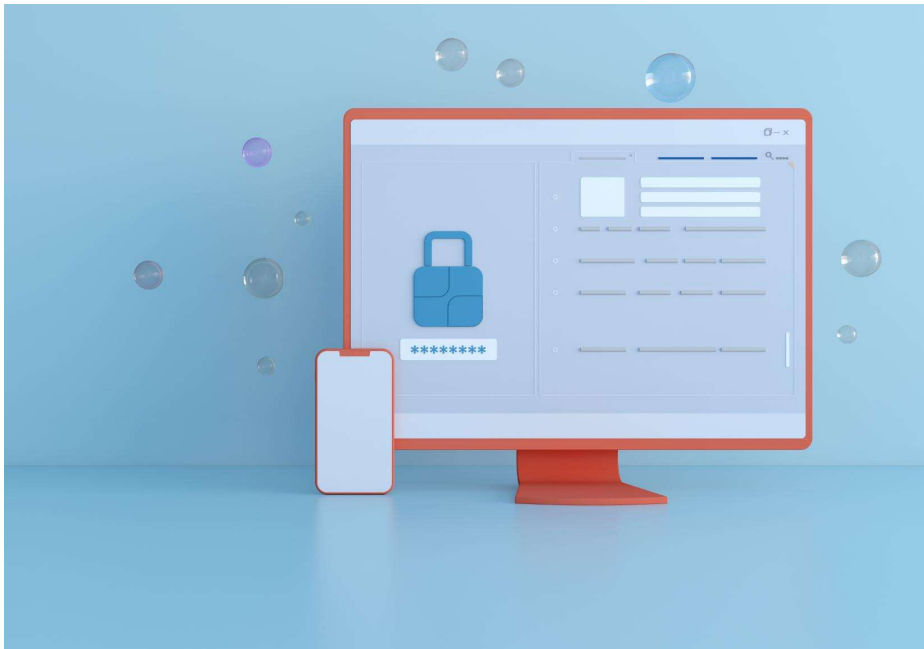
Software deinstallieren

Entfernen Sie unnötige Programme.

Systemwechsel erwägen

Überlegen Sie, von Windows 10 auf Windows 11 zu wechseln, wenn Ihr Gerät dies unterstützt.

Funktion und Bedeutung von Antiviren-Software



Antivirus als digitaler Türsteher

Antiviren-Software schützt als digitaler Türsteher vor unerwünschten Eindringlingen und Schadprogrammen.

Grundschutz durch Defender

Der integrierte Defender bietet automatischen und soliden Schutz gegen viele Bedrohungen im Alltag.

Erweiterte Kaufprodukte

Kaufbare Antivirenprogramme bieten zusätzliche Funktionen für umfangreicheren Schutz und Sicherheitserweiterungen.



Was können Sie tun?

Antivirenschutz überprüfen

Stellen Sie sicher, dass Ihr Antivirenschutz aktiv ist, meist ist Microsoft Defender automatisch eingeschaltet.

Kauf eines Antivirenprogramms

Erwägen Sie den Kauf eines professionellen Antivirenprogramms für zusätzlichen Schutz sensibler Daten.

Warum starke Passwörter wichtig sind



Passwörter als Schlüssel

Passwörter funktionieren wie Schlüssel, einfache sind leicht kopierbar und unsicher.



Merkmale starker Passwörter

Starke Passwörter haben mindestens 12 Zeichen mit Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Merkmale sicherer Passwörter und Einsatz von Passwort-Managern



Merkmale sicherer Passwörter

Sichere Passwörter sind mindestens **12 bis 14 Zeichen** lang und enthalten **Gross-** und **Kleinbuchstaben**, **Zahlen** sowie **Sonderzeichen**.

Gefahren mehrfacher Passwörter

Verwenden Sie **niemals dasselbe Passwort** für mehrere Dienste, um Sicherheitsrisiken zu vermeiden.

Funktion von Passwort-Managern

Passwort-Manager speichern und füllen komplexe Passwörter automatisch aus, sodass nur **ein starkes Master-Passwort** nötig ist.

Arten von Passwort-Managern

Es gibt integrierte Browser-Manager und Programme für Passwortverwaltung.

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung erklärt

Zwei-Faktor-Authentifizierung schützt Konten durch einen zusätzlichen Sicherheitscode neben dem Passwort.

Schwache Passwörter ändern

Aktivieren Sie die Zwei-Faktor-Authentifizierung bei allen Diensten, die das anbieten





Was können Sie tun?

Schwache Passwörter ändern

Ersetzen Sie einfache Passwörter durch starke (12 Zeichen, Sonderzeichen).

Ein Passwort nur einmal verwenden

Nutzen Sie für jeden Dienst ein einzigartiges Passwort.

Passwort-Manager nutzen

Lassen Sie den Manager Ihre Passwörter für Sie verwalten.

Zwei-Faktor-Authentifizierung aktivieren

Zusätzlicher Schutz für Ihre wichtigsten Konten.



Backup – Ihre Datenversicherung

Schutz vor Datenverlust

Backups schützen wichtige Fotos, Dokumente und Erinnerungen vor Verlust durch Defekte oder Angriffe.

Backup als Rettungsanker

Es ist die einzige sichere Methode, um nach einem Datenverlust wieder auf Ihre wichtigen Dateien zugreifen zu können.

Merkmale eines guten Backups

Mehrere Versionen speichern

Ein gutes Backup bewahrt ältere Datenversionen, um versehentliche Verluste zu vermeiden.

Vielfältige Speichermedien

Backups sollten auf verschiedenen gespeichert werden.

Offline Lagerung

Nach dem Backup muss die Sicherung vom Computer getrennt und offline gelagert werden, um Virenbefall zu verhindern.



Was können Sie tun?



Wichtigkeit der Datensicherung

Regelmässige Backups schützen wichtige Daten wie Fotos, Dokumente und Videos vor Verlust.

Backup-Methode

Daten auf eine externe Festplatte kopieren oder eine einfache Backup-Software verwenden.

Festplatte trennen

Nach dem Backup unbedingt die externe Festplatte vom Computer trennen, um Daten zu schützen.

**Regelmässige Datensicherung ist wie eine
Versicherung für Ihre persönlichen.**

Ihre wichtigste Verteidigung: Kritisch hinterfragen



Kritisches Hinterfragen

Ihre eigene Aufmerksamkeit ist der beste Schutz vor digitalen Täuschungen.

Kriminelle setzen Sie unter Druck

Betrüger nutzen immer Zeitdruck und Ängste aus. Wenn Sie nicht in Ruhe nachdenken können, ist das ein Alarmzeichen.

Ruhig bleiben und prüfen

Nehmen Sie sich eine Sekunde Zeit, lassen Sie sich nicht unter Druck setzen und hinterfragen Sie jede Situation.

Bei Unsicherheit

Haben Sie Misstrauen, legen Sie auf oder löschen Sie die Nachricht. Fragen Sie im Zweifelsfall immer eine vertrauenswürdige Person um Rat.

Was können Sie tun?



Vorsicht bei E-Mails

E-Mails sollten stets kritisch geprüft werden, um Phishing und Betrug zu vermeiden.

Misstrauen bei Anrufen

Erteilen Sie niemandem, den Sie nicht kennen, Fernzugriff auf Ihren Computer.

Vorsicht bei Angeboten

Zu gute Angebote können Täuschungsversuche sein und erfordern kritische Analyse.

Die 5 wichtigsten Tipps im Überblick

Software aktuell halten

Aktualisieren Sie regelmässig Betriebssystem und Programme.

Antivirenschutz nutzen

Nutzen Sie ein Antiviren Programm.

Sichere Passwörter verwenden

Verwenden Sie Passwort-Manager für komplexe und einzigartige Passwörter.

Regelmässige Backups erstellen

Erstellen Sie regelmässig Backups.

Kritisch hinterfragen

Seien Sie wachsam und hinterfragen Sie alle Internetinhalte und Nachrichten.

Danke für Ihre Aufmerksamkeit



- Wir schätzen Ihr Interesse an Computersicherheit.
- Bleiben Sie wachsam und schützen Sie Ihre Daten.
- Bei Fragen stehen wir Ihnen gerne zur Verfügung.