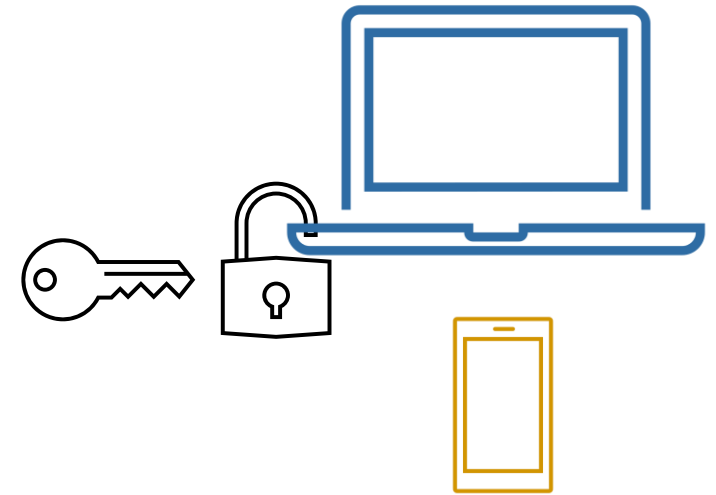


# IT-Sicherheit

- Update
- Passwörter
- Zweifaktor-Authentisierung
- Virenschutzprogramm
- Firewall



## Auf einen Blick

---

3 Basiselemente der IT-Sicherheit

4 Updates

5-8 Passwörter

9 Zweifaktor-Authentifizierung

10+11 Virenschutzprogramm

12+13 Beispiel einer verdächtigen E-Mail

14+15 Sicherheit beim Umgang mit Web-Seiten

16 Firewall

17 Haben Sie noch Fragen?

Anhang: Tabellenvorlage für Passwörter

# Basiselemente der IT-Sicherheit



# Updates

## Softwareupdates – ein Grundpfeiler der IT-Sicherheit

Hersteller beseitigen Fehler, schließen **Sicherheitslücken** oder fügen Funktionen hinzu.

- **Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!**
- **Installieren Sie Updates möglichst rasch, sobald diese verfügbar sind!**
- **Aktivieren Sie automatische Updates!**
- **Updates von Programmen, nie von Mails oder anderen Aufforderungen laden**

# Passwörter



**Vergeben Sie für jedes Online- und Benutzerkonto ein eigenes, sicheres Passwort.**

**Ändern Sie auch die von den Herstellern oder Diensteanbietern voreingestellten Passwörter nach der ersten Nutzung.**



## **Folgende Kriterien gelten für ein sicheres Passwort:**

- **Je länger das Passwort ist, desto besser**
- **Das Passwort sollte mindestens acht Zeichen lang sein**
- **Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen**
- **Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster kommen ebenfalls als sicheres Passwort nicht in Frage**
- **Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert**



## Passwortmanager

- Ein noch so starkes Passwort hilft wenig, wenn Sie es sich nicht merken können
- Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern und Ihre Passwörter speichern und auch erzeugen
- Das Abrufen der PW kann dann automatisch erfolgen
- Im Passwortmanager können auch weitere wichtige Daten gespeichert werden (Kundennummern, Telefonnummern, Steuernummer ...)
- Passwortmanager sind eine wertvolle Hilfe beim digitalen Nachlass

**Hier einige Manager: Bitwarden, 1Password, Keeper, Nordpass (Liste nicht vollständig).**

# Passwörter



## Alternative zu Passwortmanagern

Wer auf Papier nicht verzichten möchte, hier eine einfache Methode:

Sie merken sich den Teil1, der ist immer gleich, in ihre Liste schreiben Sie den Teil2 des Passworts, so kann niemand etwas mit der Liste anfangen.

Name des Zugangs	Teil1 (gemerkt)	Teil2 (aufgeschrieben)	Ges. Passwort
Sparkasse	<i>glems</i>	AbPsu14!	glemsAbPsu!
Telekom	<i>glems</i>	Cxv284#	glemsCxv184#

# Zwei-Faktor-Authentifizierung



Zwei-Faktor-Systeme greifen nach der Passwortabfrage auf externe Systeme zurück, um eine zweistufige Überprüfung der Nutzerin oder des Nutzers durchzuführen.

**Andere Beispiele:**

- Fingerabdruck
- Chipkarte
- Biometrische Systeme



# Virenschutzprogramm



**Ein Virenschutzprogramm überprüft den gesamten Rechner auf Anzeichen einer Infektion.**

**In den gängigen Betriebssystemen sind ein Virenschutz und eine Firewall integriert.**

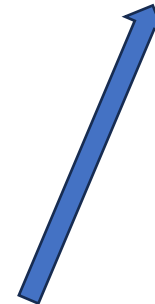
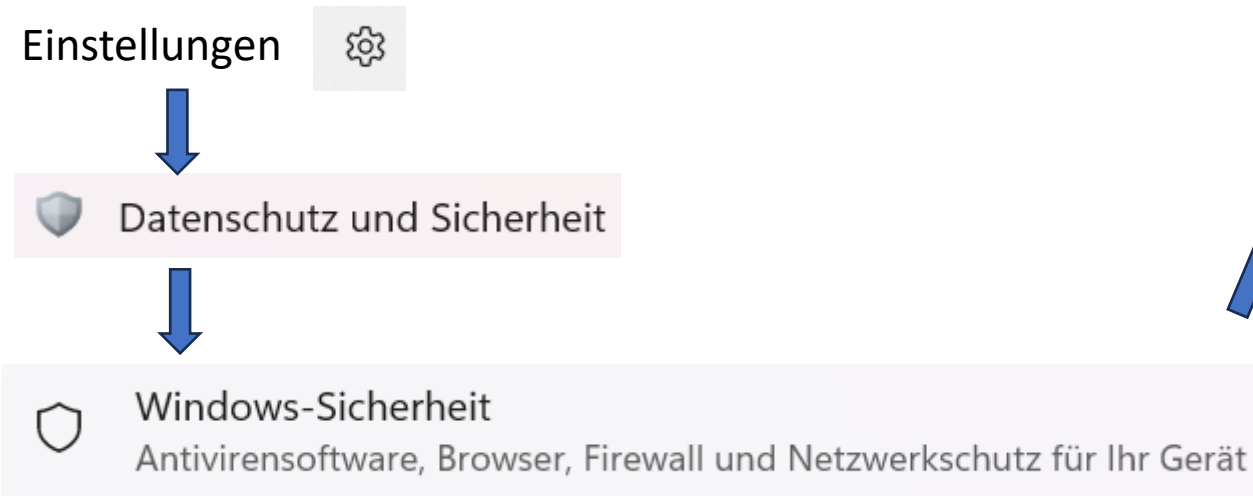
**Aktivieren Sie diese!**






# Virenschutzprogramm



11

Bei Microsoft (Windows 11):



Schutzbereiche	
	<b>Viren- und Bedrohungsschutz</b> Keine Maßnahmen erforderlich.
	<b>Kontoschutz</b> Keine Maßnahmen erforderlich.
	<b>Firewall und Netzwerkschutz</b> Keine Maßnahmen erforderlich.
	<b>App- und Browsersteuerung</b> Keine Maßnahmen erforderlich.
	<b>Gerätesicherheit</b> Keine Maßnahmen erforderlich.

# Beispiel einer verdächtigen E-Mail



Von STRATO <noreply@ewe.de> 

An noreply@ewe.de 

Betreff **Letzte Erinnerung: Ihre Rechnung ist offen**

**Absender ?**

**Impressum ?**

© 2025 Ihr Unternehmen • Musterstraße 1, 12345 Musterstadt



**Sehr geehrter Kunde**

**Anschrift?**

unsere Unterlagen zeigen, dass folgende Rechnung noch nicht beglichen wurde:

Rechnungsnummer	RE-2025-98502200001
Rechnungsdatum	01. August 2025
Offener Betrag	9,95 €
Fälligkeitsdatum	06. August 2025

Bitte überweisen Sie den offenen Betrag bis zum Fälligkeitsdatum, um eine unterbrechungsfreie Nutzung Ihrer Services sicherzustellen.

Sobald Ihre Zahlung bei uns eingeht, wird Ihr Zugang automatisch aktiviert und Sie erhalten eine Zahlungsbestätigung per E-Mail.

Falls Sie die Zahlung bereits veranlasst haben, betrachten Sie diese Nachricht bitte als gegenstandslos.

**Link?**

**Jetzt sicher bezahlen**

# Beispiel einer verdächtigen E-Mail



**Achtsamkeit bei E-Mails, hier sind Sie selbst gefragt:**

- **Ist der Absender verdächtig?**
- **Ist die Anschrift unpersönlich?**
- **Ist das Impressum verdächtig?**
- **Nie einen Link bei fremden Mails anklicken!**

# Sicherheit beim Umgang mit Web-Seiten



14

Startpage Suchergebnisse x Girokonto - finden Sie Ihr Konto | x +

www.sparkasse-pforzheim-calw.de/de/home/privatkunden/giro

AKARS Compcaf 31 Kalender pbb Überblick Einreichen m we

Privatkunden Firmenkunden

Sparkasse Pforzheim Calw Produkte Firmenkunden Private Banking

## Aus meinem Girokonto mehr rausholen

**Finanzorganisation leicht gemacht.**

Mit den zahlreichen Zusatzleistungen des Sparkassen-Girokontos organisieren Sie Ihre Finanzen noch einfacher.

**Giro Gold eröffnen**

# Sicherheit beim Umgang mit Web-Seiten



15

**Was können Sie tun, um im Browser auf der *sicheren Web-Seite* zu sein?**

- Deaktivieren sie alle Cookies auf der WEB-Seite
- Gehen sie nach Möglichkeit immer auf die originale Anbieter Seite, vor allem bei der Google Suche!






**Starten Sie ihre sensiblen Seiten (Bank und Bezahlssysteme) immer direkt aus dem Browser, nie über einen Link!**

# Firewall

Eine Firewall (Brandwand‘ oder ‚Brandmauer‘) ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.

Auch in den meisten Routern (Fritz Box, Telekom Speedport) ist eine Grundeinstellung „Firewall“ vorhanden, Bei Bedarf kann man diese einstellen.

## Schutzbereiche

-  Viren- und Bedrohungsschutz  
Keine Maßnahmen erforderlich.
-  Kontoschutz  
Keine Maßnahmen erforderlich.
-  Firewall und Netzwerkschutz  
Keine Maßnahmen erforderlich.
-  App- und Browsersteuerung  
Keine Maßnahmen erforderlich.
-  Gerätesicherheit  
Keine Maßnahmen erforderlich.

## Basiselemente der IT-Sicherheit

### Updates:

Halten Sie Ihre Software durch Sicherheits-Updates auf dem neuesten Stand.

### Passwörter:

Verwenden Sie möglichst starke und unterschiedliche Passwörter. Hierfür können Sie einen Passwortmanager nutzen.

### Zwei-Faktor-Authentisierung:

Schützen Sie sich zweifach: Neben dem ersten Faktor, meist einem Passwort, nutzen Sie in einem zweiten Schritt z.B. Ihren Fingerabdruck oder eine TAN.



**Häufig vorhandener Schutz auf PCs und Laptops**

### Virenschutzprogramm:

Es überprüft den gesamten Rechner auf Anzeichen einer Infektion.

### Firewall:

Sie schützt vor Angriffen von außen und verhindert, dass Programme, z.B. Spyware, Kontakt vom Gerät zum Internet aufnehmen.

© Bundesamt für Sicherheit in der Informationstechnik (BSI)

www.bsi.bund.de



*Haben Sie noch Fragen?*

*Kontaktieren Sie uns:*

***Computercafé, jeden Dienstag von 15 bis 18 Uhr***

*Tel. 07156-3071972 (AB)*

*Mail: [compcaf-schoeckingen@posteo.de](mailto:compcaf-schoeckingen@posteo.de)*

Grafiken tlw.: Bundesamt für Sicherheit in der Informationstechnik

# Beispieltabelle für Zugangsdaten

Anbieter/Konto	Benutzer/Anmeldename	Passwort/PIN	Sonstige
Kreissparkasse Ludwigsburg	AnOp2531	gerSte890#	
Mikrosoft Konto	meier@t-online.de	kAter468!	Ondrive PIN ....
Google Konto	Müller66@gmail.com	24435Ankom*	
E-Mail Konto T-Online	meier@t-online.de	oNT#260s!	www.telekom.de/kunden center