



## Internet- und PC-Unterstützung für die Generation 50plus

### Vortrag Nr. 94 „Aktuelle Tipps zu PC und Smartphone“ zum 24.05.2025 Bürgerhaus

1. **Warnhinweise:**  
Betrugsmaschen, Schockanrufe, Schufa-IdentChecker,  
Tipps der Polizei, Telefonbetrug/Recovery-Scam,  
angebliche Microsoft-Mitarbeiter, Verbraucherzentralen **Seite 2**
2. **Smartphones Handy über Nacht laden: Eine gute Idee?**  
Ladekabel in der Steckdose, Stromverbrauch **Seite 9**
3. **Smartphone, Tablet, PC: Ladegeräte Achtung Brandgefahr** **Seite 11**
4. **PC und Smartphone: Skype > Teams**  
Alternative: Chatten mit WhatsApp **Seite 12**
5. **PC: Ende Support für Windows 10, Windows 8.1 und Windows 7**  
Datensicherung erstellen in Windows 10 und 11 **Seite 14**
6. **Datenverlust** **Seite 16**
7. **PC: Programm mrt, Bits-Bytes-MB-GB-TB** **Seite 17**
8. **Tipps vom BSI, IT-Sicherheit, Sicherheits-Irrtümer** **Seite 21**
9. **Kostenlose Vorträge herunterladen : [www.stsr-heidenheim.de](http://www.stsr-heidenheim.de)** **Seite 22**



## 1. Warnhinweise

[Tipp von der Verbraucherzentrale >> hier klicken zum ganzen Bericht](#)

Das Wichtigste in Kürze:

1. Es sind wieder vermehrt Fake-Nachrichten von Versanddienstleistern im Umlauf.
2. Betrüger wollen damit auf diesem Wege Schadsoftware auf Ihren Geräten installieren, persönliche Daten abfischen und Kasse machen.
3. Prüfen Sie Sendungsverfolgungen von Paketdienstleistern kritisch. Seien Sie insbesondere dann misstrauisch, wenn Sie offene Geldbeträge zahlen sollen.

**Was Sie niemals tun sollten:** SMS und Mails öffnen unbekannter Herkunft, vor allem, wenn eine Sendung, Paket oder Päckchen angekündigt wird. Wer nichts bestellt hat, erwartet keine Sendung!  
**Was soll man tun? Sofort löschen.**

**Klicken Sie niemals auf so einen Link. Geben Sie keine Daten ein. Hier ein Beispiel:**

Aufgrund unvollständiger Adressangaben kann Ihr Paket nicht zugestellt werden. Sie sollen Ihre Adresse innerhalb von 12 Stunden bestätigen, über diesen Link [DHL. de-podx.com/tracking](https://de-podx.com/tracking).

**So läuft ein echter Bestellvorgang in der Regel ab:** Haben Sie im Internet etwas bestellt, erhalten Sie immer sofort eine Mail, in der Sie namentlich angesprochen werden. Die bestellte Ware wird im Text beschrieben, eine Bestätigung der Bestellung. Ebenso wird der Preis in der Mail genannt. Und meistens kommt relativ zügig eine weitere Mail mit der Tracking-Nummer und dem Hinweis, dass das Paket bereits unterwegs ist.



## 1. Warnhinweise

### Umfrage zeigt: Auf diese Betrugsmaschen fallen die meisten herein

von t-online, [sha](#) 14.05.2025 - 08:11 Uhr

**Identitätsdiebstahl, Scamming, Fake Shops: Onlinebetrug nimmt zu – mit teils drastischen Folgen für die Betroffenen, wie eine Umfrage zeigt. Mehr als 10.000 Euro haben manche Verbraucher verloren, weil sie auf gefälschte Shops im Internet hereingefallen sind. Das hat eine [Umfrage](#) der Schufa ergeben, die t-online vorab vorliegt.**

Wer wissen möchte, ob die eigenen Daten im Internet gestohlen wurden, kann laut **Schufa** den kostenlosen [IdentChecker](#) nutzen. Dieser prüft, ob Daten bei dubiosen Quellen im Internet oder Darknet veröffentlicht wurden.

 schufa

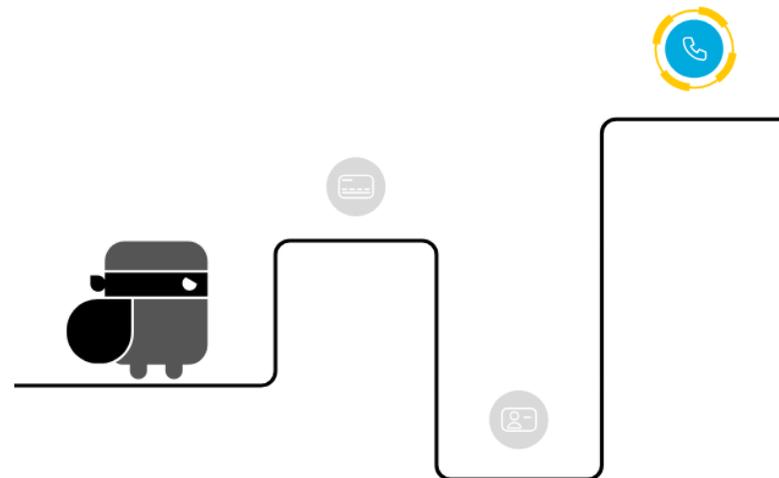


**IDENTITÄT**

**GEKLAUT?**

Auf dieser Seite können Sie **kostenlos prüfen**, ob Ihre Daten bei **einem Datendiebstahl** im Internet veröffentlicht wurden. Nach der Prüfung wird Ihnen ein Ergebnis angezeigt und Sie erhalten Handlungsempfehlungen, um Ihre Daten besser schützen zu können.

 In Partnerschaft mit  
Deutsche Telekom Security



Quelle: <https://www.schufa.de/identchecker/>

**Zur Startseite**



## 1. Warnhinweise

Man kann nacheinander auf der Seite der Schufa diese 5 Eingaben machen und prüfen

Was möchten Sie prüfen?  
Ihre eingegebenen Daten werden nicht gespeichert.

E-MAIL    MOBILFUNK-NR.    KREDITKARTEN-NR.    IBAN    AUSWEIS-NR.

mustermann@example.com    Anti-Roboter-Verifizierung    jetzt kostenlos prüfen

FriendlyCaptcha

**schufa** In Partnerschaft mit Deutsche Telekom Security

**IHR PRÜFERGEBNIS:**  
**KEINE AKTUELLEN TREFFER**

Detaillierter Bericht

Geprüfte E-Mail-Adresse:  
stadtseniorenrat-hdh@t-online.de

Suchdatum	14.05.2025, 17:44 Uhr
Prüfzeitraum	die letzten 90 Tage
Suchort	✓ öffentliches Internet ✓ Deep Web ✓ Darknet

Lassen Sie sich dauerhaft mit dem **SCHUFA:IdentSafe** schützen und per E-Mail/SMS über Datenlecks informieren

Wir wünschen Ihnen jeweils so ein positives Ergebnis

Quelle: <https://www.schufa.de/identchecker/>

Zur Startseite



## **1. Warnhinweise**

**Die Polizei** ruft niemals unter der 110 an und auch nicht mit einer anderen Nummer !!!

Immer wieder sind Betrüger unterwegs, die sich als Polizisten ausgeben, um in den Besitz von Geld und anderen Wertgegenständen ihrer Opfer zu gelangen.

**Was tun? Sofort auflegen!!!**

**Lassen Sie grundsätzlich keine Unbekannten in Ihre Wohnung.**

Fordern Sie von angeblichen Amtspersonen, zum Beispiel Polizisten, den Dienstausweis.

Rufen Sie beim geringsten Zweifel bei der Behörde an, von der die angebliche Amtsperson kommt.

Suchen Sie die Telefonnummer der Behörde selbst heraus oder lassen Sie sich diese durch die Telefonauskunft geben. **Wichtig:** Lassen Sie den Besucher währenddessen vor der abgesperrten Tür warten.

Geben Sie am Telefon keine Details zu Ihren finanziellen Verhältnissen preis.

**Lassen Sie sich am Telefon nicht unter Druck setzen.** Legen Sie einfach auf.

Übergeben Sie niemals Geld an unbekannte Personen.

Weitere Tipps der Polizei z.B. zum Enkeltrick finden Sie bei diesem Link:

<https://www.polizei-beratung.de/themen-und-tipps/betrug/betrug-durch-falsche-polizisten/>



## 1. Warnhinweise

### Polizei und Opferhilfevereine warnen vor sogenannten Schockanrufen:

Vor allem älteren Menschen wird am Telefon zum Beispiel vorgegaukelt, Sohn oder Tochter hätten einen schweren Unfall verursacht und nun müsse eine horrende Kautionszahlung geleistet werden.

**Was tun? Sofort auflegen!!!** Auf gar keinen Fall sollte man irgendeinen Namen nennen, also niemals sagen: "bist Du es ....." Oder: "geht es um meinen ....."

**Betroffene sollten keinesfalls darauf eingehen und sofort den Hörer auflegen.** Man sollte sich niemals in ein Gespräch verwickeln lassen. Vereinbaren Sie ein Codewort, das nur die Personen in der Familie und ggf. engste Freunde kennen und fragen dieses Codewort im Zweifelsfall ab !

### Abzocke durch angebliche Microsoft-Mitarbeiter

Warnung vor falschem Microsoft-Support: Angebliche Mitarbeiter des technischen Supports von Microsoft versuchen per Telefon oder über gefälschte Warnhinweise am PC, Zugriff auf Ihren PC zu erlangen. Welche Masche dahinter steckt und wie Sie sich schützen können.

Das Wichtigste in Kürze: Vorsicht bei gefälschten Warnhinweisen am PC oder Anrufen von vermeintlichen Microsoft-Mitarbeitern, die versuchen Ihnen weis zu machen, dass Ihr Computer von Viren befallen sei.

### **Was tun? Sofort auflegen!!! Gerät vom Netz trennen!**

Microsoft führt nach eigenen Angaben keine unaufgeforderten Telefonanrufe durch, um schadhafte Geräte zu reparieren. Selbst auf offizielle Support-Anfragen erfolgen Hilfestellungen fast ausschließlich per E-Mail.

**Werden Sie von einem angeblichen Microsoft-Mitarbeiter angerufen, beenden Sie das Gespräch sofort. Haben Sie bereits mit einem falschen Microsoft-Mitarbeiter gesprochen, trennen Sie Ihren PC vom Netz und ändern Sie Ihre Passwörter. Melden Sie den Vorfall sofort der Polizei.**



## **1. Warnhinweise**

**Smartphones** sind ein beliebtes Angriffsziel für Cyberkriminelle. Wie Sie mit einem einfachen Kniff das Risiko für Attacken verringern, verrät der US-Geheimdienst NSA.

Moderne Smartphones haben die Rechenkapazitäten eines vollwertigen Computers und sind praktisch immer online. Das machen sich viele Hacker zunutze. Durch fiese Tricks schleusen sie Viren und Trojaner auf die Geräte und kapern deren System, um es zu ihren eigenen Zwecken zu missbrauchen. Sich zu 100 Prozent vor solchen Angriffen zu schützen, ist nur schwer möglich.

Es gibt jedoch eine simple Methode, um das Risiko für Cyberattacken auf Ihr Handy deutlich zu senken:  
**Öfter mal abschalten, am besten über Nacht.**

**Durch das Herunter- und wieder Hochfahren des Systems verhindern Sie demnach in vielen Fällen die Installation von Schadsoftware durch sogenanntes Spear-Fishing.**

Dabei handelt es sich um sehr gezielt eingesetzte Phishing-Versuche, mit denen eine Person bewusst von den Angreifenden ins Visier genommen wird.



## 1. Warnhinweise

### **Aufgeklärt: Telefonbetrug – Recovery-Scam**

**Beim Recovery-Scam haben es Kriminelle auf Personen abgesehen, die bereits Opfer von Betrug wurden und viel Geld verloren haben. Sie geben sich als Kanzlei oder Fachabteilung aus und behaupten, dass das verlorene Geld wieder zurückgeholt werden kann.**

Erfahren Sie im Videoclip des Landeskriminalamts mehr über diese Masche und helfen Sie uns, den Betrüger\*innen das Handwerk zu legen: →

[https://www.youtube.com/watch?v=DVTEVR2gdAg&list=PLHlto8FZiDxtThWg\\_QGI0xIDImmVjebf8&index=1](https://www.youtube.com/watch?v=DVTEVR2gdAg&list=PLHlto8FZiDxtThWg_QGI0xIDImmVjebf8&index=1)

### **Betrüger wenden psychologische Techniken an (Scamming)**

**Am schlimmsten sind Betrügereien bei denen, die bereits Opfer eines Betrugs geworden sind. Man kann es sich kaum vorstellen, dass man wieder reinfällt, oder doch?**

Nachdem Sie betrogen wurden, sind Sie anfälliger für einen Erstattungs- oder Rückforderungsbetrug. Jemand verspricht, Ihnen dabei zu helfen, Ihr Geld zurückzubekommen. Aber Sie müssen ihn erst für seine Dienste bezahlen. **Werden Sie hellhörig und glauben nicht den Versprechungen, denn es geht nur darum, Ihnen erneut Geld aus der Tasche zu ziehen. Es werden Forderungen für Vorauszahlungen für angebliche Wiederherstellungsdienste gestellt.**

Um die Versprechungen in die Tat umzusetzen, wird eine Anfangsinvestition verlangt.

**Ein Beispiel: Das Opfer muss mehr als 1000 € im Voraus bezahlen, um sein Geld zurückzubekommen. Dann wird die Summe durch weitere Zahlungen auf das Dreifache des ursprünglichen Wertes erhöht.**



## 1. Warnhinweise

Wissen Sie, wie wichtig die **Verbraucherzentralen** sind? Dass es sie überhaupt gibt, was sie machen?

Informieren Sie sich und klicken hier auf diese Seite:

[Verbraucherschutz2go](#) [Schluss mit Abo-Fallen, Bio-Schwindel und Fake-Shops.](#)

Oben rechts finden Sie im **Menü** eine Auswahl zu allen relevanten aktuellen Themen, viele Videos und Informationen.

The screenshot shows the homepage of Verbraucherzentrale. At the top left is the logo 'verbraucherzentrale'. On the right, there is a 'Menü' button with a dropdown menu containing: 'Artikel', 'Videos', 'Interaktiv', 'Über Uns', 'Impressum', and 'Datenschutz'. Below the menu are three article cards:

- Card 1:** '#Finanzen' with a photo of hands typing on a laptop. Title: 'Online bezahlen: Welche Möglichkeiten gibt es?'. Text: 'Wenn du online auf Shoppingtour gehst, gibt's verschiedene Möglichkeiten zu bezahlen. Hier findest du einen Überblick über Vor- und Nachteile...'. Button: 'Artikel lesen'.
- Card 2:** '#Finanzen' with a pink background and 'BUY NOW PAY LATER' text. Title: 'Gefährlicher Trend? „Buy now, pay later“'. Text: '„Ich zahl einfach in 30 Tagen mit Klarna, was soll schon passieren?“ Wie „Buy now, pay later“ zur Schuldenfalle wird...'. Button: 'Artikel lesen'.
- Card 3:** '#Digitales' with a photo of a smartphone. Title: 'App-Tracking: Personalisierte Werbung auf dem Handy'. Text: 'Beeinflusst Tracking nur unser Surfverhalten oder werden wir etwa ausspioniert? Besser ausstellen als anlassen! Täglich nutzt du Apps auf deinem...'. Button: 'Artikel lesen'.

At the bottom center, there is a button 'Alle Artikel →'. A red arrow from the text above points to the 'Menü' button.

[Zur Startseite](#)



## **2. Smartphone Handy über Nacht laden: Eine gute Idee?**

Fast jeder Smartphone Nutzer tut es: Sein Handy abends vor dem Zubettgehen zum Laden an das Ladegerät anstecken und über Nacht laden lassen. Doch nur, weil es jeder tut, heisst es noch nicht, dass das auch gut ist. Das nächtliche Laden kann nämlich die empfindliche Technologie der Akkuzellen schädigen. Und manche Menschen fragen sich gar, ob es gefährlich ist, das Handy über Nacht laden zu lassen.

### **Handy über Nacht laden – die wichtigsten Punkte kurz zusammengefasst:**

- Handys nachts zu laden, stellt heute kein Sicherheitsrisiko mehr dar.
- Es ist allerdings empfehlenswert, am Handy Einstellungen zum Schutz des Smartphones zu aktivieren, um den Akku zu schonen.
- Überprüfe regelmässig alle Anschlüsse, die **Netzteile** und das **Ladekabel**. Haben Ladekabel oder Netzteil Beschädigungen, ersetze das entsprechende Teil.
- **Wenn das Handy über Nacht ausgeschaltet ist, lädt es schonender.**

### **Die gute Nachricht zuerst: Es ist nicht gefährlich, das Handy über Nacht zu laden.**

Moderne Smartphones verfügen über ausreichende Schutzmechanismen. Ein Überladeschutz schützt den Akku vor einer Überhitzung. Es ist also äusserst unwahrscheinlich, dass ein Handy zu brennen beginnt, nur weil es über Nacht mit der Stromversorgung verbunden ist.

### **Was allerdings beim Laden über Nacht passieren kann, ist, dass der Akku schneller altert.**

**Quelle:** <https://www.alao.ch/de/blogs/handy-ueber-nacht-laden-eine-gute-idee/>



## 2. Smartphone

### **Infowelt Energie: Ladekabel in der Steckdose verbraucht Strom, wissen Sie das?**

Sie kennen das sicher: Nach dem Aufladen des Smartphones bleibt das Ladegerät in der Steckdose. Es ist bequem, das Handy bei Bedarf einfach anstecken zu können und das Ladekabel nicht suchen zu müssen.

**Wir erklären, warum Sie das Kabel dennoch aus der Steckdose nehmen sollten.**

[Mit einer Kilowattstunde Strom](#) können Sie einmal die [Geschirrspülmaschine nutzen](#) oder 15 Hemden bügeln. Verbleibt das Ladekabel täglich über mehrere Stunden (auch ohne Handy) in der Steckdose, verbraucht das etwa 2,5 Kilowattstunden Strom im Jahr. Einzeln betrachtet ist das eine überschaubare Menge Strom. Mit Blick auf die gesamte Bevölkerung Deutschlands ergibt sich eine unglaubliche Summe, denn allein in Deutschland nutzen mittlerweile etwa 68 Millionen Menschen ein Smartphone. (Quelle: Statista)

**2,5 Kilowattstunden \* 68.000.000 Smartphones = 170.000.000 Kilowattstunden zusätzlicher Stromverbrauch im Jahr**

Das entspricht in der Summe also 170.000.000 Kilowattstunden. Mit diesem Verbrauch könnte man 170.000.000 Mittagessen für vier Personen kochen oder sich 85.000-mal rasieren. Ein deutscher Haushalt mit zwei Personen verbraucht im Durchschnitt etwa 3.100 kWh im Jahr.

**Mit dem Energieverlust durch Ladegeräte in der Steckdose könnten etwa 5.800 Zweipersonenhaushalte in Deutschland ein Jahr lang mit Strom versorgt werden. Diese Summe ergibt sich allein aus dem Stromverbrauch von Handyladegeräten.**



### 3. Smartphone, Tablet, PC: Achtung Brandgefahr

Ein Ladegerät permanent in der Steckdose zu lassen, verschwendet nicht nur Strom, sondern ist auch gefährlich. Denn einem Ladegerät sieht man von außen nicht an, ob es defekt ist. Vor allem bei billigen No-Name-Produkten ist die Brandgefahr besonders hoch.

#### Verbrauch senken (nicht nur) bei Smartphone & Laptop !

Wer zu faul ist, das Ladegerät täglich aus der Steckdose zu ziehen, für den gibt es ein paar hilfreiche Tipps. Am einfachsten vermeiden Sie zusätzliche Kosten, indem Sie eine Steckdosenleiste mit einem separaten **Kippschalter** nutzen. Den können Sie einfach ausschalten, wenn Sie die Wohnung verlassen. So wird nicht nur das Handyladegerät am Stromfressen gehindert, sondern auch alle anderen Geräte, die angeschlossen sind.



**Noch besser:**  
**Jeden Stecker**  
**einzeln**  
**ausschalten**



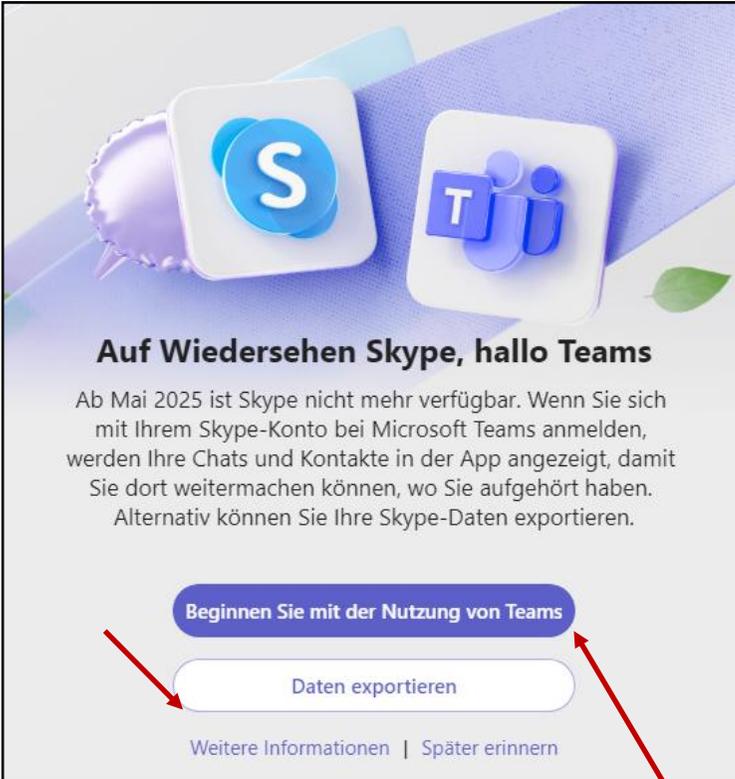
**Quelle Foto und Text:**

[https://www.vattenfall.de/infowelt-energie/energie-sparen/ladekabel-verbraucht-strom?utm\\_source=google&utm\\_medium=paid&utm\\_campaign=de\\_pmax\\_www-solar-solar-kompletanlage\\_pros\\_act\\_sd&gad\\_source=5&gad\\_campaignid=22432085747&gclid=EAlalQobChMI49OaisqOjQMVSKWDBx3auDcqEAAYASAAEgM6PD\\_BwE](https://www.vattenfall.de/infowelt-energie/energie-sparen/ladekabel-verbraucht-strom?utm_source=google&utm_medium=paid&utm_campaign=de_pmax_www-solar-solar-kompletanlage_pros_act_sd&gad_source=5&gad_campaignid=22432085747&gclid=EAlalQobChMI49OaisqOjQMVSKWDBx3auDcqEAAYASAAEgM6PD_BwE)



## 4. PC und Smartphone – Skype > Teams

Wer nach dem 05. Mai 2025 **Skype** öffnet, wird mit dieser Meldung darüber informiert, dass **Skype** nicht mehr zur Verfügung steht. Alternativ wird **Teams** angeboten von Microsoft.



Klicken Sie auf **Daten exportieren**, öffnet sich der Browser mit Infos von Microsoft.

Sie haben Fragen ? **Gewusst wie meine Skype-Daten exportieren oder löschen?** Die folgenden Informationen helfen Ihnen beim Exportieren oder Löschen bestimmter Skype-Inhalte.

Exportieren, Löschen oder Löschen von Nachrichten und Unterhaltungen	▼
Exportieren und Löschen von Aktivitäts- oder Diagnosedaten	▼
Exportkaufverlauf	▼
Exportieren des Verlaufs bezahlter Anrufe	▼
Exportieren und Löschen von Kontakten	▼
Löschen von Standortdaten	▼
Exportieren gemeldeter Benutzer	▼
Weitere Informationen zu <a href="#">wie lange Dateien und Daten in Skype verfügbar sind</a> .	

Hier klicken

Wenn Sie auf **Beginnen Sie mit der Nutzung von Teams** klicken, öffnet sich Teams und man kann sofort chatten.



## **4. PC und Smartphone: Chatten mit WhatsApp**

**Wie kann man noch viel einfacher chatten, als mit Teams?**

**Das geht gratis mit **WhatsApp**. Tipp: [Unser Vortrag Nr. 65 vom 03.06.2019](#)**

### **Sprach- und Videoanrufe**

Ob ein Gruppenanruf mit Klassenkamerad\*innen oder ein kurzes Telefonat mit Mama – mit Sprach- und Videoanrufen ist es so, als wären alle im selben Raum.

### **Unbekümmert sprechen**

Mit der Ende-zu-Ende-Verschlüsselung sind deine privaten Nachrichten und Anrufe geschützt. Das bedeutet, dass nur du und die Person, mit der du kommunizierst, die Konversation lesen bzw. hören könnt – und niemand dazwischen, nicht einmal WhatsApp.

### **In Kontakt bleiben mit deinen Gruppen**

Ganz gleich, ob du einen Ausflug mit Freund\*innen planst oder im Familienchat einfach nur auf dem Laufenden bleiben möchtest, Gruppengespräche sollten unkompliziert sein.

**Quelle:** [https://www.whatsapp.com/?lang=de\\_DE](https://www.whatsapp.com/?lang=de_DE)



## 5. PC: Ende des Supports für Windows 10, Windows 8.1 und Windows 7

**BSI empfiehlt Upgrade oder Wechsel des Betriebssystems nach Supportende von Windows 10** [BSI Bundesamt für Sicherheit in der Informationstechnik 14.04.2025](#)

**Zum 14. Oktober 2025** stellt Microsoft den Support für Windows 10 ein, u.a. in den Editionen Home, Pro und Education. **Das Betriebssystem erhält dann keine kostenlosen Updates mehr – auch solche nicht, die sicherheitsrelevant sind und z.B. Schwachstellen schließen.**

Allen, die noch Windows 10 nutzen, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI), rechtzeitig ein Upgrade durchzuführen bzw. auf ein anderes Betriebssystem umzusteigen. Das können etwa Windows 11, ein Unix-basiertes Betriebssystem wie macOS oder ein Linux-basiertes Betriebssystem sein. Nach dem Supportende veröffentlicht Microsoft voraussichtlich nur noch im Rahmen eines kostenpflichtigen Abonnements und für höchstens drei weitere Jahre kritische und wichtige Sicherheitsupdates.

**Wenn Ihr PC die [Mindestanforderungen](#) erfüllt, sollten Sie in den Einstellungen bei Windows Update eine Option für ein kostenloses Upgrade auf Windows 11 sehen. Wenn Ihr PC die Anforderungen für ein Upgrade auf Windows 11 **nicht erfüllt** oder wenn Sie ihn ersetzen möchten, können Sie auf Windows 11 umsteigen, indem Sie einen neuen PC kaufen. [Überprüfen Sie jetzt Ihre Einstellungen für Windows Update](#)  
>>>><https://www.microsoft.com/de-de/windows/end-of-support>**



## 5. PC: Eine Datensicherung erstellen in Windows 10 und 11

1. Klicken Sie auf die Windows-Suchleiste oder die Lupe.
2. Dort tippen Sie ‚Sicherheitseinstellungen‘ und klicken auf den gleichnamigen Eintrag.
3. Wählen Sie anschließend den Menüpunkt ‚Zu Sichern und Wiederherstellen (Windows 7) wechseln‘.  
Unter Windows 11 geben Sie in die Suche ‚Systemsteuerung‘ ein, wählen den Punkt aus und finden auch dort ‚Sichern und Wiederherstellen (Windows 7)‘.
4. Dort angekommen wählen Sie ‚Sicherheit einrichten‘.
5. Nun entscheiden Sie, wo Sie Ihre Datensicherung ablegen wollen und klicken schließlich ‚Weiter‘.  
Hierbei kann es sich zum Beispiel um eine externe Festplatte handeln. Das Speichermedium, auf das Sie Ihre Sicherheitskopien ablegen, sollte ausreichend viel Speicherplatz bereithalten. Das heißt, der Speicher sollte größer sein als der Speicher Ihres PC, wenn Sie alle Daten sichern möchten. Zudem sollten Sie das Speichermedium außerhalb des Sicherungsprozesses vom Gerät trennen und nur dann anstecken, wenn der Rechner sicher nicht infiziert ist, damit Schadsoftware oder Defekte nicht auch die Datensicherung schädigen.
6. Durch einen Klick auf ‚Auswahl durch Benutzer‘ entscheiden Sie selbst, welche Daten und Ordner gesichert werden. Stattdessen können Sie hier ‚Auswahl durch Windows‘ wählen und überlassen Windows die Entscheidung.
7. Wählen Sie nun, welche Daten oder Laufwerke eine Sicherungskopie erhalten und klicken Sie erneut ‚Weiter‘.
8. Mit einem Klick auf ‚Zeitplan ändern‘ legen Sie fest, wann und wie häufig Windows von diesen Dateien Sicherungskopien erstellt.
9. Wenn Sie alles eingestellt haben, ‚Einstellungen speichern und Sicherung ausführen‘.



## 6. PC Datenverlust

Die Gefahren für Ihre Daten sind vielzählig und reichen von Kurzschlüssen bis hin zu Softwaremängeln. Einer der Klassiker, der für Datenverlust verantwortlich zu machen ist, ist das nicht vollständige Herunterfahren des Computers. Wenn durch einen Stromausfall oder aus Ungeduld die Energiezufuhr einfach gekappt wird, können Schreibprozesse nicht beendet und Informationen nicht hinterlegt werden.

**Für eine langfristige Datensicherung empfiehlt sich eine Externe Festplatte, mit 1 bis 4 TB, je nach Menge der zu sichernden Datenmenge.**

Quelle: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/datensicherung-und-datenverlust\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/datensicherung-und-datenverlust_node.html)

So mancher Fehler lässt sich durch einen simplen Neustart des Betriebssystems bei eingeschaltetem PC beheben. Sie können unsere Anleitung kostenlos Herunterladen auf unserer Homepage auf der Seite DOWNLOADS: **Neustart des PC.pdf**

### Wie viel macht 1 GB auf MB und KB?

1 Bit

1 Byte = 8 Bit

1 Kilobyte (KB) = 1024 Byte

1 Megabyte (MB) = 1024 KB = 1 048 576 Byte

1 Gigabyte (GB) = 1024 MB = 1 048 576 KB

1 Terabyte (TB) = 1024 GB

MegaByte (MB) in GigaByte (GB) umrechnen:

<https://www.online-rechner.net/datenmenge/mb-gb/>



## 7. PC: Das Programm mrt - Was ist das?

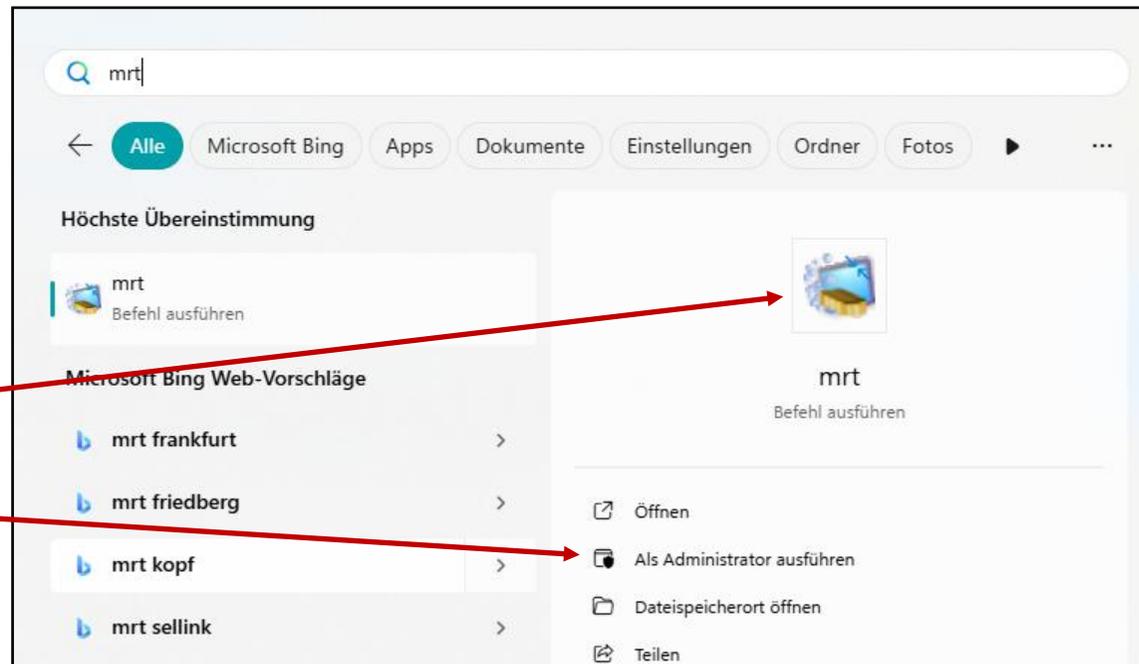
Das ist ein Microsoft Windows-Tool zum Entfernen bössartiger Software.

Es sind sich viele Nutzer gar nicht darüber im Klaren, dass ihre Windows-Installation neben dem eigens aufgespielten Antiviren-Programm (oder dem [Defender](#)) einen zweiten Antivirus beherbergt: das "Microsoft Windows-Tool zum Entfernen bössartiger Software". Man nennt das Utility auch MRT/mrt oder mrt.exe. Der Aufruf gelingt, indem Sie die Windows-Taste und R drücken und den Befehl *mrt* eingeben.

### So geht's:

Schreiben Sie ins Suchfeld in der Taskleiste **mrt** ein, bestätigen mit OK, dann geht dieses Fenster auf.

Klicken Sie **hier**,  
oder auf  
**Als Administrator ausführen**.

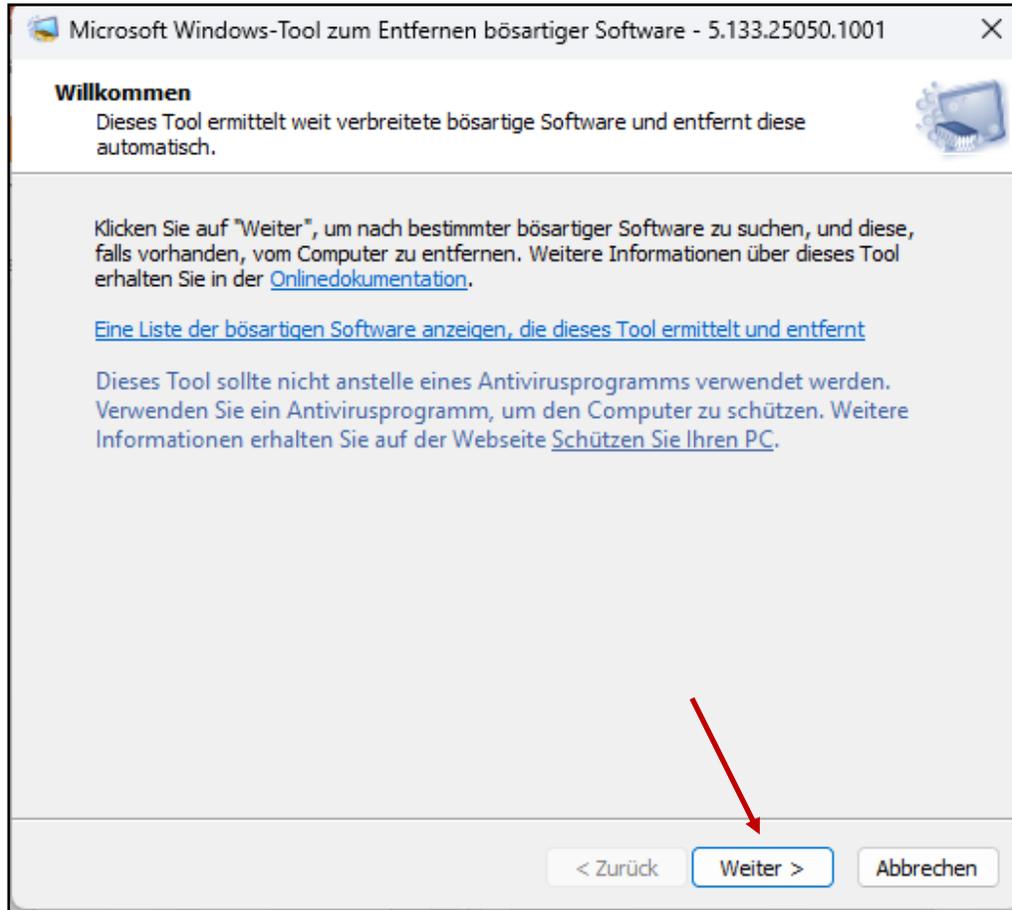


<https://www.computerbild.de/artikel/cb-Tipps-Windows-mrt.exe-Microsoft-Windows-Entfernen-viren-39636641.html>

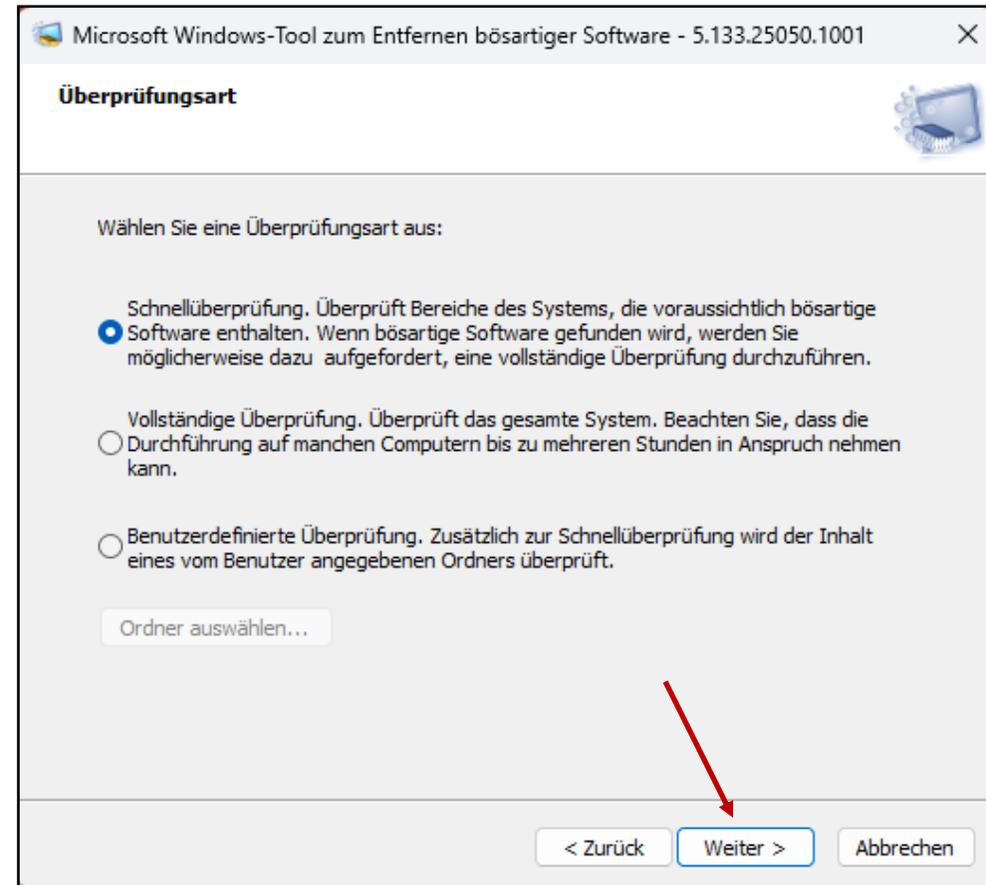


## PC: mrt

### mrt wurde gestartet – auf Weiter klicken



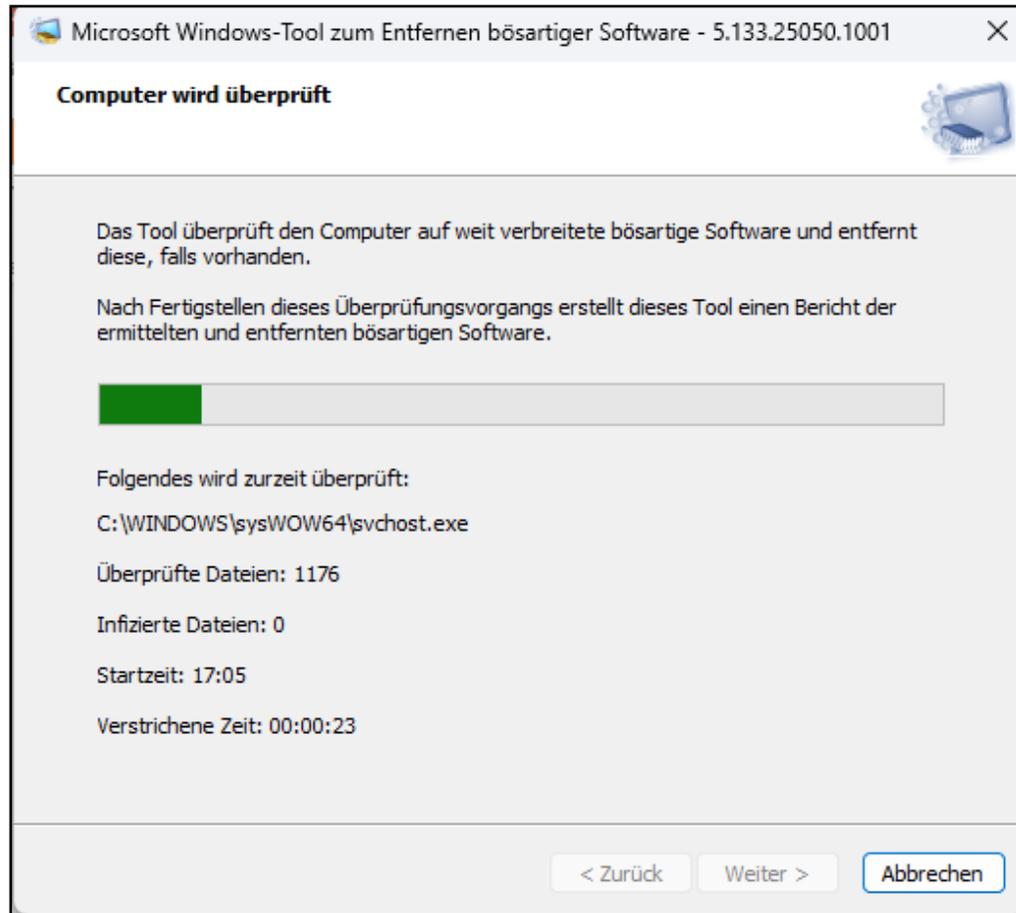
### auf Weiter klicken



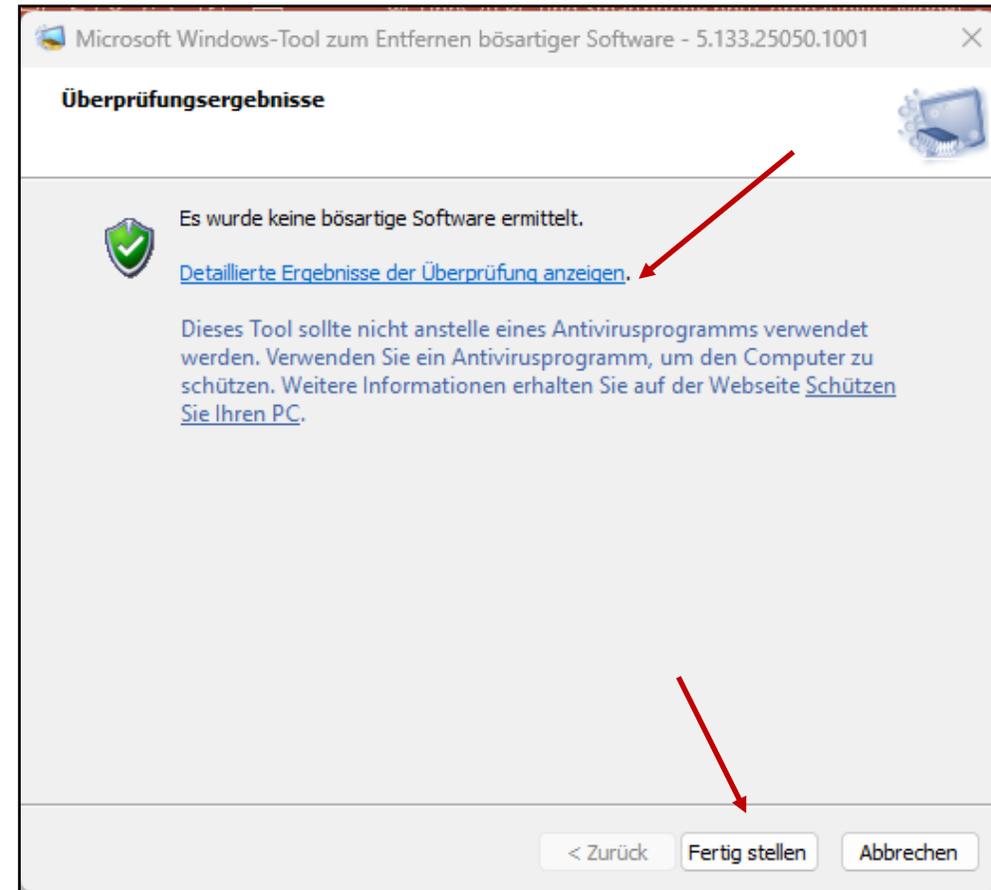


## PC: mrt

### Der Computer wird überprüft



### Das Ergebnis wird angezeigt Auf **Fertig stellen** klicken



Zur Startseite



## 8. Tipps vom BSI: Bundesamt für Sicherheit und Informationstechnik.

Beim BSI finden Sie zu diesen Themen:

→ [Basistipps zur IT-Sicherheit](#)

- Schützen Sie Ihre Online- und Benutzerkonten mit sicheren Passwörtern
- Vergeben Sie für jedes Online- und Benutzerkonto ein eigenes, sicheres Passwort und ändern Sie schnellstmöglich alle Passwörter, wenn diese in falsche Hände geraten sein könnten.
- Ändern Sie auch die von den Herstellern oder Diensteanbietern voreingestellten Passwörter nach der ersten Nutzung.
- Kriterien gelten für ein sicheres Passwort: Je länger das Passwort ist, desto besser.
- Klick auf diesen Link [Tipps zur](#) Mehr Sicherheit für Online-Konten und vernetzte Geräte → [„Zwei-Faktor-Authentisierung“](#)
- Seien Sie vorsichtig bei E-Mails und deren Anhängen
- Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten
- Fertigen Sie regelmäßig Sicherheitskopien an

BSI: Bundesamt für Sicherheit und Informationstechnik.

→ [Sicherheitsirrtümer](#)

- 1. [Sicherheits-Irrtümer: Internet-Sicherheit](#)
- 2. [Sicherheits-Irrtümer: Mobile Sicherheit](#)
- 3. [Sicherheits-Irrtümer: Computer-Sicherheit](#)
- 4. [E-Mail-Sicherheit: Mythen im Faktencheck](#)



## 9. Alle kostenlosen Vorträge können Sie herunterladen unter: [www.stsr-heidenheim.de](http://www.stsr-heidenheim.de) auf der Seite **DOWNLOADS**

Alle bereits gehaltenen kostenpflichtigen Vorträge können Sie gegen einen kleinen Unkostenbeitrag von 2 € je Vortrag auch nachträglich als pdf-Datei erhalten. Kontaktieren Sie die Internetlotsen.

Eine Übersicht aller Vorträge erhalten Sie auf unserer Homepage auf dieser Seite:



Das [Team](#) der ehrenamtlichen Internetlotsen steht Ihnen mit neutraler Beratung und Unterstützung jeden Montag von 10-12 Uhr zur Seite, bei offenen Treffpunkten in den Räumen des Bürgerhauses Heidenheim im 1.OG, Raum 102+103 (außer in den Ferien und an Vortrags-Terminen) Infos unter [www.stsr-heidenheim.de](http://www.stsr-heidenheim.de) auf der Seite → **TERMINE**

Bringen Sie Ihren Laptop, Smartphone oder Tablet mit, wenn Sie Unterstützung und Hilfe benötigen. Wir bieten auch Hilfe bei der Einrichtung neuer Geräte an, sowie Installation von Programmen. Wir freuen uns, Sie im Bürgerhaus begrüßen zu dürfen.  
Ohne Anmeldung - einfach kommen!

**Vielen Dank für Ihre Aufmerksamkeit**