



Digitale Schule
der Zukunft

Pilotversuch DSDZ

Einrichtung von digitalen Endgeräten mit Windows
Informationen zur IT-Sicherheit

Agenda

- Sichere Konfiguration
- Möglichkeiten der Kontrolle und Überwachung
- Datensicherung
- Virens Scanner und Co.
- Rund um das Passwort
- Vorsicht bei Mail, Messengern und Web
- Tipps zum Weiterlesen



Sichere Konfiguration

Das Betriebssystem Windows einrichten

Windows Sicherheit

Windows 10

The screenshot shows the Windows 10 Settings application. The left sidebar is titled 'Einstellungen' and includes 'Startseite', a search bar 'Einstellung suchen', and a list of categories under 'Update und Sicherheit': Windows Update, Übermittlungsoptimierung, Windows-Sicherheit, Sicherung, Problembehandlung, Wiederherstellung, Aktivierung, and Mein Gerät suchen. The main content area is titled 'Windows-Sicherheit' and contains the following text: 'Windows-Sicherheit ist Ihr zentraler Anlaufpunkt, über den Sie die Sicherheit und Integrität Ihres Geräts überprüfen und verwalten können.' Below this is a button 'Windows-Sicherheit öffnen'. Under the heading 'Schutzbereiche', there are six items: Viren- & Bedrohungsschutz (Keine Maßnahmen erforderlich.), Kontoschutz (Maßnahmen empfohlen.), Firewall & Netzwerkschutz (Keine Maßnahmen erforderlich.), App- & Browsersteuerung (Keine Maßnahmen erforderlich.), and Gerätesicherheit (Keine Maßnahmen erforderlich.).

Windows 11

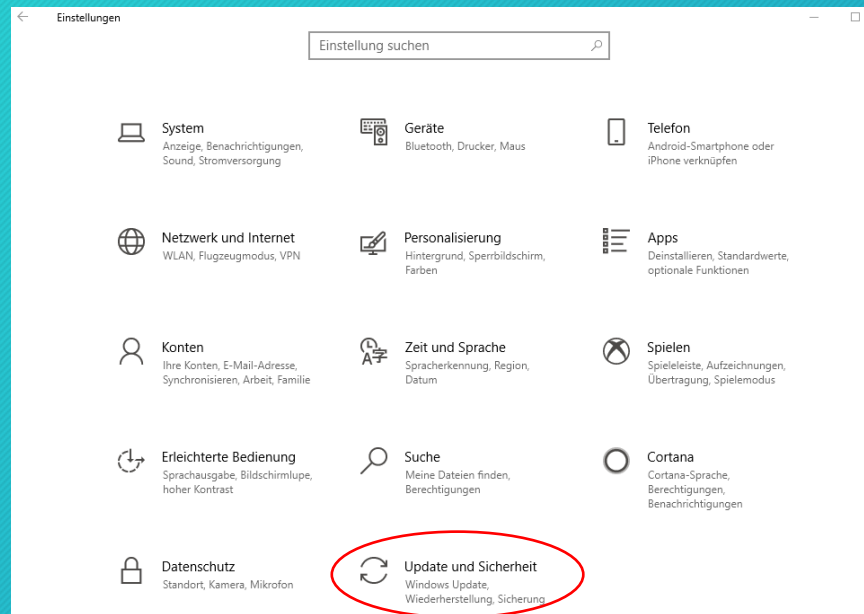
The screenshot shows the Windows 11 Settings application. The top left shows the user profile 'Bernd Lemaczyk' and a search bar 'Einstellung suchen'. The left sidebar lists categories: System, Bluetooth und Geräte, Netzwerk und Internet, Personalisierung, Apps, Konten, Zeit und Sprache, Spielen, Barrierefreiheit, 'Datenschutz und Sicherheit' (highlighted), and Windows Update. The main content area is titled 'Datenschutz und Sicherheit > Windows-Sicherheit' and contains the following text: 'Windows-Sicherheit ist Ihr zentraler Anlaufpunkt, über den Sie die Sicherheit und Integrität Ihres Geräts überprüfen und verwalten können.' Below this is a button 'Windows-Sicherheit öffnen'. Under the heading 'Schutzbereiche', there are seven items: 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.), Geräteleistung & -integrität (Stellt Berichte zur Integrität Ihres Geräts bereit.), and Familienoptionen (Verwalten Sie, wie Ihre Familie die Geräte verwendet.).

Windows-Updates: Sicherheitslücken schließen

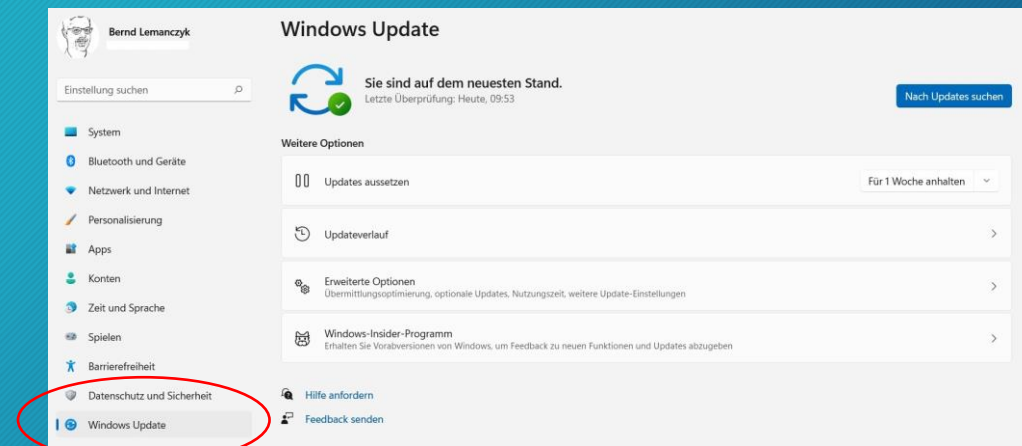
- Microsoft hat mindestens einmal pro Monat größere Updates, oft mit Sicherheitsbezug. Updates werden automatisch gesucht und - je nach Konfiguration- eingespielt.
- Sicherheitshalber auch manuell nach Updates suchen.
- IMMER die neuesten Updates rasch einspielen!
- Auch bei Anwendungen automatisch die neusten Updates installieren lassen.
- Bei Meldungen wegen Updates in Pop-Up-Fenstern trotzdem misstrauisch bleiben: ist das, was es zu sein vorgibt?

Windows Updates

Windows 10



Windows 11



Möglichkeiten der Kontrolle und Überwachung

Wie können Eltern sehen und ggf. beschränken, was ihr Kind auf dem Rechner macht?

Gibt es eine Pflicht zur Kontrolle?

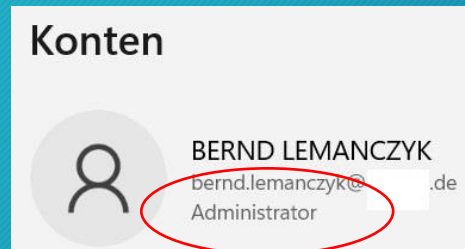
Urteil des BGH vom 15.11.2012 / I ZR 74/12

Sinngemäß: Eltern müssen ihre Kinder altersgemäß belehren und ihnen die Nutzung rechtswidriger Dienste untersagen. Das ist ausreichend, wenn die Kinder derartige Anweisungen der Eltern in der Regel befolgen.

Wenn Eltern Anhaltspunkte dafür haben, dass das Kind solche Regeln nicht befolgen könnte, müssen sie die Aktivitäten des Kindes einschränken bzw. überprüfen.

Die Basis: Keine Adminrechte

- Windows 10 bzw. 11 kennt „normale“ Benutzer und Systemadministratoren. Damit die Kinder nicht alles machen können ist es sehr wichtig, dass nur die Eltern das Administratoren-Passwort haben.
- Unter Einstellungen -> Konten sieht das so aus:



- Unter Einstellungen -> Konten -> Familie & andere Benutzer können Konten für Kinder hinzugefügt und individuell konfiguriert werden

Familienmitglied hinzufügen

- Windows 10

The screenshot shows the Windows 10 Settings application. The left sidebar is open to 'Einstellungen' (Settings), with 'Familie & andere Benutzer' selected. The main pane displays 'Familie & andere Benutzer' with a sub-section 'Ihre Familie'. Below this, there is a '+ Familienmitglied hinzufügen' button and a link for 'Weitere Informationen'. Under 'Andere Benutzer', there is a description and a 'Weiteren Benutzer hinzufügen' button. Overlaid on the right is a 'Microsoft-Konto' dialog box with the title 'Jemanden hinzufügen'. It contains an input field for an email address and a link to create an account for minors.

- Windows 11

The screenshot shows the Windows 11 Settings application. The left sidebar is open to 'Einstellungen', with 'Konten' selected. The main pane displays 'Konten > Familie & andere Benutzer'. Under 'Ihre Familie', there is a description and a 'Weiteren Benutzer hinzufügen' button. Below this, there is a 'Weiteren Benutzer hinzufügen' button. At the bottom, a user profile for 'Andrea' is partially visible.

Schulkonto hinzufügen

Windows 10

The screenshot shows the Windows 10 Settings application. The left sidebar is open to 'E-Mail und Konten'. The main content area is titled 'E-Mail und Konten' and contains the following elements:

- Section: 'Von E-Mail, Kalender und Kontakten verwendete Konten'
- Button: '+ Konto hinzufügen'
- Account card: 'bernd.lemanczyk@...de' with an envelope icon.
- Section: 'Von anderen Apps verwendete Konten'
- Text: 'Fügen Sie hier die für Ihre Apps verwendeten Konten hinzu, und melden Sie sich einfacher und schneller bei Ihren bevorzugten Apps an.'
- Links: 'Microsoft-Konto hinzufügen' and 'Geschäfts- oder Schulkonto hinzufügen'
- Account card: 'bernd.lem' with the Microsoft logo and 'Microsoft-Konto'.

Windows 11

The screenshot shows the Windows 11 Settings application. The left sidebar is open to 'Konten > E-Mail und Konten'. The main content area is titled 'Konten > E-Mail und Konten' and contains the following elements:

- Section: 'Von E-Mail, Kalender und Kontakten verwendete Konten'
- Button: 'Neues Konto hinzufügen' (with a blue 'Konto hinzufügen' button on the right)
- Account card: 'bernd.lem' with an envelope icon.
- Account card: 'bernd.lemanczyk@...de' with an envelope icon.
- Section: 'Von anderen Apps verwendete Konten'
- Text: 'Konten hinzufügen' with links for 'Microsoft-Konto hinzufügen' and 'Geschäfts- oder Schulkonto hinzufügen'
- Account card: 'bernd.lem' with the Microsoft logo and 'Microsoft-Konto'.
- Account card: 'bernd.lemanczyk@gymnasium-kirchheim.de' with the Microsoft logo and 'Geschäfts- oder Schulkonto'.

Einrichtung und Funktionen von Microsoft Family

- Zur Einrichtung einer Microsoft-Familiengruppe muss ein Erwachsener über ein Microsoft-Konto verfügen.
- Nach der Einrichtung sind u.a. folgende Funktionen verfügbar:
 - Aktivitätsberichte abrufen oder automatisch per Mail schicken lassen
 - Planung und Beschränkung von Bildschirmzeiten
 - Festlegung von Inhaltsbeschränkungen (z.B. Apps, Spiele, Medien, Webfilter)
 - Funktion“Erziehungsberechtigte fragen“
 - Verwaltung von Einkäufen und Ausgaben im Microsoft Shop
- Informationen zur Einrichtung und den Möglichkeiten von Microsoft Family: <https://support.microsoft.com/de-de/account-billing/erste-schritte-mit-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344>

Fazit zu Microsoft Family

Vorteile

- Kontrolle und ggf. Beschränkung der Bildschirmzeit
- Kontrolle und ggf. Einschränkung der Aktivitäten
- Microsoft Family Safety App (für Android & iOS)
- Erfüllung der Aufsichtspflicht

Nachteile

- Microsoft-Konto zwingend erforderlich
- Totale Überwachung
- Nur Microsoft-Browser können kontrolliert werden

MS Teams: unterschiedliche Versionen



Microsoft Teams auf den Windows-Desktop herunterladen

Teams für zu Hause oder kleine Unternehmen

Teams herunterladen



Teams für Beruf, Schule und Studium

Teams herunterladen



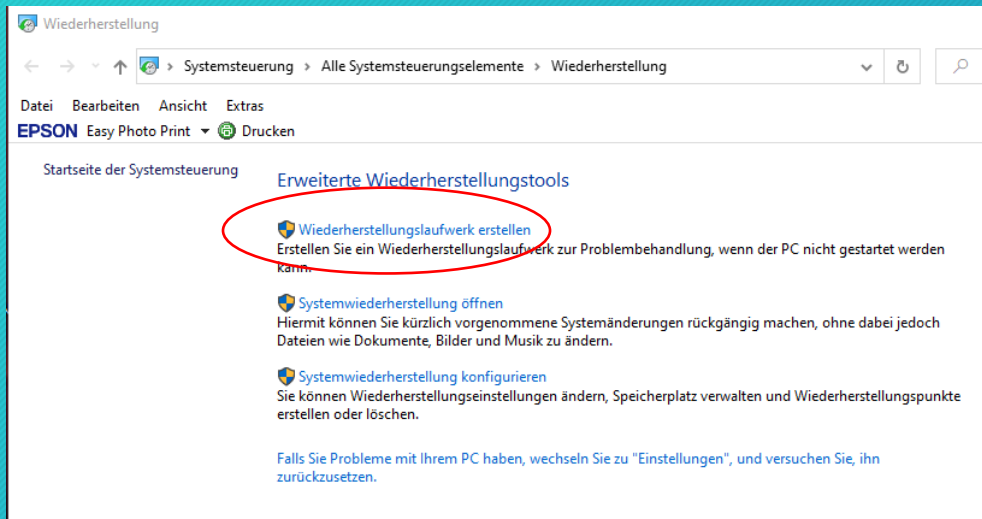
Datensicherung

Systemdaten sichern

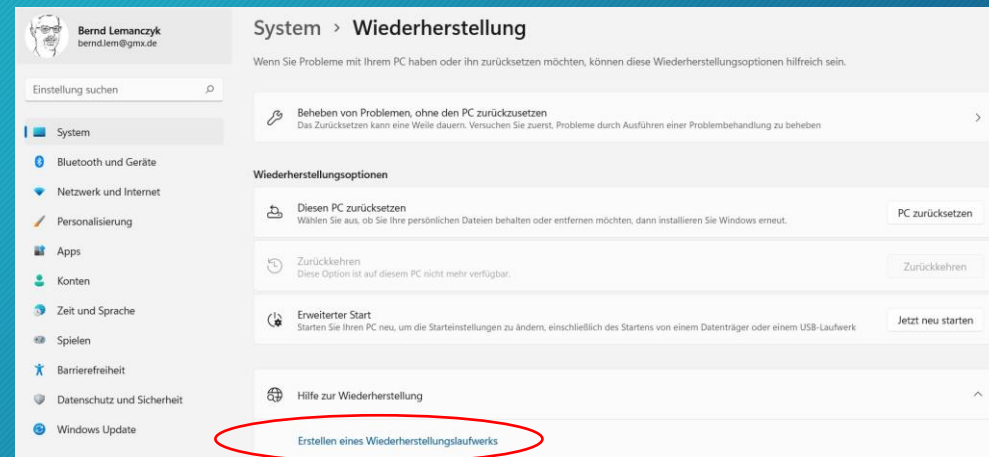
- Hier geht es darum, das Betriebssystem wieder erhalten zu können.
- Diese Option ist etwas versteckt - Sie suchen nach „Wiederherstellung“

Systemdaten sichern (Wiederherstellung)

Windows 10



Windows 11

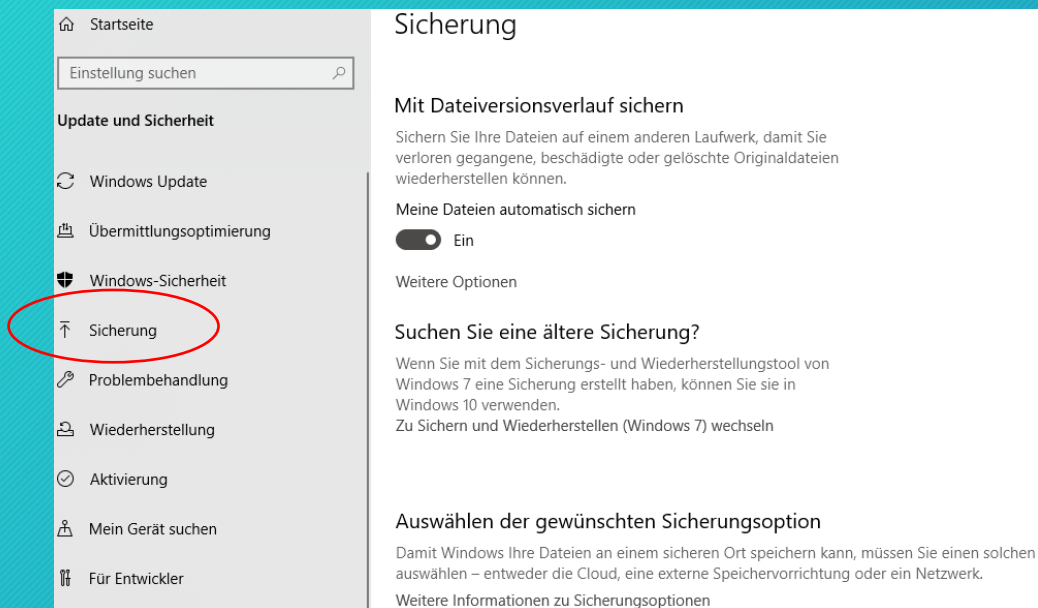


Nutzerdaten sichern

- Kann Windows automatisch machen
- Zusätzlich: in einzelnen Anwendungen einstellen (bei den Office-Anwendungen aber nur in der Cloud möglich)
- Beim Abspeichern in einer Cloud (z.B. OneDrive) gibt es automatisch eine Sicherung.
- Zusätzlich möglich: Datensicherung-Software und manuelle Sicherung auf eine Festplatte, die man an einem anderen Ort unterbringt

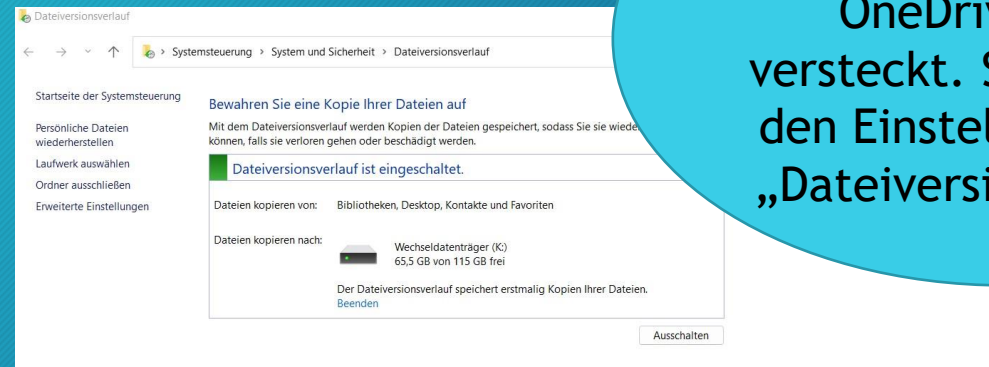
Nutzerdaten sichern

Windows 10



The screenshot shows the Windows 10 Settings application. The left sidebar is visible, with the 'Sicherung' (Backup) option highlighted by a red circle. The main content area shows the 'Sicherung' settings page, which includes sections for 'Mit Dateiversionsverlauf sichern', 'Meine Dateien automatisch sichern', 'Suchen Sie eine ältere Sicherung?', and 'Auswählen der gewünschten Sicherungsoption'.

Windows 11

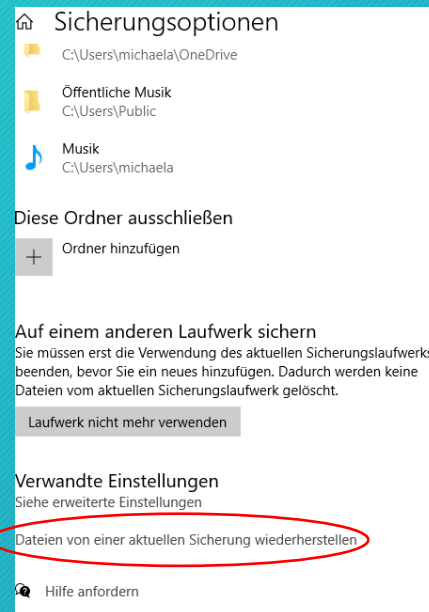


The screenshot shows the Windows 11 Settings application, specifically the 'Dateiversionsverlauf' (File History) settings page. The page is titled 'Dateiversionsverlauf' and shows the 'Dateiversionsverlauf ist eingeschaltet' (File History is on) status. It includes options for 'Dateien kopieren von' (Copy files from) and 'Dateien kopieren nach' (Copy files to). The 'Dateien kopieren nach' section shows a storage device with 65.5 GB free out of 115 GB. There is an 'Ausschalten' (Turn off) button at the bottom right.

In Windows 11 ist die Datensicherung ohne OneDrive etwas versteckt. Suchen Sie in den Einstellungen nach „Dateiversionsverlauf“.

Gesicherte Daten wiederherstellen

Windows 10



Sicherungsoptionen

- C:\Users\michaela\OneDrive
- Öffentliche Musik
C:\Users\Public
- Musik
C:\Users\michaela

Diese Ordner ausschließen

+ Ordner hinzufügen

Auf einem anderen Laufwerk sichern

Sie müssen erst die Verwendung des aktuellen Sicherungslaufwerks beenden, bevor Sie ein neues hinzufügen. Dadurch werden keine Dateien vom aktuellen Sicherungslaufwerk gelöscht.

Laufwerk nicht mehr verwenden

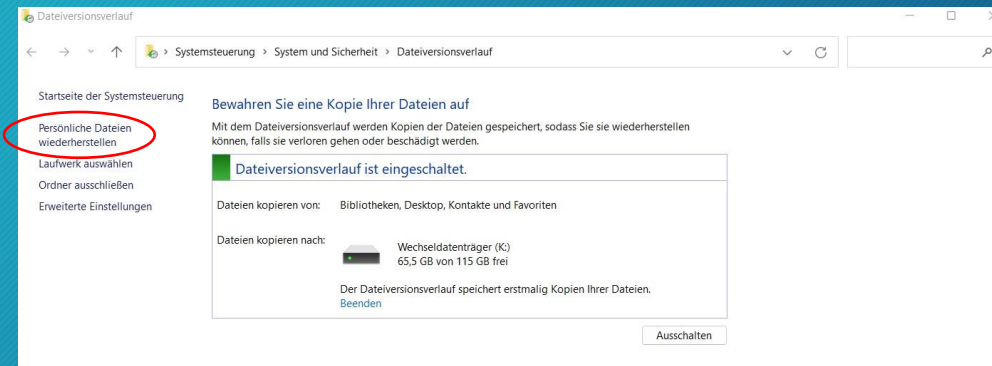
Verwandte Einstellungen

Siehe erweiterte Einstellungen

Dateien von einer aktuellen Sicherung wiederherstellen

Hilfe anfordern

Windows 11



Dateiversionsverlauf

Systemsteuerung > System und Sicherheit > Dateiversionsverlauf

Startseite der Systemsteuerung

Persönliche Dateien wiederherstellen

Laufwerk auswählen
Ordner ausschließen
Erweiterte Einstellungen

Bewahren Sie eine Kopie Ihrer Dateien auf

Mit dem Dateiversionsverlauf werden Kopien der Dateien gespeichert, sodass Sie sie wiederherstellen können, falls sie verloren gehen oder beschädigt werden.

Dateiversionsverlauf ist eingeschaltet.

Dateien kopieren von: Bibliotheken, Desktop, Kontakte und Favoriten

Dateien kopieren nach: Wechseldatenträger (K:) 65,5 GB von 115 GB frei

Der Dateiversionsverlauf speichert erstmalig Kopien Ihrer Dateien.

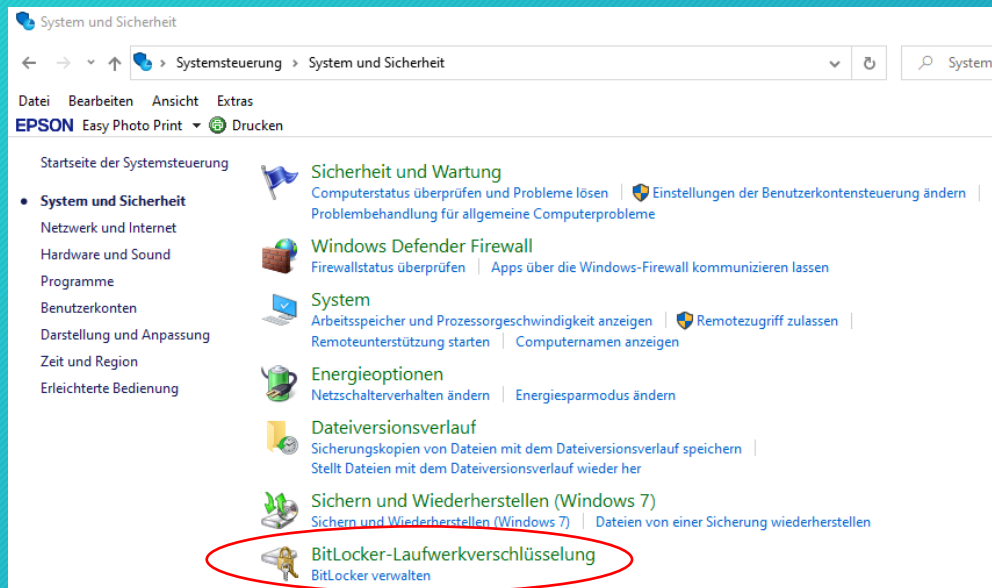
Beenden

Ausschalten

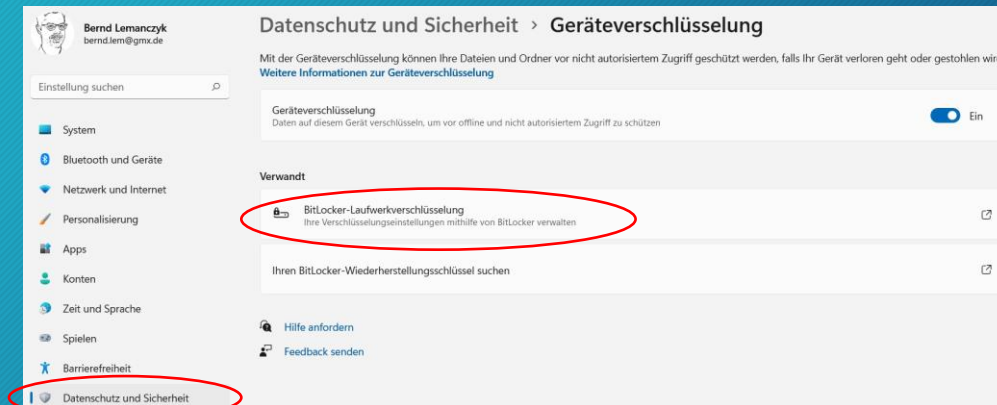
Laufwerksverschlüsselung

Vor allem bei mobilen Geräten ist es wichtig, die Laufwerksverschlüsselung einzuschalten. So kann niemand Ihre Daten lesen, wenn das Gerät abhanden kommt.

Windows 10



Windows 11



Virensscanner und Co.

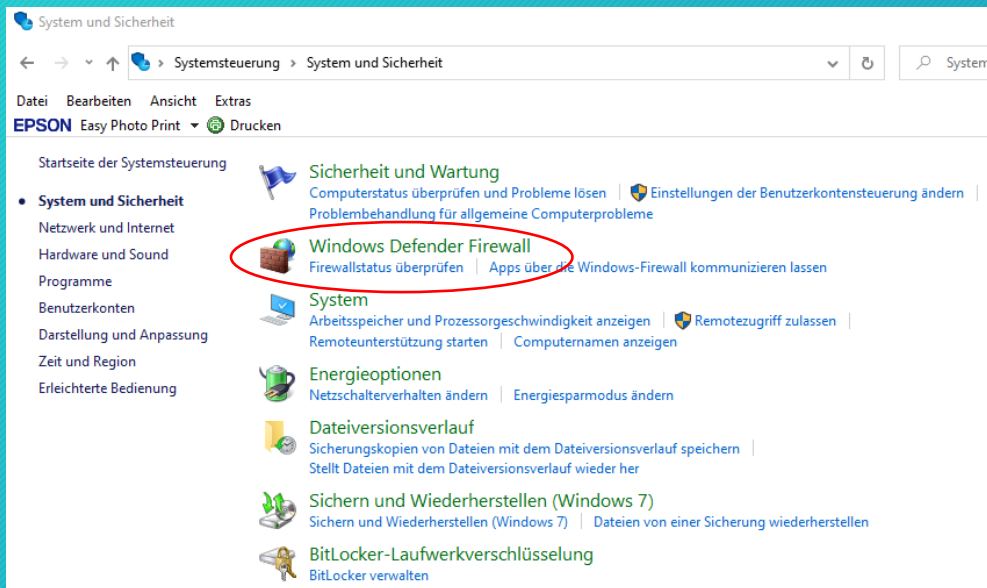
Brauche ich sowas? Helfen die noch?

Warum Virens Scanner und Firewall?

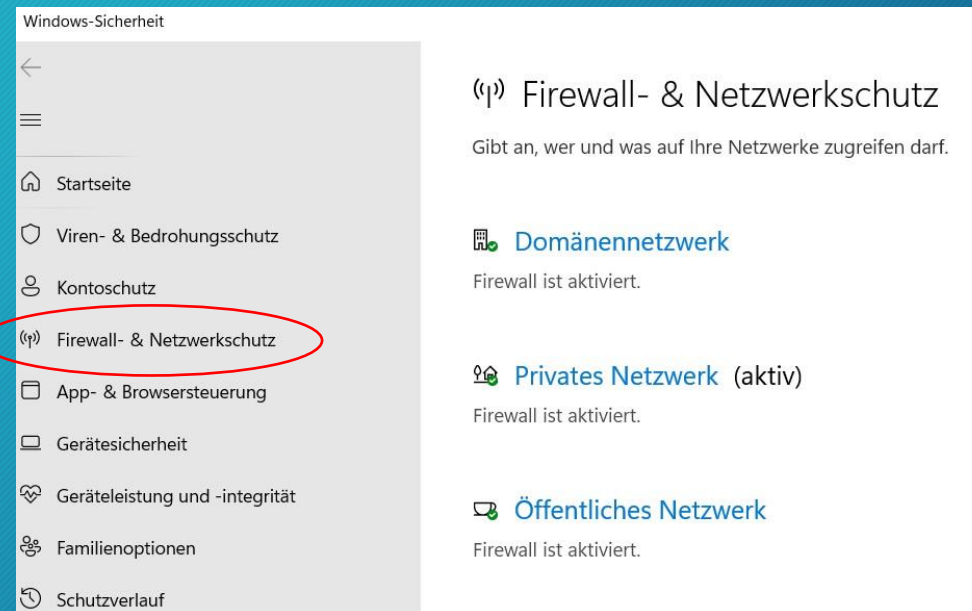
- Dateien und Anwendungen können laufend und aktuell auf Schadsoftware überprüft werden
- Eine Firewall auf dem Rechner kann unbefugte Zugriffe von innen und außen unterbinden (z.B. Verwendung Ihres Rechners für Bot-Netzwerke)
- Einfachste Lösung: Windows Defender (Bestandteil von Windows)
- Alternativ: Kostenfreie Virens Scanner (Antivir, Norton etc.)
- Lösung für sehr vorsichtige Nutzer: kostenpflichtige Virens Scanner

Firewall (Defender; in Windows integriert)

Windows 10



Windows 11



Rund um das Passwort

..denn leider geht es nicht ohne

Rund um das Passwort

- Passwörter müssen vor allem LANG sein und am besten Groß- und Kleinbuchstaben, Ziffern und Satzzeichen erhalten.
- Passwörter nicht mehrfach verwenden. Denn: ist ein Passwort bekannt, sind mehrere Zugänge offen!
- Im Netz kursieren Sammlungen gehackter Konten und Passwörter - bei denen, die bekannt wurden, kann man testen, ob die eigenen dabei sind!

Rund um das Passwort - Ein Beispiel

- Als relativ sicheres und gleichzeitig nicht allzu schwer zu merkendes Passwort kann man eine Passphrase verwenden
- Beispiel: Aus den Anfangsbuchstaben des Satzes „Die Axt im Haus ersetzt den Zimmermann“ wird das Passwort DAiHedZ
- Durch Verwendung von Satzzeichen kann die Sicherheit deutlich gesteigert werden: DA.iHedZ?!
- Noch sicherer wird das Passwort, wenn bestimmte Buchstaben durch Zahlen ersetzt werden: DA.1Hed3?!




Nutzerkonten	Leaks	Geleakte Accounts pro Tag
10.244.979.113	992	1.100.487

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

 Bitte geben Sie hier Ihre E-Mail-Adresse ein.

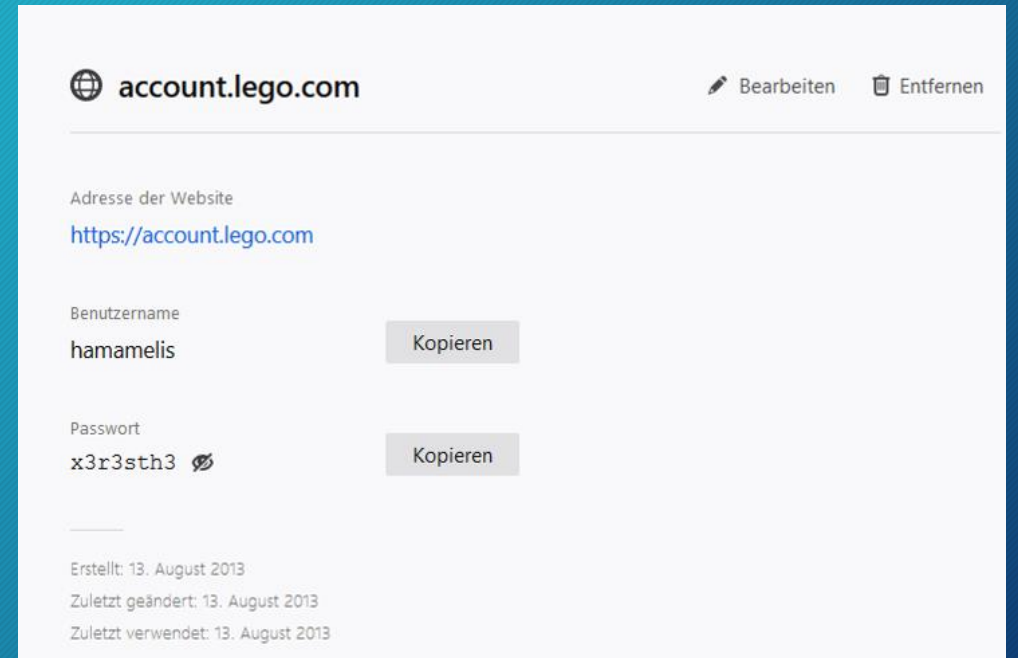
Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

E-Mail-Adresse prüfen!

Auf dieser Webseite können Sie prüfen, ob Daten in Zusammenhang mit Ihrer E-Mail-Adresse bekannt wurden.
Das Ergebnis wird an Ihre E-Mail versendet.

Sie speichern Passwörter im Browser?

- Diese Passwörter sind im Klartext abrufbar
- Wenn Sie irgendein Sicherheitsproblem am Rechner haben, sind ALLE Accounts, deren Passwörter Sie im Browser gespeichert haben, kompromittiert!



Was ist mit Identifikation über google oder facebook?

- Man kann sich mit der google- oder facebook-Identität bei vielen Shops oder anderen Webseiten authentisieren.
- Jede dieser Verbindungen zwischen Anbieter und Ihnen steht dann google oder facebook für deren Zwecke zur Verfügung.
- Sie können dieser Authentisierung soweit vertrauen, wie Sie google oder facebook vertrauen.
- Express-Einkauf per Paypal ohne weitere Authentisierung ist o.k., wenn Sie ohnehin über Paypal bezahlt hätten.

Wie merkt man sich 200 Passwörter?

- Gar nicht. Verwenden Sie einen Passwort-Manager.
- Solche Programme gibt es oft bei Sicherheits-Software wie Virens Scanner oder kostenfrei wie Bitwarden oder KeePass.
- Idealerweise mit 2-Faktor-Authentisierung.
- Wahl: Cloud-Lösung oder offline
- Wenn offline: bei Ausmustern des Rechners Festplatte SICHER löschen (mindestens 7mal überschreiben)
- Excel-Tabellen mit Passwortsicherung sind keine Alternative!

Vorsicht bei Mail, Messengern und Webseiten

...denn dort erhält man manchmal Dateien, die man bestimmt nicht wollte!

Mail: Betrug durch direkte Ansprache

- Inhalte auch von bekannten Adressaten hinterfragen
- Vorsicht bei allen Forderungen nach Geld, auch wenn diese von Vorgesetzten, Freunden, bekannten Organisationen etc. kommen!
- Vorsicht auch bei halb-anonymen Geldtransfer-Methoden wie z.B. Moneygram und natürlich Bitcoin-Zahlungen



Mail: Betrug durch Phishing

- Phishing ist Abfangen von Daten meist durch Umleiten auf gefälschte Webseiten
- Ganz klassisch: Zustimmung zu neuen AGB, DSGVO o.ä.
- Seit Einführung der 2-Faktor-Authentisierung im Banking werden vermehrt Bestellinfos für Shops abgegriffen.

Sehr geehrter Kunde,
Unsere AGB haben sich geändert. Bitte besuchen Sie daher unsere Webseite mit untenstehendem Link und stimmen Sie diesen zu. Sie müssen sich dabei einmal durch Angabe Ihrer Kundennummer und Passwort identifizieren.

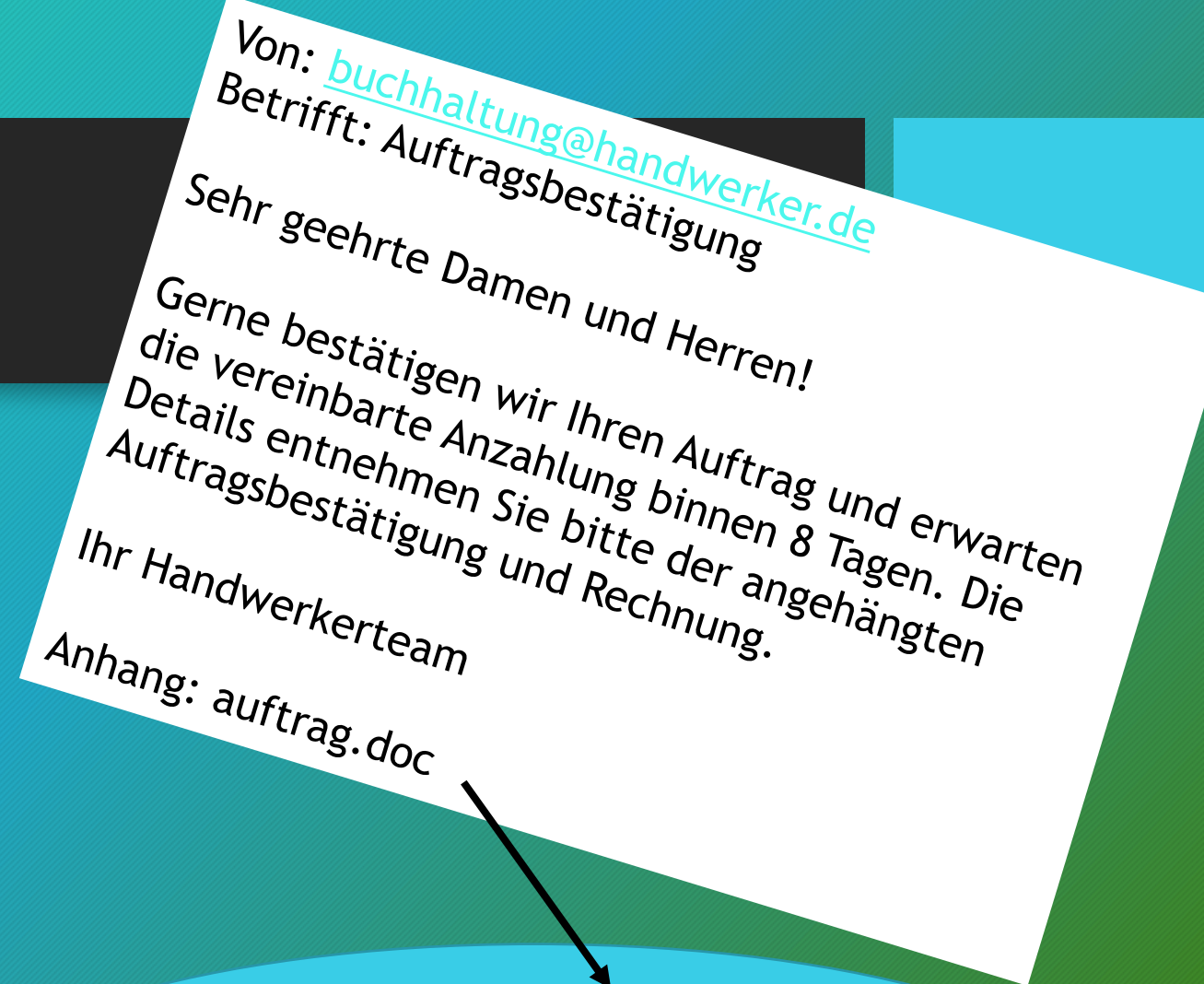
<http://ihr-shop.de/agb>

Mit freundlichen Grüßen
Ihr Serviceteam

Hinter dem Link versteckt sich aber:
<http://betrugsseite.bla.blubb.nz/irgendwas.html>

Infektion durch Dateianhänge

- In vielen Dateitypen kann man kleine Schadprogramme verstecken. Wenn Sie die Datei öffnen, wird das Schadprogramm ausgeführt.
- Besonders beliebt sind Word- und PDF-Dateien, wobei sich oft andere Dateitypen dahinter verbergen.
- Das funktioniert auch bei Dateien, die per Messenger geschickt werden, EGAL WIE SICHER DER MESSENGER IST!



In der Word-Datei ist aber ein Virus versteckt, der sich in Ihrem Rechner einnistet und demnächst Daten abzieht.

Vorsichtsregeln bei Mail

- Anhänge und Links nur öffnen, wenn diese von bekannten, vertrauenswürdigen Absendern kommen und die gesamte Mail Sinn macht.
- Wenn da etwas komisch aussieht: den Absender auf einem anderen Kanal (Messenger, Telefon) fragen, ob die Mail mit den Anhängen von ihm stammt.
- Aufforderung von angeblich offiziellen Stellen erst kritisch hinterfragen: kann das von dort kommen? Kennen die meine Mailadresse?
- Testen Sie doch mal bei:
<https://www.heise.de/security/dienste/Emailcheck-2109.html>

Vorsichtsregeln beim Surfen

- Seiten, auf denen man Finanztransaktionen vornimmt (Banking, Bestellungen) nur durch direkte (korrekte) Eingabe des Links bzw. durch Nutzen eines bewährten Bookmarks ansurfen. Betrüger nutzen oft ähnliche Links, um Daten abzugreifen.
 - Statt „abc-muenchen-bank.de“ -> „abc-mienchen-bank.de“
- Browser so konfigurieren, dass ein mittleres Sicherheitslevel eingeschaltet ist.
 - Sog. „aktive Inhalte“ einschränken
- Verwenden Sie alternative Browser (firefox, opera, chrome)
 - Viele Angriffe sind auf Microsoft-Browser abgestimmt

Sicherheit

Schutz vor betrügerischen Inhalten und gefährlicher Software

- Gefährliche und betrügerische Inhalte blockieren [Weitere Informationen](#)
- Gefährliche Downloads blockieren
- Vor unerwünschter und ungewöhnlicher Software warnen

Zertifikate

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt

- Automatisch eins wählen
- Jedes Mal fragen
- Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Ausschnitt aus den
Einstellungen zur
Sicherheit im Browser
„Firefox“

Browsercheck

Java	JavaScript/JScript	Visual Basic Script
ActiveX	Cookies	XPI-Erweiterungen
Phishing		

Das World Wide Web ist bunt und vielfältig – doch diese Vielfalt hat ihren Preis. Solange das Web im Wesentlichen aus formatiertem Text mit eingebundenen Bildern bestand, war das Risiko beim Betrachten der Seiten vergleichsweise gering. Immer weniger Web-Sites kommen jedoch ohne JavaScript-Menüs, eingebettete Filme, Spiele oder andere so genannten aktiven Inhalte aus.

Sie können auch die Einstellungen Ihres Browsers überprüfen lassen

Tipps zum Weiterlesen

- www.bsi-fuer-buerger.de: Info über Sicherheitslücken
- www.heise.de/security
- Windows 11, Buch der Stiftung Warentest
- Tik Tok, Snapchat und Instagram - Der Elternratgeber, Buch der Stiftung Warentest
- Windows 10 - Das Kompendium (Wolfram Gieseke), Verlag Markt und Technik
- Windows 11 Praxisbuch - das neue Windows komplett erklärt (Wolfram Gieseke), Verlag Markt und Technik
- Hacking für Manager, Tobias Schrödel, Verlag Gabler

Quelle:

Dr. Michaela Harlander

Vorstand ISAR AG / Harlander-Stiftung

Expertin auf dem Gebiet der IT-Sicherheit

Kontakt für Fragen:

bernd.lemanczyk@gymnasium-kirchheim.de

089/907784922