Digitale Schule der Zukunft

Pilotversuch DSDZ

Einrichtung von digitalen Endgeräten mit Windows

Informationen zur IT-Sicherheit

Agenda

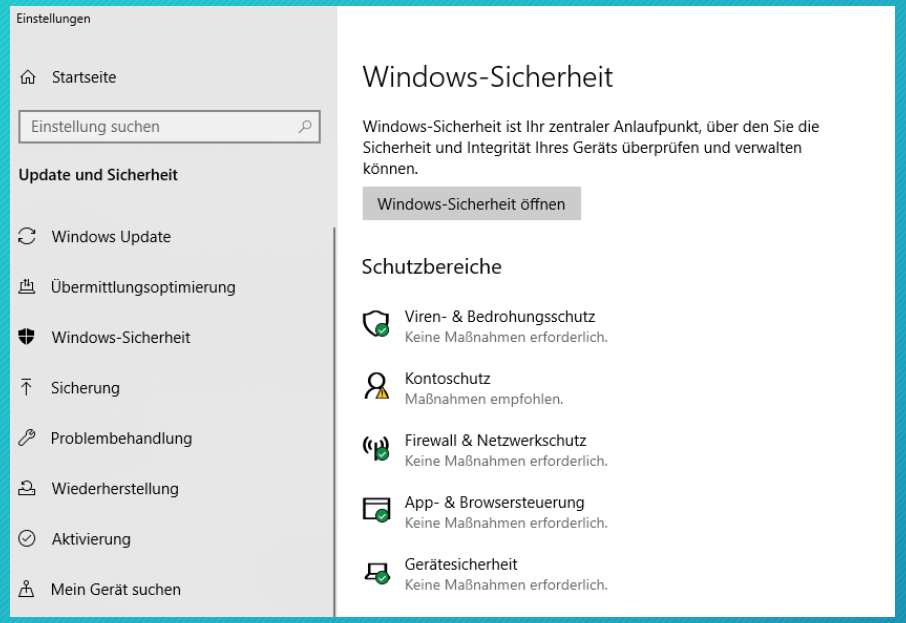
- Sichere Konfiguration
- Möglichkeiten der Kontrolle und Überwachung
- Datensicherung
- Virenscanner und Co.
- Rund um das Passwort
- Vorsicht bei Mail, Messengern und Web
- Tipps zum Weiterlesen

Sichere Konfiguration

Das Betriebssystem Windows einrichten

Windows Sicherheit

Windows 10



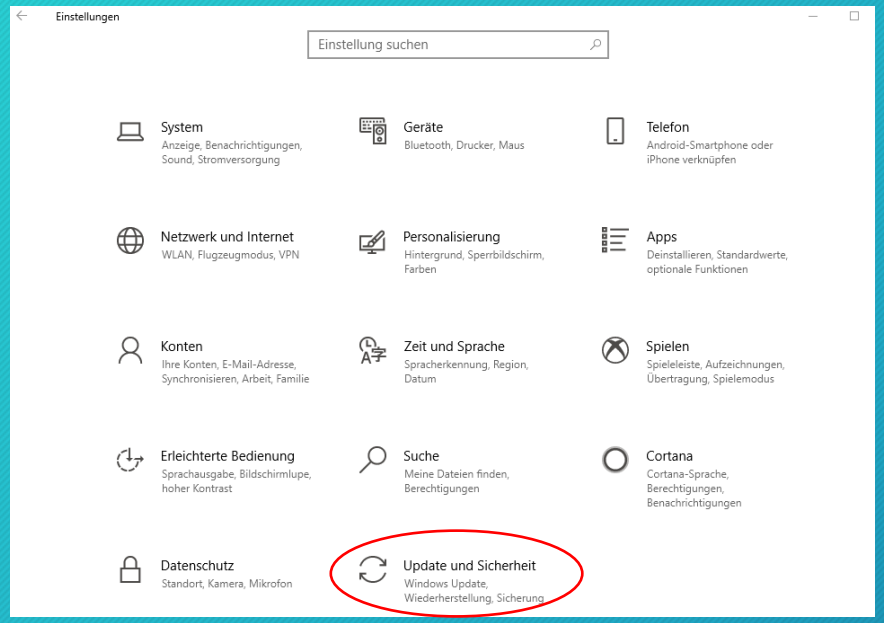
Windows 11

Windows-Updates: Sicherheitslücken schließen

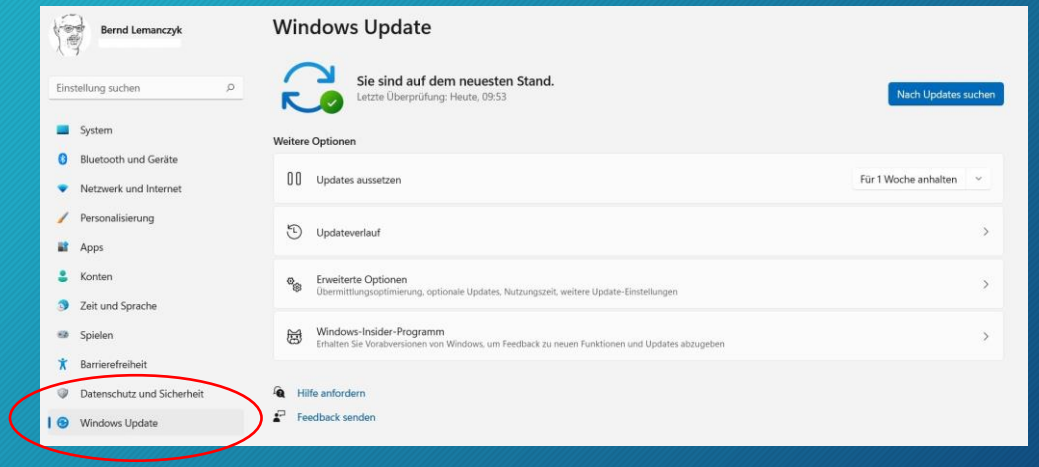
- Microsoft hat mindestens einmal pro Monat größere Updates, oft mit Sicherheitsbezug. Updates werden automatisch gesucht und – je nach Konfiguration- eingespielt.
- Sicherheitshalber auch manuell nach Updates suchen.
- IMMER die neuesten Updates rasch einspielen!
- Auch bei Anwendungen automatisch die 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?

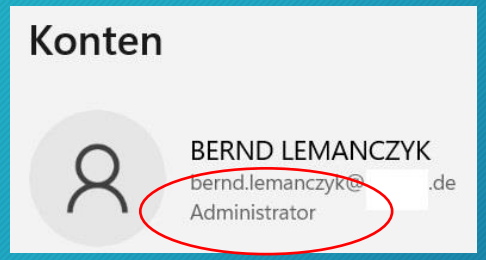
Urteil des BGH vom 15.11.2012 / I ZR 74/12

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

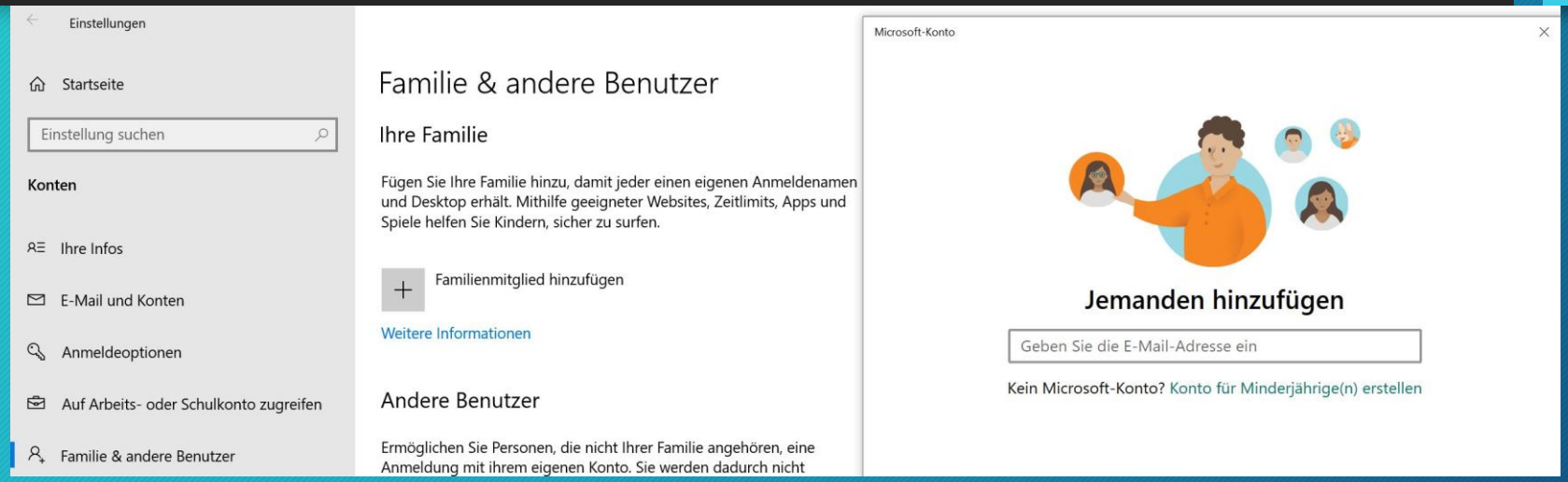
- Windows 10 bzw. 11 kennt „normale“ Benutzer und Systemadministratoren. Damit die Kinder nicht alles machen können ist es sehr wichtig, dass nur die Eltern das Administratoren-Passwort haben.
- Unter Einstellungen -> Konten sieht das so aus:



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

Familienmitglied hinzufügen

- Windows 10

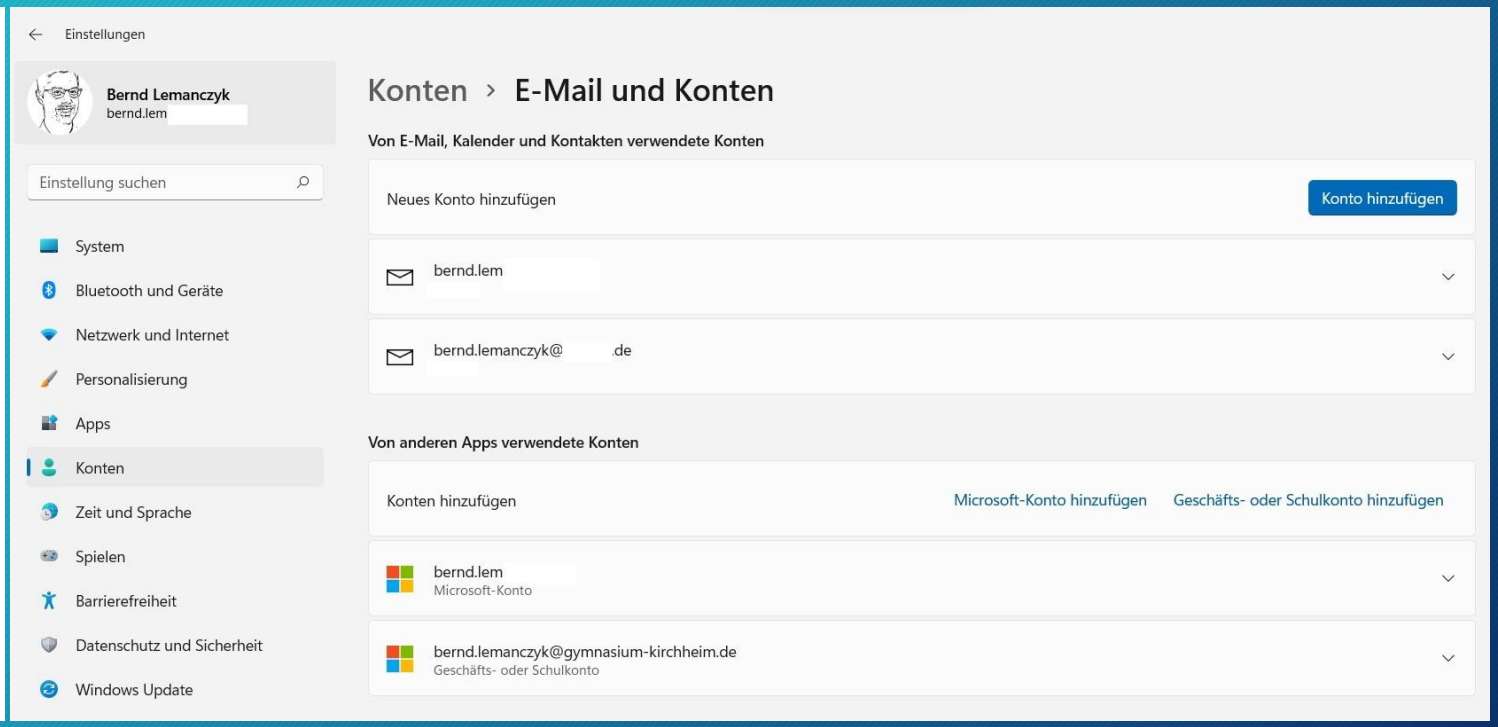


- Windows 11

Schulkonto hinzufügen

Windows 10

Windows 11



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

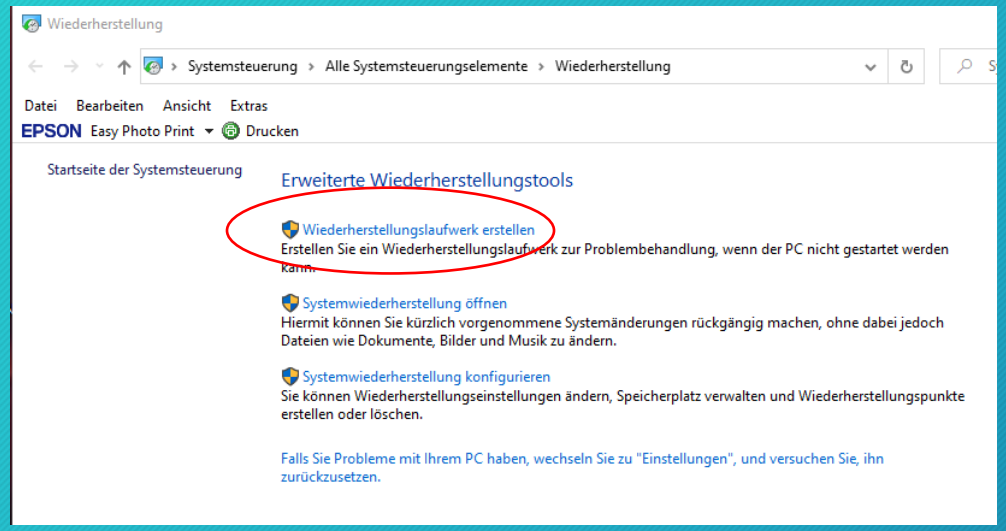
Datensicherung

Systemdaten sichern

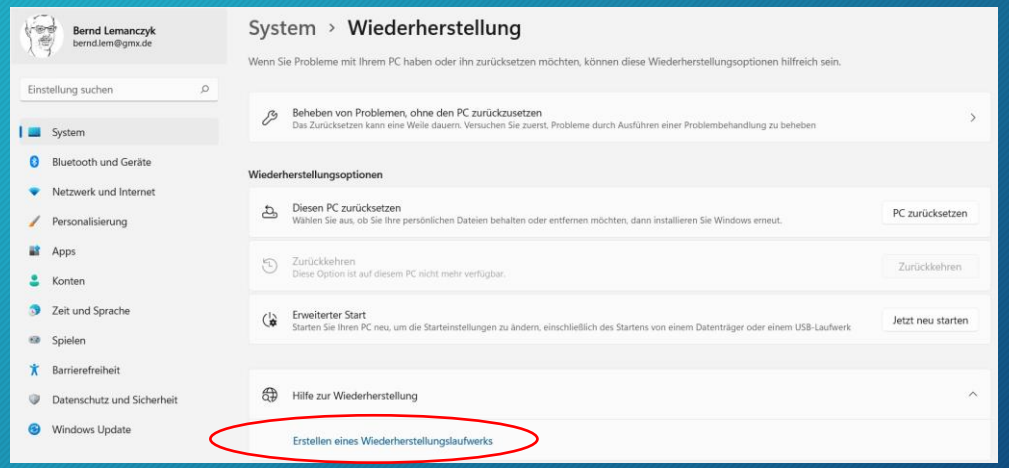
- Hier geht es darum, das Betriebssystem wieder erhalten zu können.
- Diese Option ist etwas versteckt – Sie suchen nach „Wiederherstellung“

Systemdaten sichern (Wiederherstellung)

Windows 10



Windows 11

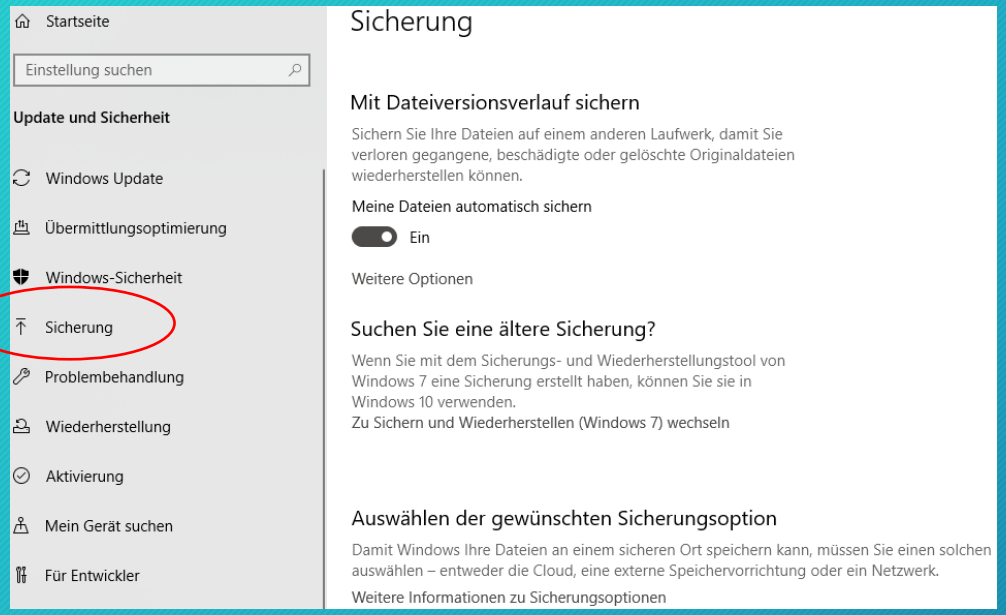


Nutzerdaten sichern

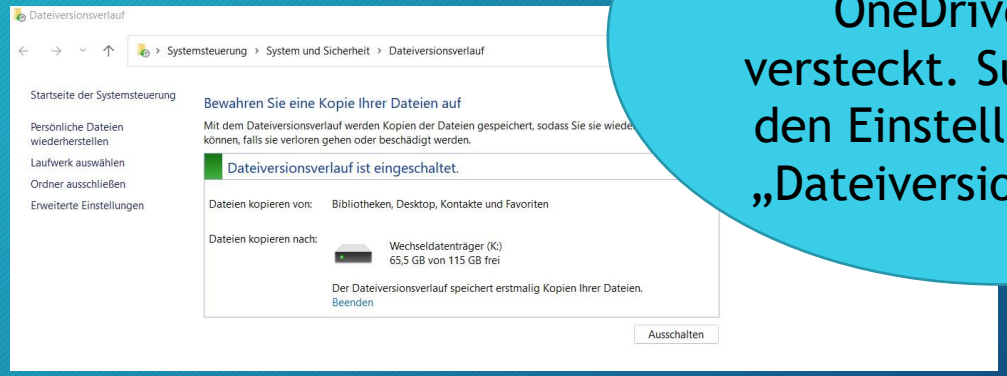
- Kann Windows automatisch machen
- Zusätzlich: in einzelnen Anwendungen einstellen (bei den Office-Anwendungen aber nur in der Cloud möglich)
- Beim Abspeichern in einer Cloud (z.B. OneDrive) gibt es automatisch eine Sicherung.
- Zusätzlich möglich: Datensicherung-Software und manuelle Sicherung auf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

Nutzerdaten sichern

Windows 10



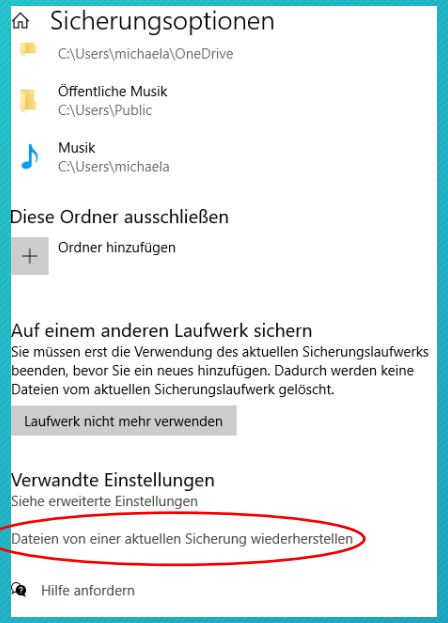
Windows 11



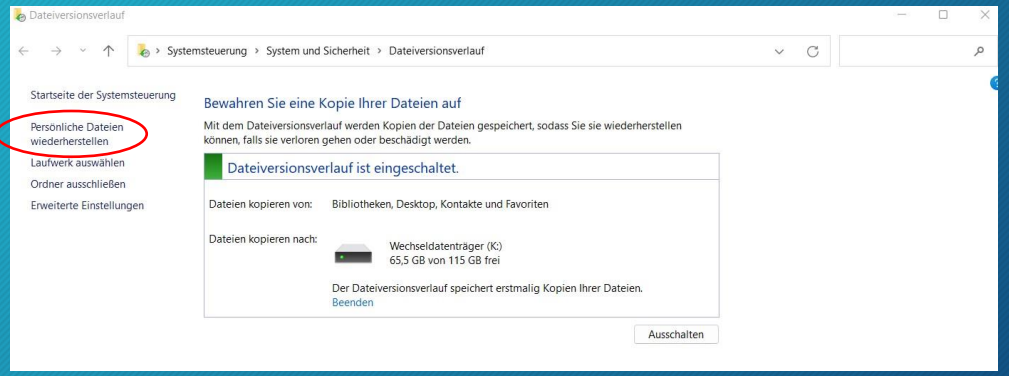
In Windows 11 ist die Datensicherung ohne OneDrive etwas versteckt. Suchen Sie in den Einstellungen nach „Dateiversionsverlauf“.

Gesicherte Daten wiederherstellen

Windows 10



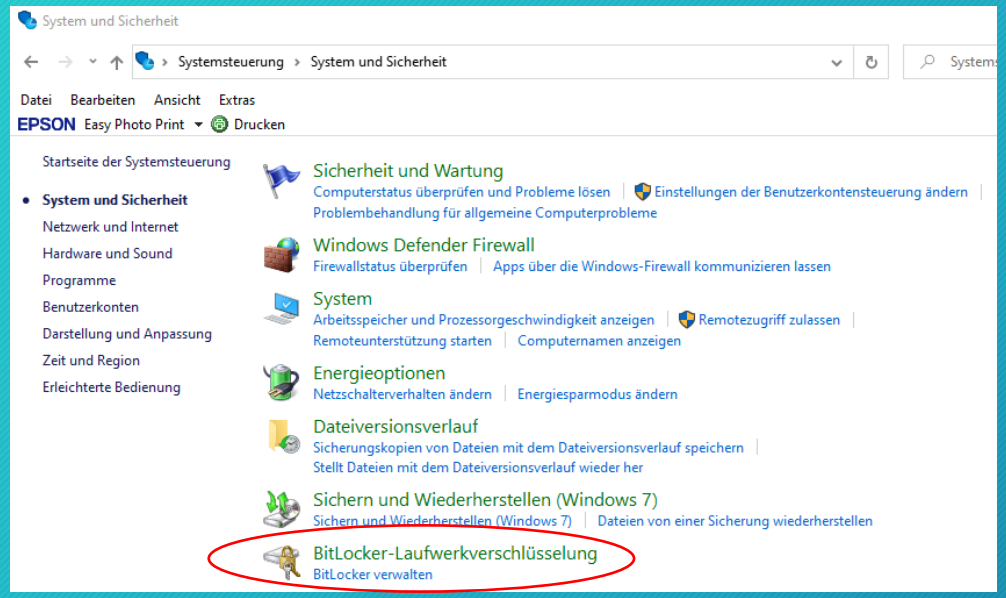
Windows 11



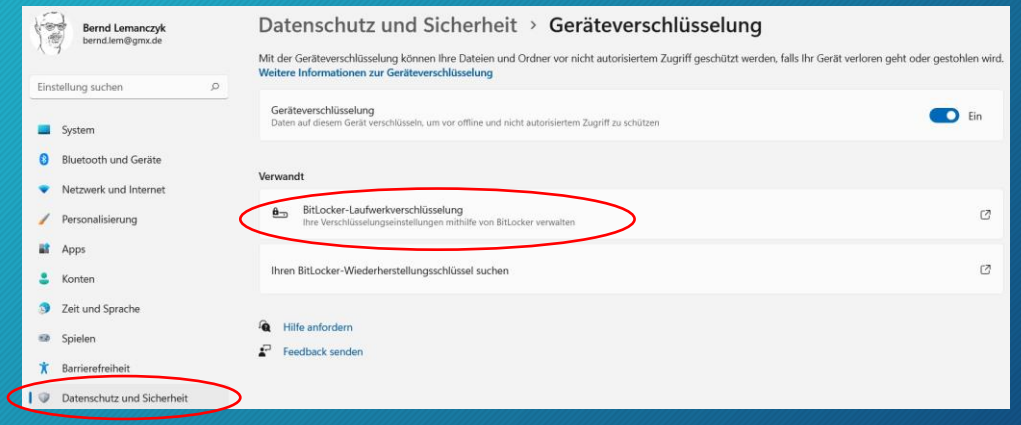
Laufwerksverschlüsselung

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

Windows 10



Windows 11



Virenscanner und Co.

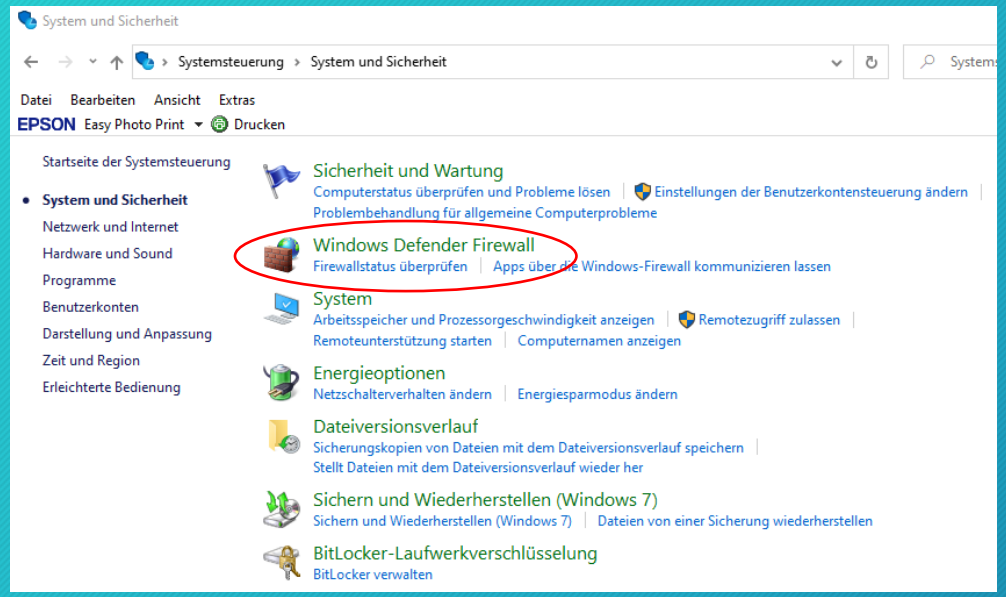
Brauche ich sowas? Helfen die noch?

Warum Virenscanner und Firewall?

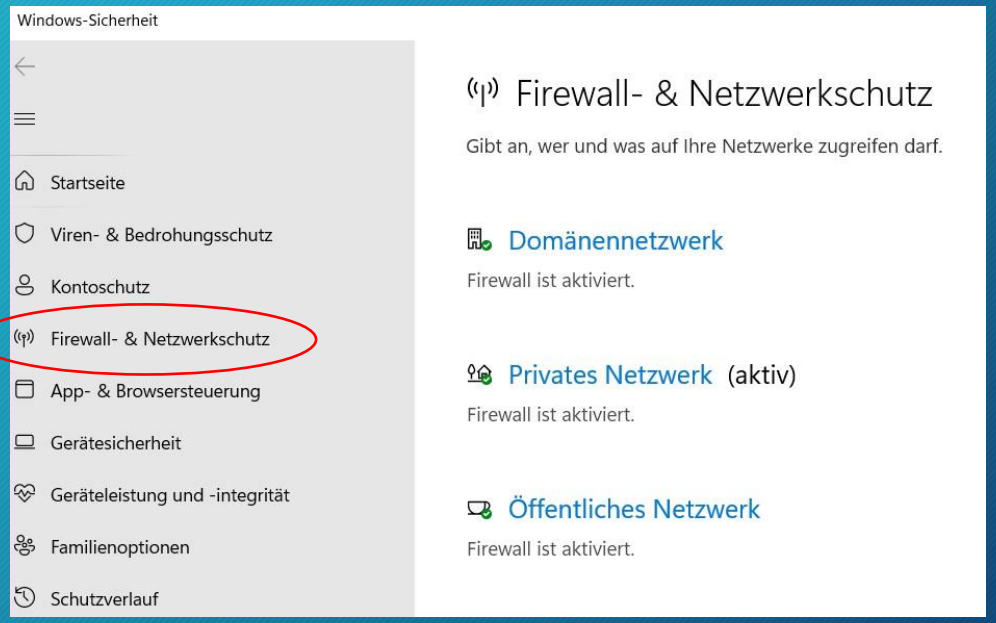
- Dateien und Anwendungen können laufend und aktuell auf Schadsoftware überprüft werden
- Eine Firewall auf dem Rechner kann unbefugte Zugriffe von innen und außen unterbinden (z.B. Verwendung Ihres Rechners für Bot-Netzwerke)
- Einfachste Lösung: Windows Defender (Bestandteil von Windows)
- Alternativ: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

Firewall (Defender; in Windows integriert)

Windows 10



Windows 11



Rund um das Passwort

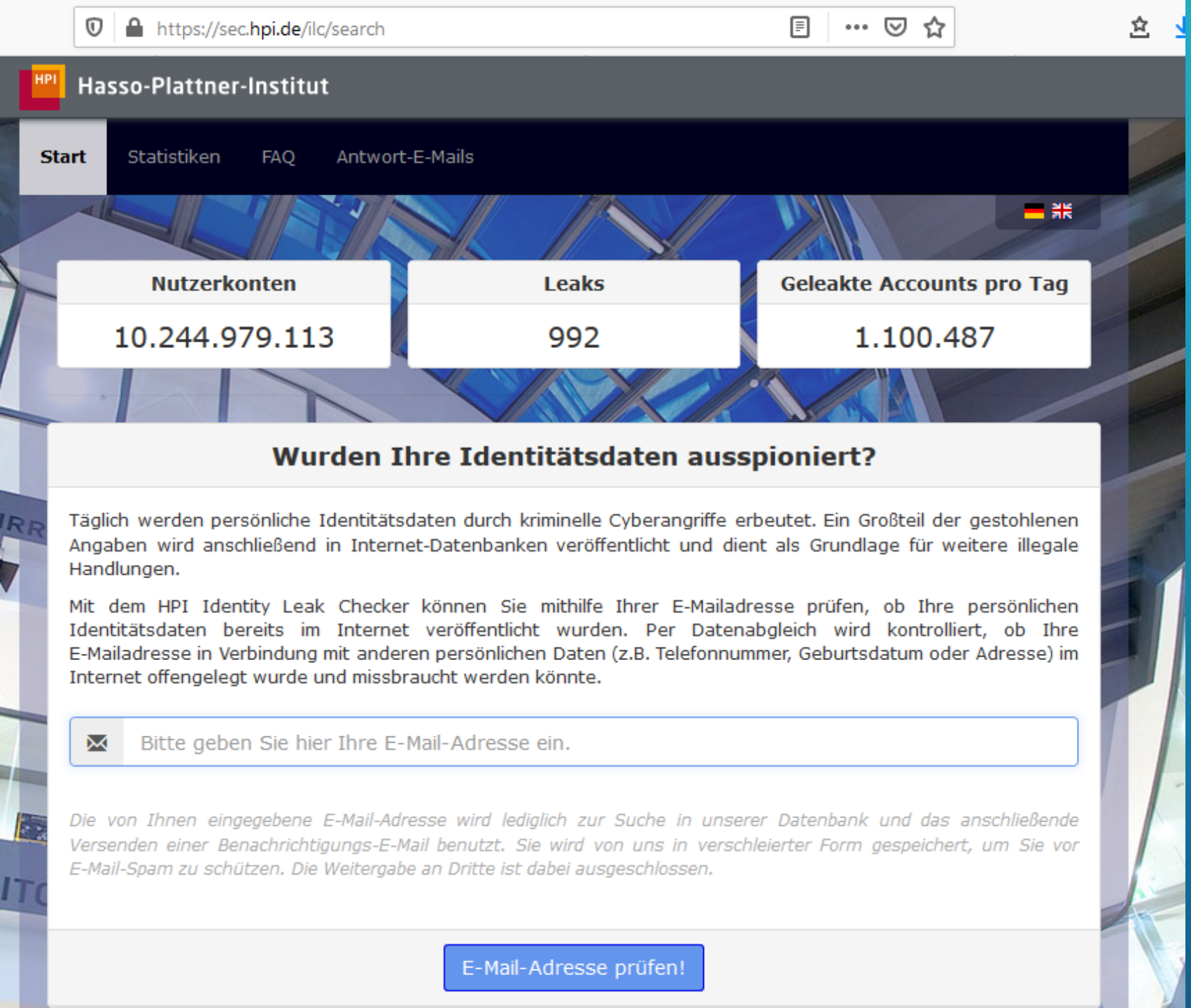
..denn leider geht es nicht ohne

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

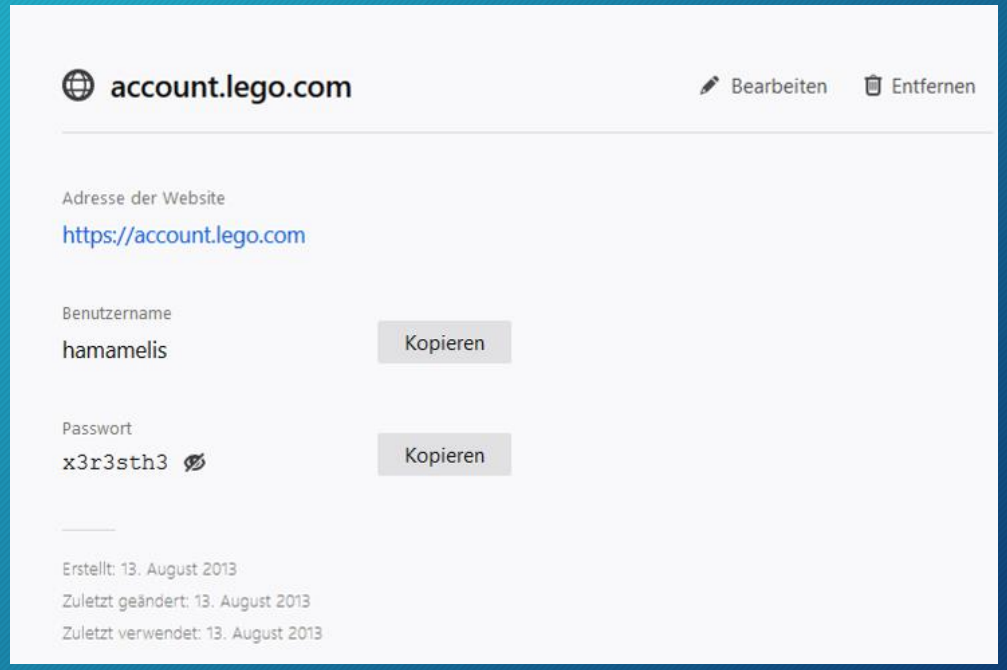
- Als relativ sicheres und gleichzeitig nicht allzu schwer zu merkendes Passwort kann man eine Passphrase verwenden
- Beispiel: Aus den Anfangsbuchstaben des Satzes „Die Axt im Haus ersetzt den Zimmermann“ wird das Passwort DAiHedZ
- Durch Verwendung von Satzteichen kann die Sicherheit deutlich gesteigert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



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?

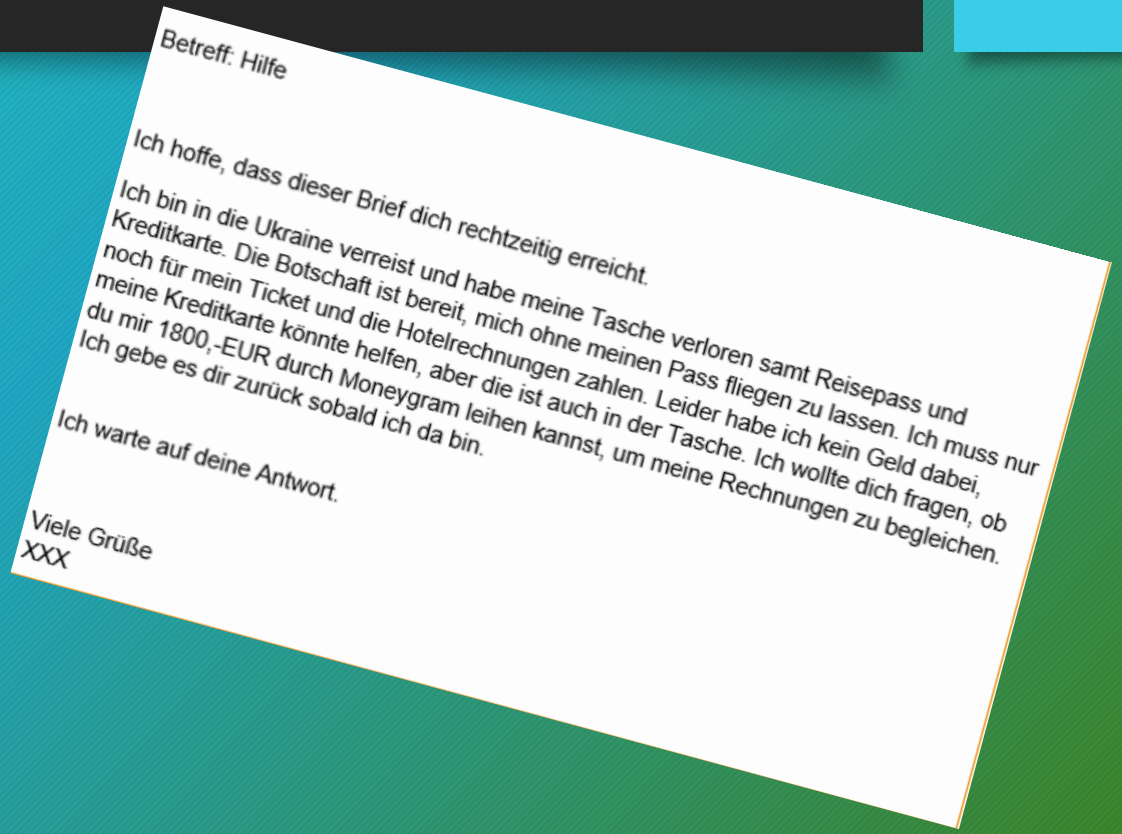
- Gar nicht. Verwenden Sie einen Passwort-Manager.
- Solche Programme gibt es oft bei Sicherheits-Software wie Virenscanner oder kostenfrei wie Bitwarden oder KeePass.
- Idealerweise mit 2-Faktor-Authentisierung.
- Wahl: Cloud-Lösung oder offline
- Wenn offline: bei Ausmustern des Rechners Festplatte 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



Betreff: Hilfe

Ich hoffe, dass dieser Brief dich rechtzeitig erreicht.

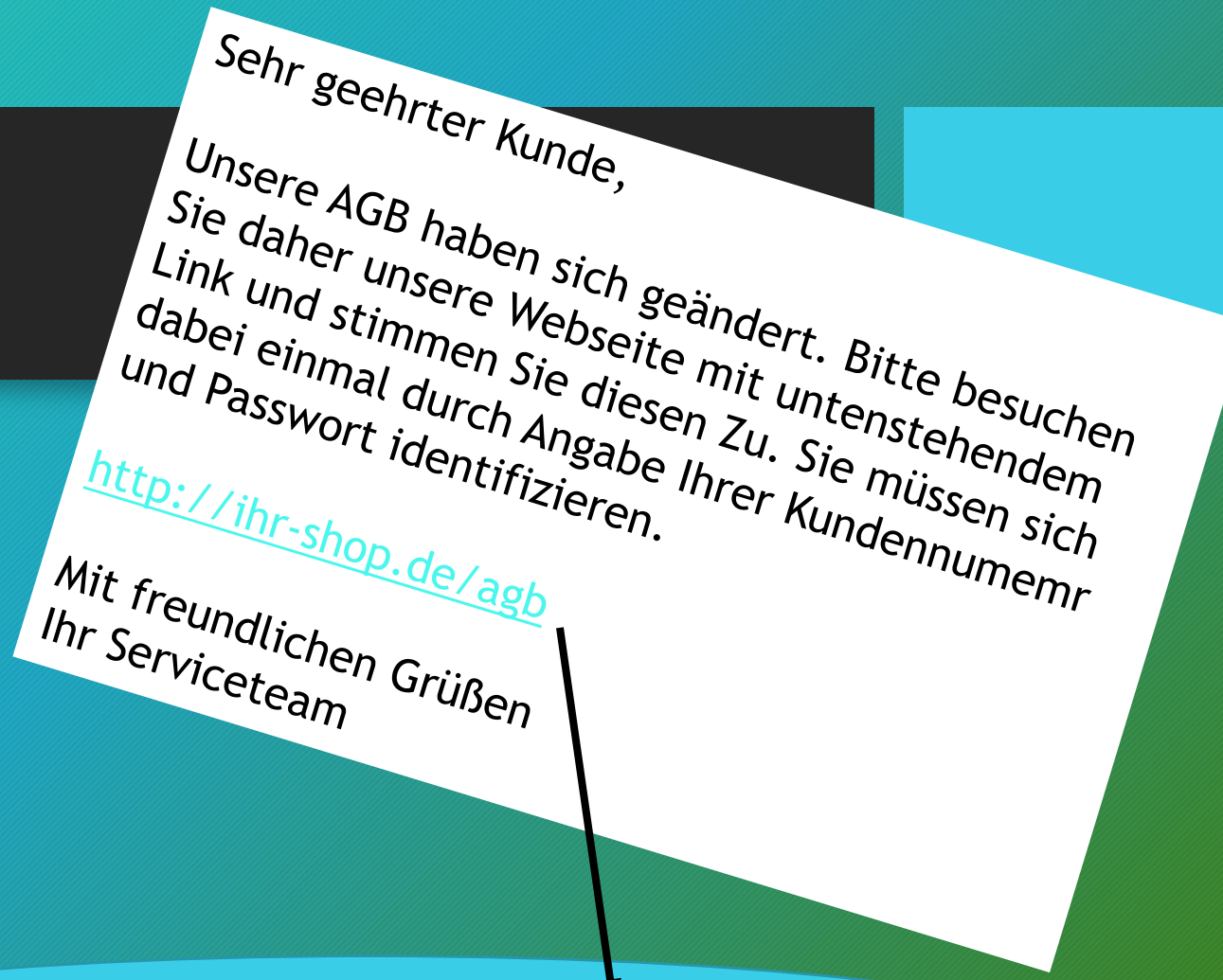
Ich bin in die Ukraine verreist und habe meine Tasche verloren samt Reisepass und Kreditkarte. Die Botschaft ist bereit, mich ohne meinen Pass fliegen zu lassen. Ich muss nur noch für mein Ticket und die Hotelrechnungen zahlen. Leider habe ich kein Geld dabei, meine Kreditkarte könnte helfen, aber die ist auch in der Tasche. Ich wollte dich fragen, ob du mir 1800,-EUR durch Moneygram leihen kannst, um meine Rechnungen zu begleichen. Ich gebe es dir zurück sobald ich da bin.

Ich warte auf deine Antwort.

Viele Grüße
XXX

Mail: Betrug durch Phishing

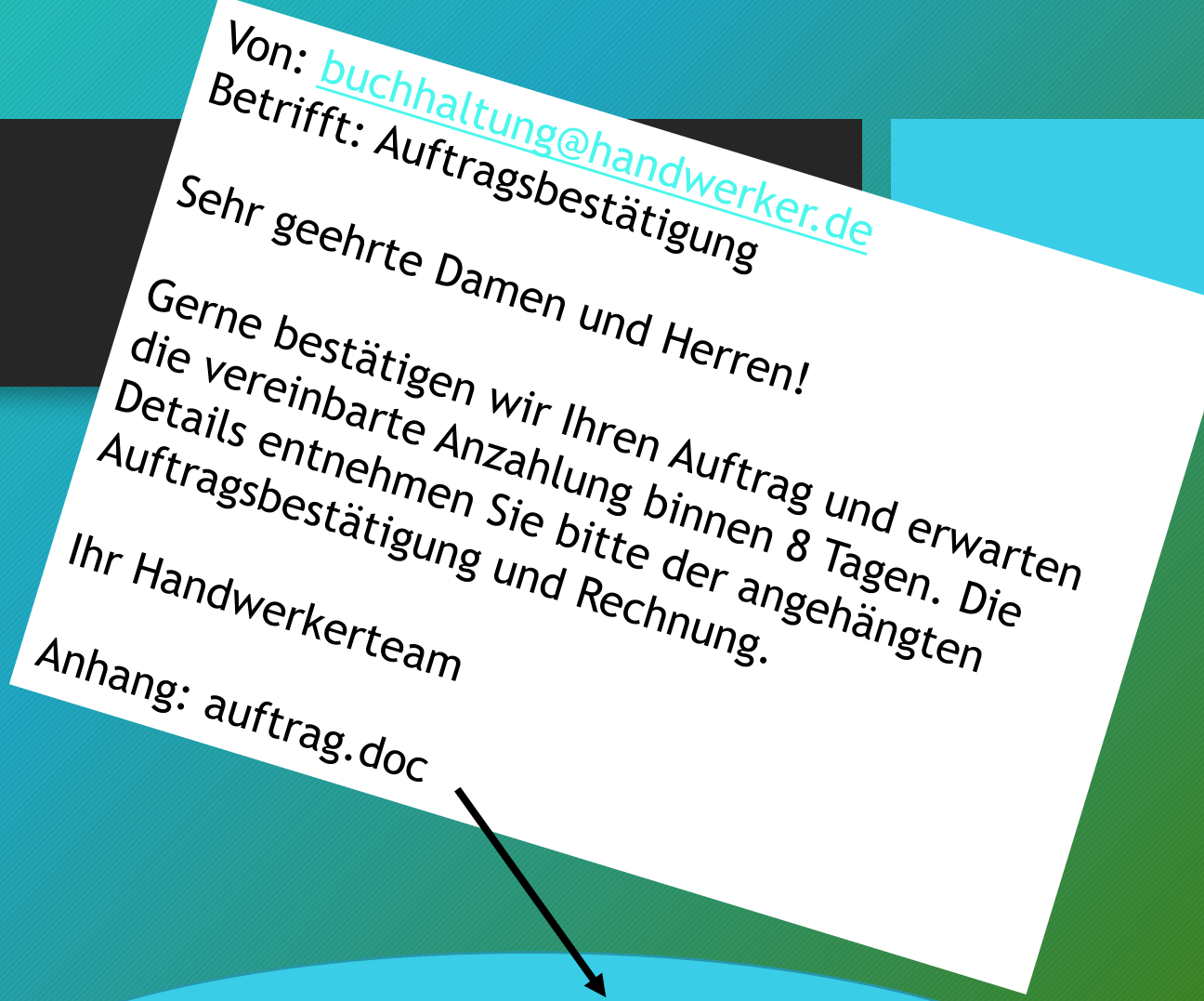
- Phishing ist Abfangen von Daten meist durch Umleiten auf gefälschte Webseiten
- Ganz klassisch: Zustimmung zu neuen AGB, DSGVO oä.
- Seit Einführung der 2-Faktor-Authentisierung im Banking werden vermehrt Bestellinfos für Shops abgegriffen.



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 warden, 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

- [x] Gefährliche und betrügerische Inhalte blockieren Weitere Informationen
  - [x] Gefährliche Downloads blockieren
  - [x] 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“

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