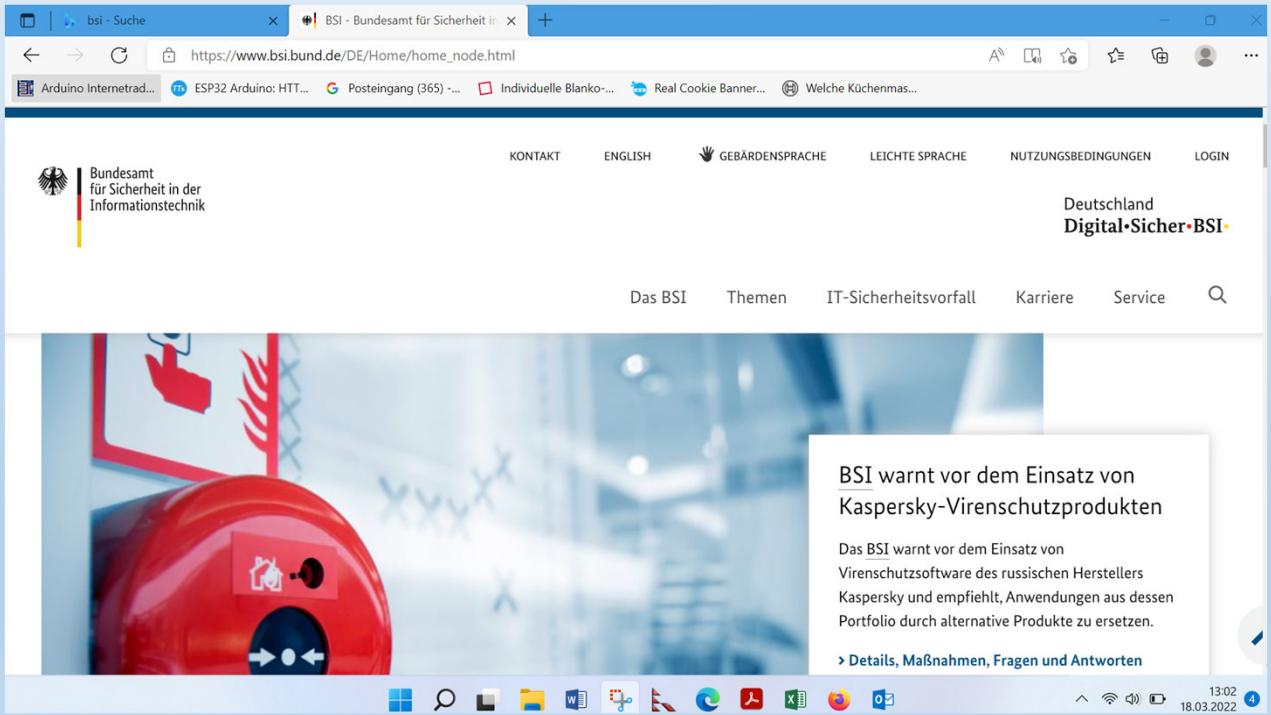
# Sicherheit in der Informationstechnik


Michael Fischer, 25.06.2022

Sicherheit in der Informationstechnik

# Bundesamt für Sicherheit in der Informationstechnik

[Bundesoberbehörde](#) im [Geschäftsbereich](#) des [Bundesministeriums des Innern und für Heimat](#)




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

Der Arbeitsauftrag des BSI umfasste von Beginn an den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge. Mit der Novellierung des BSI-Gesetzes 2009 konnte das BSI für die Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln. Das BSI wurde zudem zur zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung, um bei IT-Krisen nationaler Bedeutung durch Informationen und Analysen die Handlungsfähigkeit der Bundesregierung sicherzustellen. Für Wirtschaft, Wissenschaft, Gesellschaft sowie für die Bürgerinnen und Bürger fungierte das BSI als kompetenter Ansprechpartner und Berater für alle Fragen der Informationssicherheit.

Mit dem › **IT-Sicherheitsgesetz 2.0** wurde der Auftrag des BSI 2021 erneut erweitert, um den Herausforderungen der fortschreitenden Digitalisierung zu begegnen. So verankert das IT-SiG 2.0 den digitalen Verbraucherschutz im BSI. Als Gestalter einer sicheren Digitalisierung in Deutschland unterstützt das BSI Verbraucherinnen und Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten, etwa durch die Einführung eines IT-Sicherheitskennzeichens.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

CERT-Bund, das **C**omputer **E**mergency **R**esponse **T**eam für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen.

Das Computer-Notfallteam

- erstellt und veröffentlicht präventive Handlungsempfehlungen zur Schadensvermeidung,
- weist auf Schwachstellen in Hardware- und Software-Produkten hin,
- schlägt Aktionen vor, um bekannte Sicherheitslücken zu beheben,
- unterstützt bei der Reaktion auf IT-Sicherheitsvorfälle,
- empfiehlt reaktive Maßnahmen zur Schadensbegrenzung oder -beseitigung
- arbeitet eng mit dem › **IT-Lagezentrum** und dem › **IT-Krisenreaktionszentrum** zusammen und unterstützt beide personell.

## Bürger-CERT

Für interessierte Privatpersonen stellt CERT-Bund umfangreiche Informationen über den › **Warn- und Informationsdienst Bürger-CERT** zur Verfügung. Das Bürger-CERT informiert kostenfrei und neutral über aktuelle Attacken durch Schadsoftware sowie über Sicherheitslücken in Computeranwendungen.

Michael Fischer, 25.06.2022

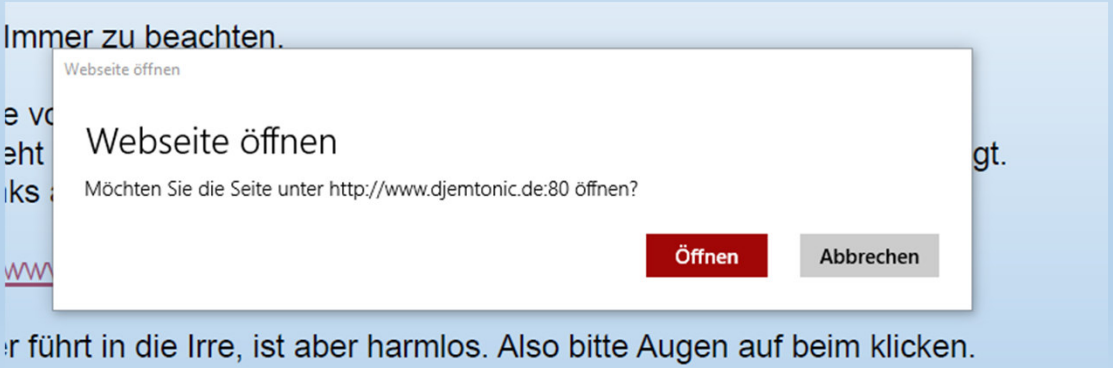
# Sicherheit in der Informationstechnik

Tipp 1 immer zu beachten.

**Seien Sie vorsichtig mit Links, wo auch immer sie auftauchen.**
**Man sieht nur einen Text, der Link wird nicht immer und zuverlässig angezeigt.**
**Nur Links anklicken, die in einem Umfeld stehen, dem Sie vertrauen**.

https://www.bsi.de

Der hier führt in die Irre, ist aber harmlos. Also bitte Augen auf beim Klicken.




Manche Applikation verrät deutlich, wo es hingehen soll.

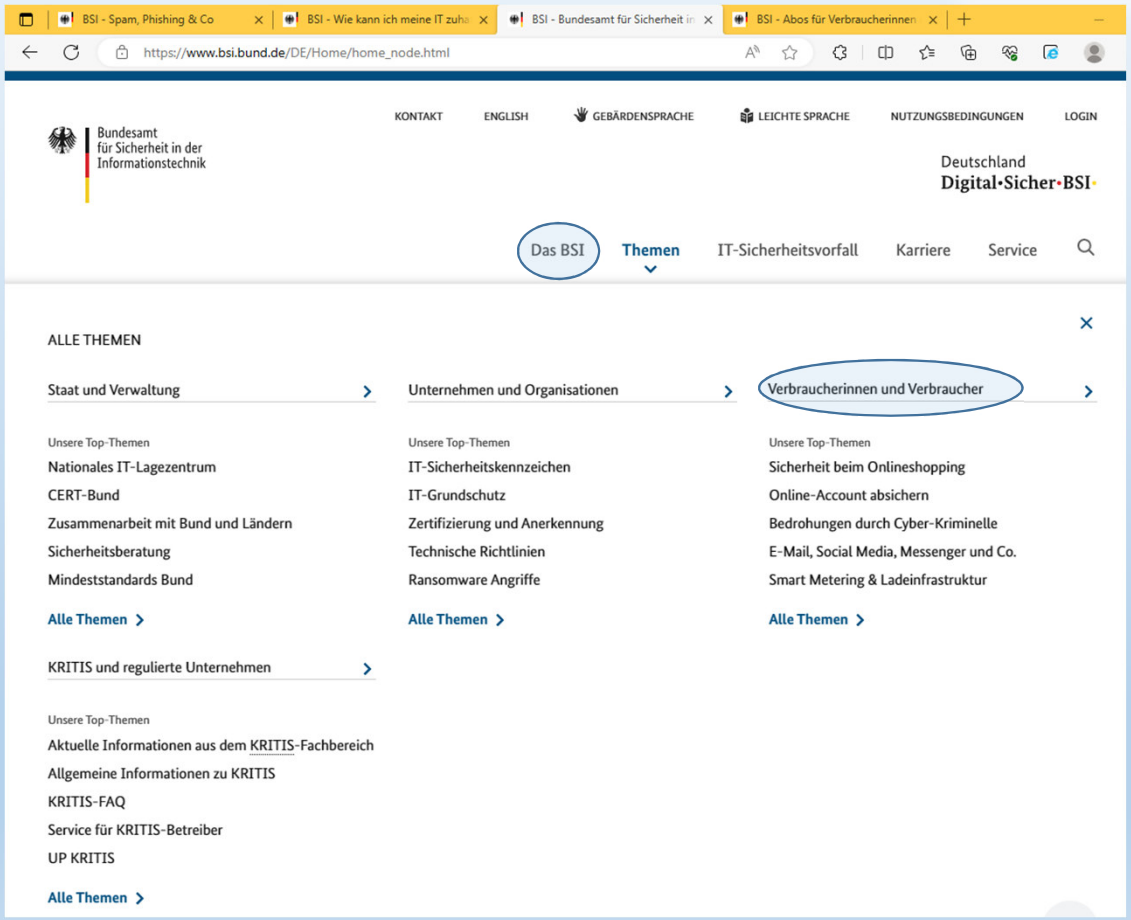

Andere machen das viel diskreter, und wieder andere gar nicht.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

Der Link hier ist in Ordnung und führt zum BSI

https://www.bsi.de




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

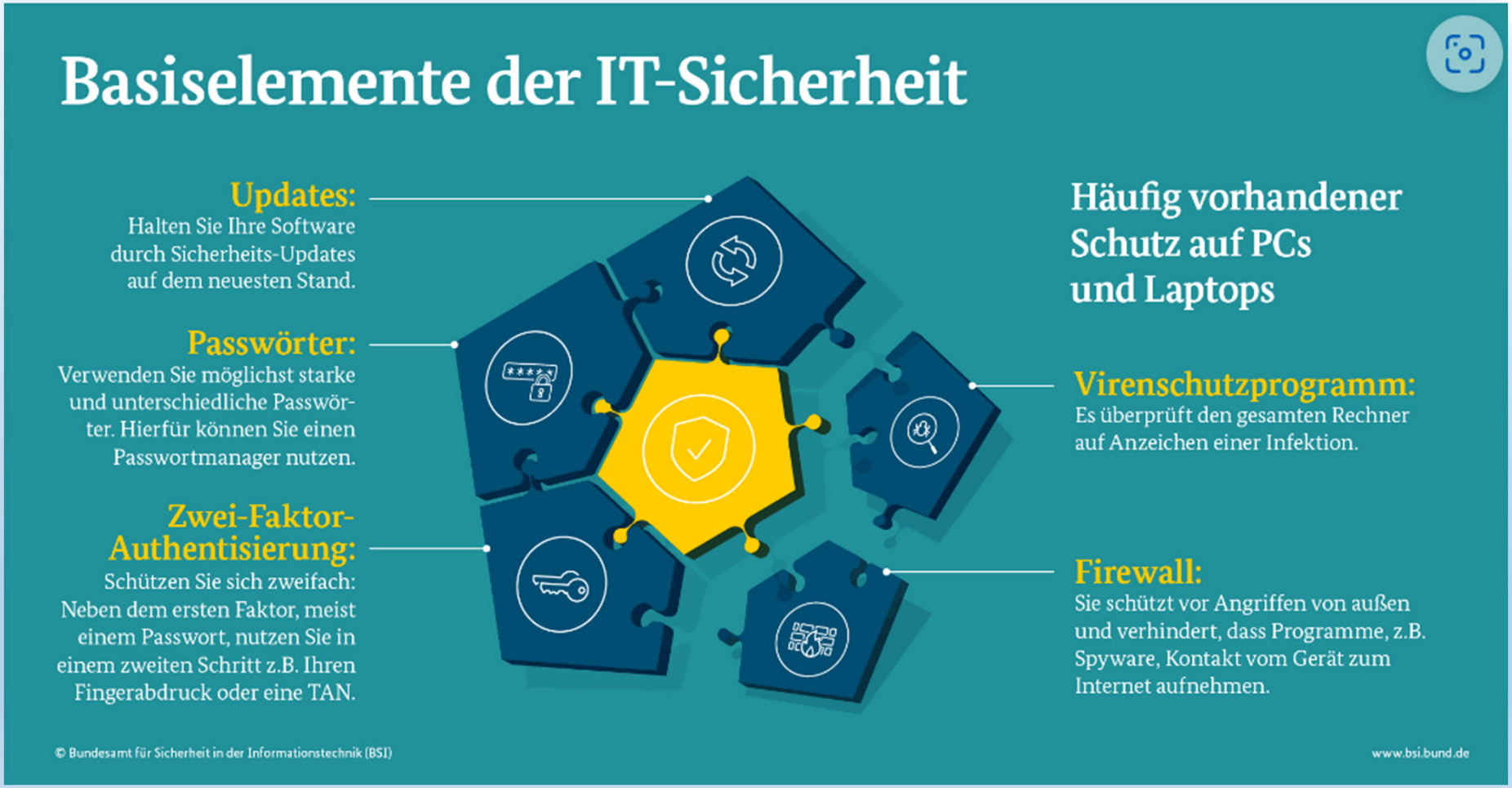
**Newsletter: Alle 14 Tage auf Nummer sicher gehen:**

Mit dem **Newsletter 'Sicher Informiert'** und den **Sicherheitshinweisen** des BSI erhalten Sie regelmäßig Informationen zu aktuellen Sicherheitslücken und wichtigen Ereignissen rund um IT-Sicherheit. Sowohl leicht verständliche Erklärungen, praxisnahe Tipps, aber auch tiefergehende technische Details bringen Sie auf den aktuellen Stand. **› Zum Newsletter 'Sicher Informiert'.**

Wenn Sie möchten, können Sie den Newsletter hier bestellen.

Michael Fischer, 25.06.2022

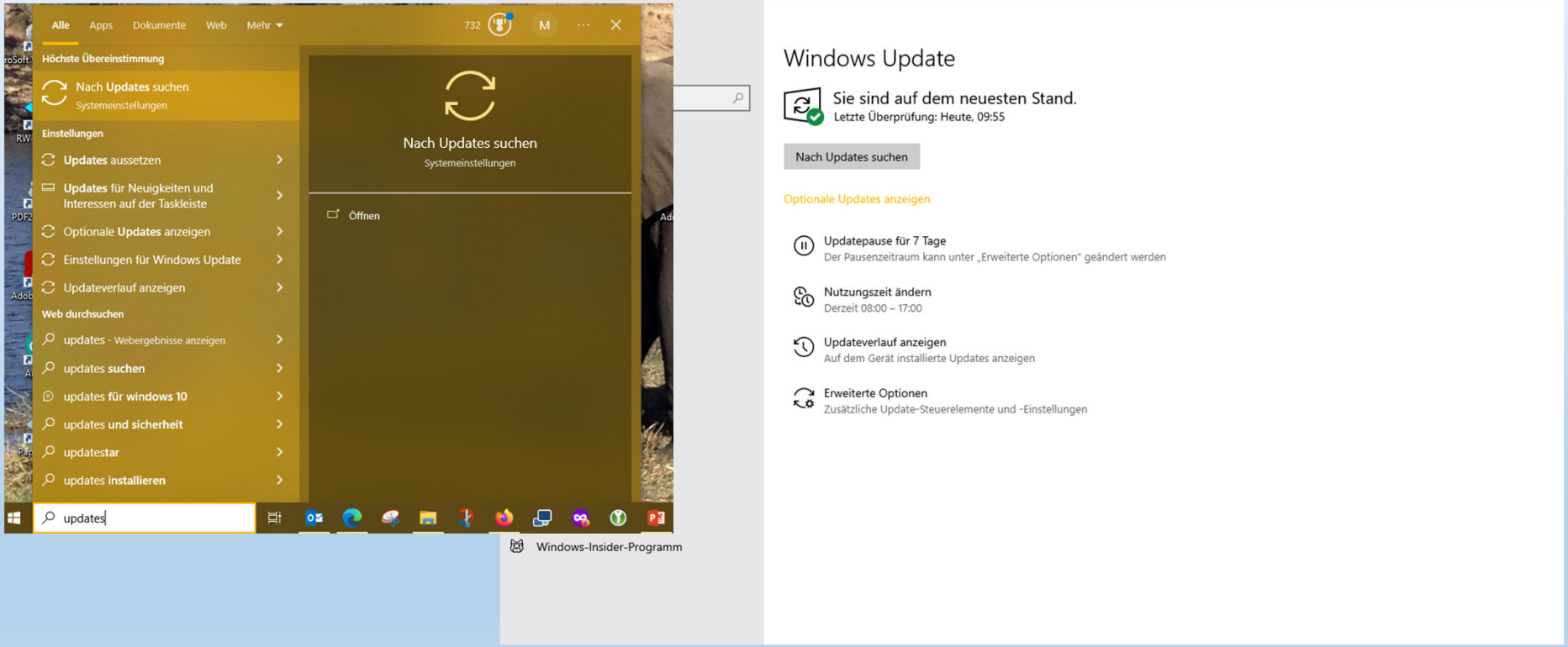
# Sicherheit in der Informationstechnik




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

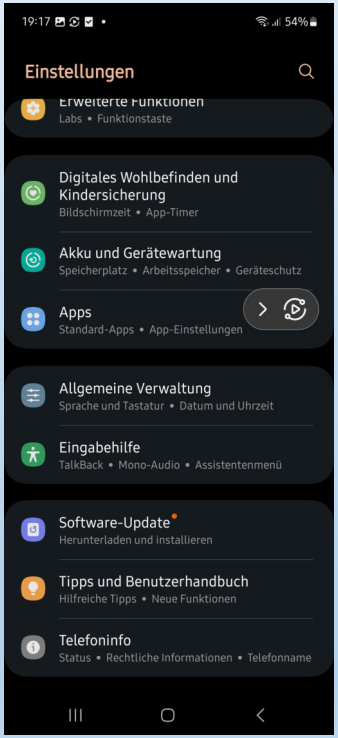
So kann man bei Windows Rechnern überprüfen ob alles aktuell ist.

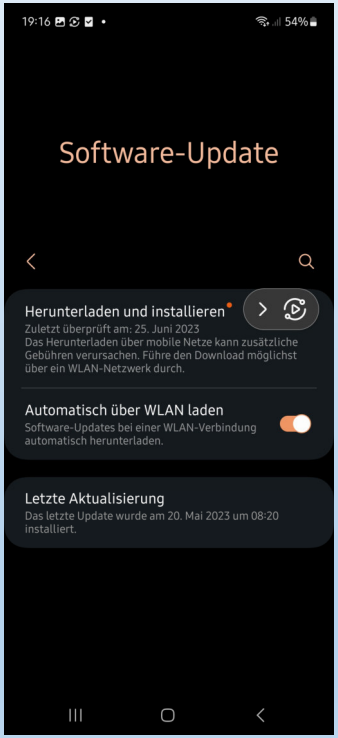



Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

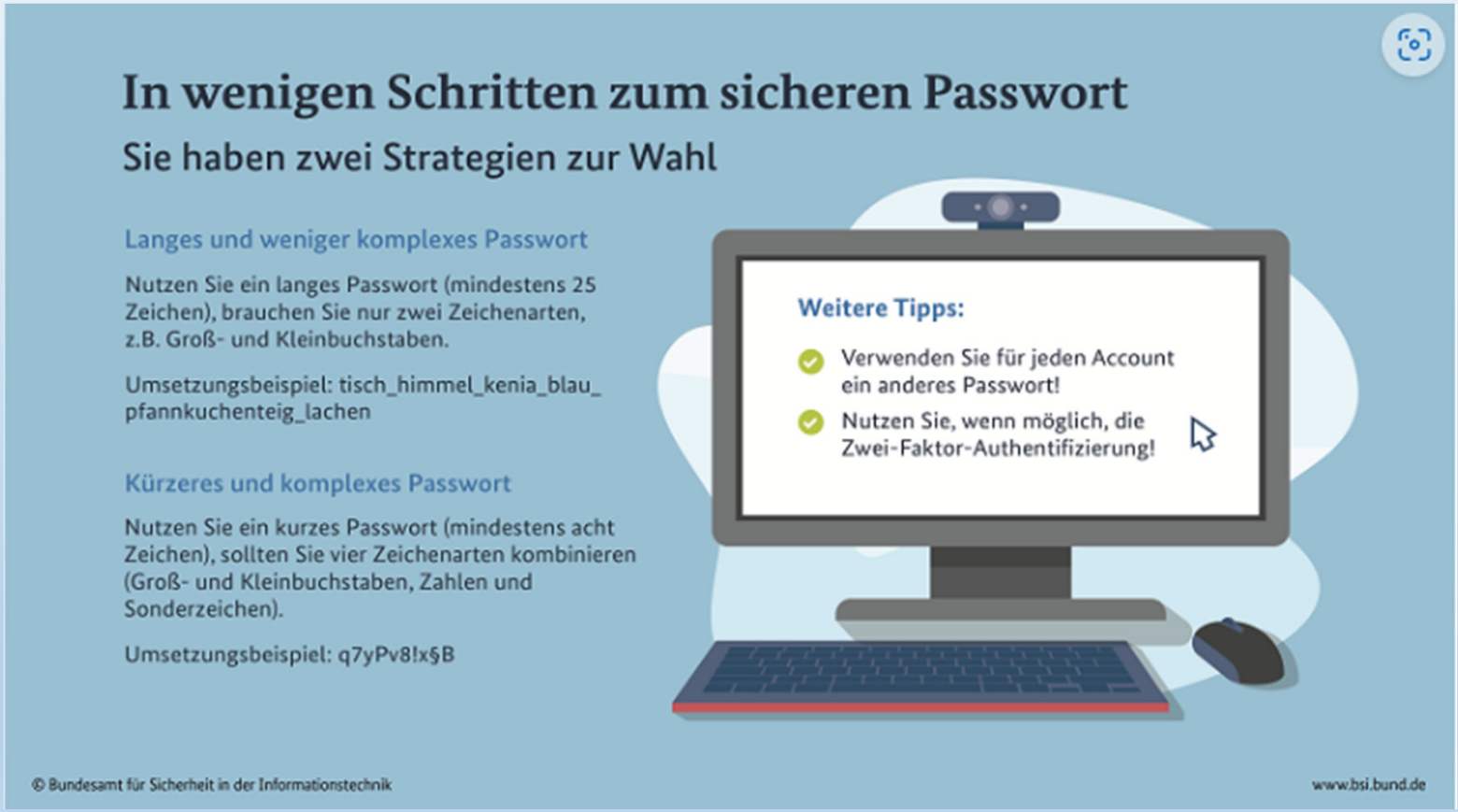
Ein Android Handy gibt üblicherweise eine Meldung aus, wenn ein update zur Verfügung steht, man kann aber auch in den Einstellungen nach Software updates schauen.




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

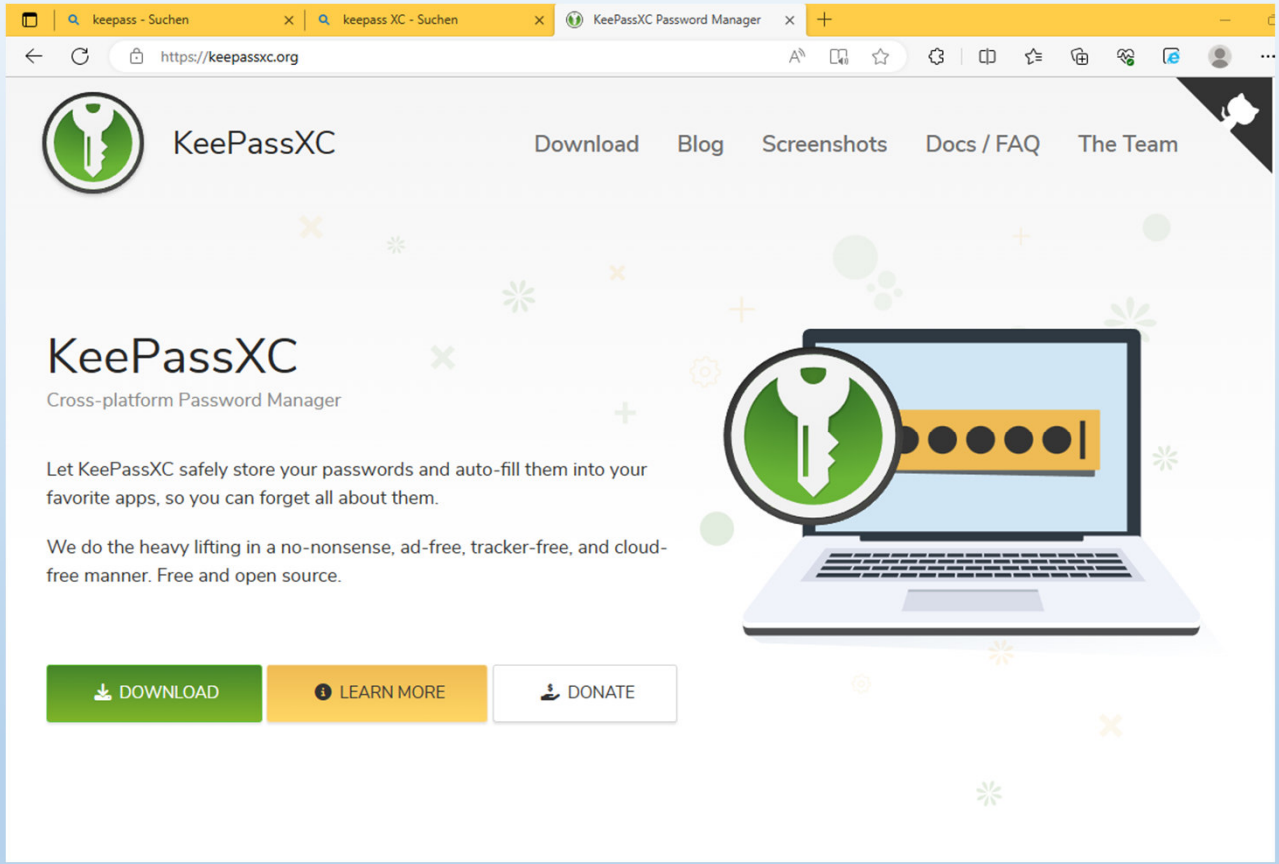
## Nachteile des Passwort-Managers

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Alle Passwörter können auf einmal gestohlen werden, sollte ein Cyber-Angriff auf einen Passwort-Manager erfolgreich sein.
- Bei cloudbasierten Diensten vertrauen Sie den Zugang zu all Ihren sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind.

## Lohnt sich ein Passwort-Manager?

Ja, in der Regel lohnt sich der Einsatz eines Passwort-Managers. Es ist in jedem Fall besser, als gängige Passwörter wiederholt zu benutzen. Die konkrete Entscheidung darüber, welches Programm genutzt wird, erfordert ein individuelles Abwägen der jeweiligen Nutzung. Es geht dabei auch um die Einschätzung des damit verbundenen Risikos.

# Sicherheit in der Informationstechnik




Ich verwende KeePassXC,
das ist eine deutsche Open Source Applikation, die KeePass verwendet.

Kostenlos einsetzbar, plattformunabhängig.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

[Zwei-Faktor-Authentisierung]


Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

Mit einigen einfachen Maßnahmen können Sie die Sicherheit beim Surfen im Internet erheblich erhöhen. Dazu gehört unter anderem, dass Sie Schutzprogramme wie zum Beispiel Virenschutzprogramme oder eine Personal Firewall auf Ihrem Rechner installieren. Beachten Sie beim Einsatz solcher Programme folgende Hinweise:

- Kostenfreie Produkte bieten häufig nur eingeschränkte Funktionalitäten. Informieren Sie sich über die unterschiedlichen Funktionen kostenfreier und kostenpflichtiger Programme und wägen Sie ab, ob sich ein Kauf für Sie lohnt.
- Laden Sie Programme grundsätzlich von den Herstellerwebseiten herunter. Nur so können Sie sicher gehen, dass das installierte Programm auf dem aktuellen Stand ist.
- Achten Sie darauf, ob es Sicherheitsupdates für die von Ihnen installierten Programme gibt und führen Sie diese regelmäßig durch. Halten Sie alle Programme auf dem aktuellen Stand.

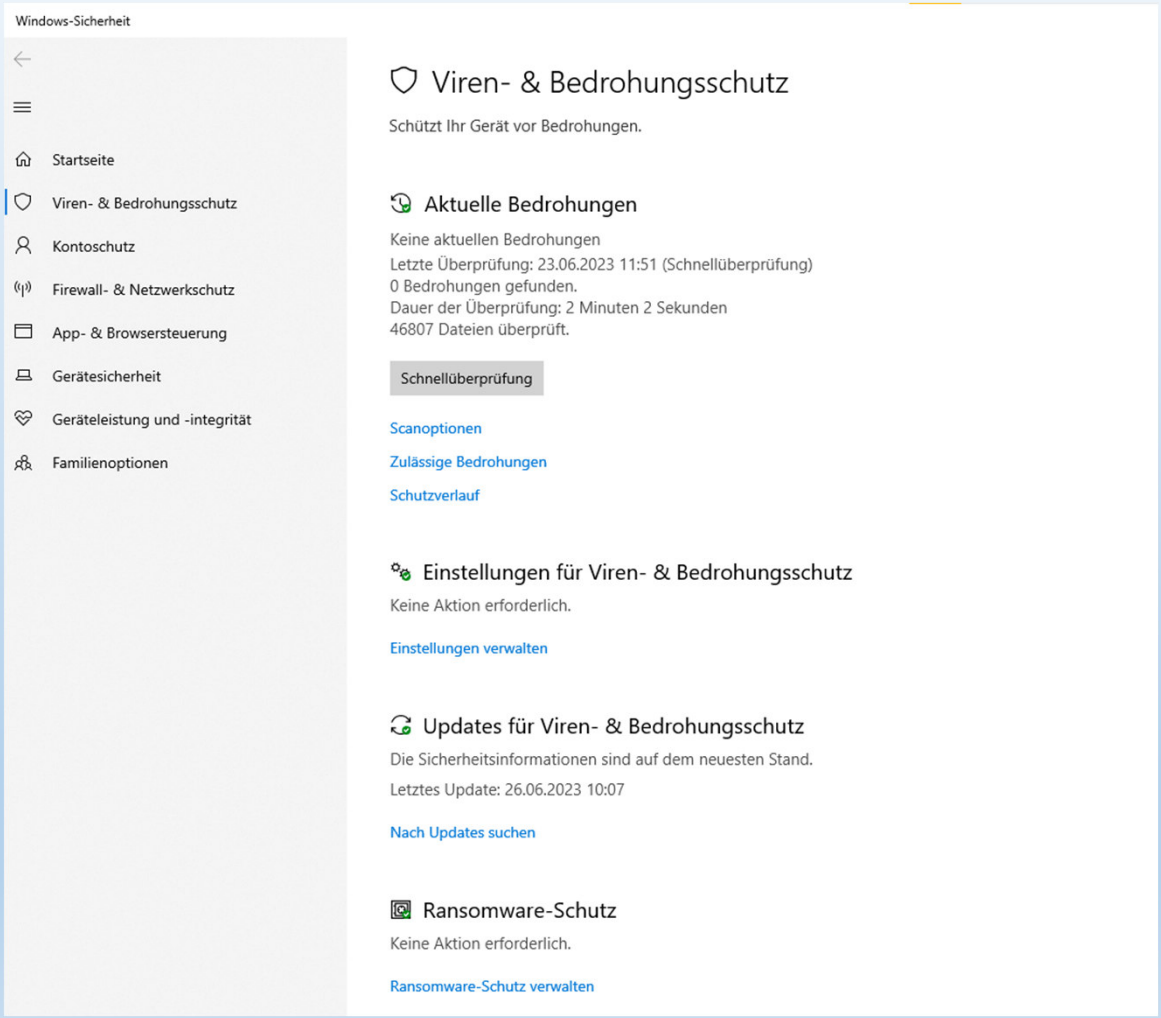
# Sicherheit in der Informationstechnik

Für einen hinreichenden Schutz des Systems gegen Computer-Viren und andere Schadprogramme kommen für Privatanwender sowohl kostenlose als auch kostenpflichtige Varianten von Virenschutz-Software infrage. Letztere verfügen unter Umständen über mehr Funktionen. Sofern die sinnvollen, zusätzlichen Funktionen der kostenpflichtigen Lösungen, wie beispielsweise

- Kinderschutzfilter
- Überwachung von Browser- und E-Mail-Aktivitäten auf Schadprogramme
- erweiterte, verhaltensbasierte Erkennung von Schadsoftware

dennoch nicht benötigt werden, sind kostenlose Virenschutzprogramme seriöser Hersteller ausreichend. Auch die Hersteller der Betriebssysteme selbst bieten ein kostenloses Virenschutzprogramm an.

# Sicherheit in der Informationstechnik

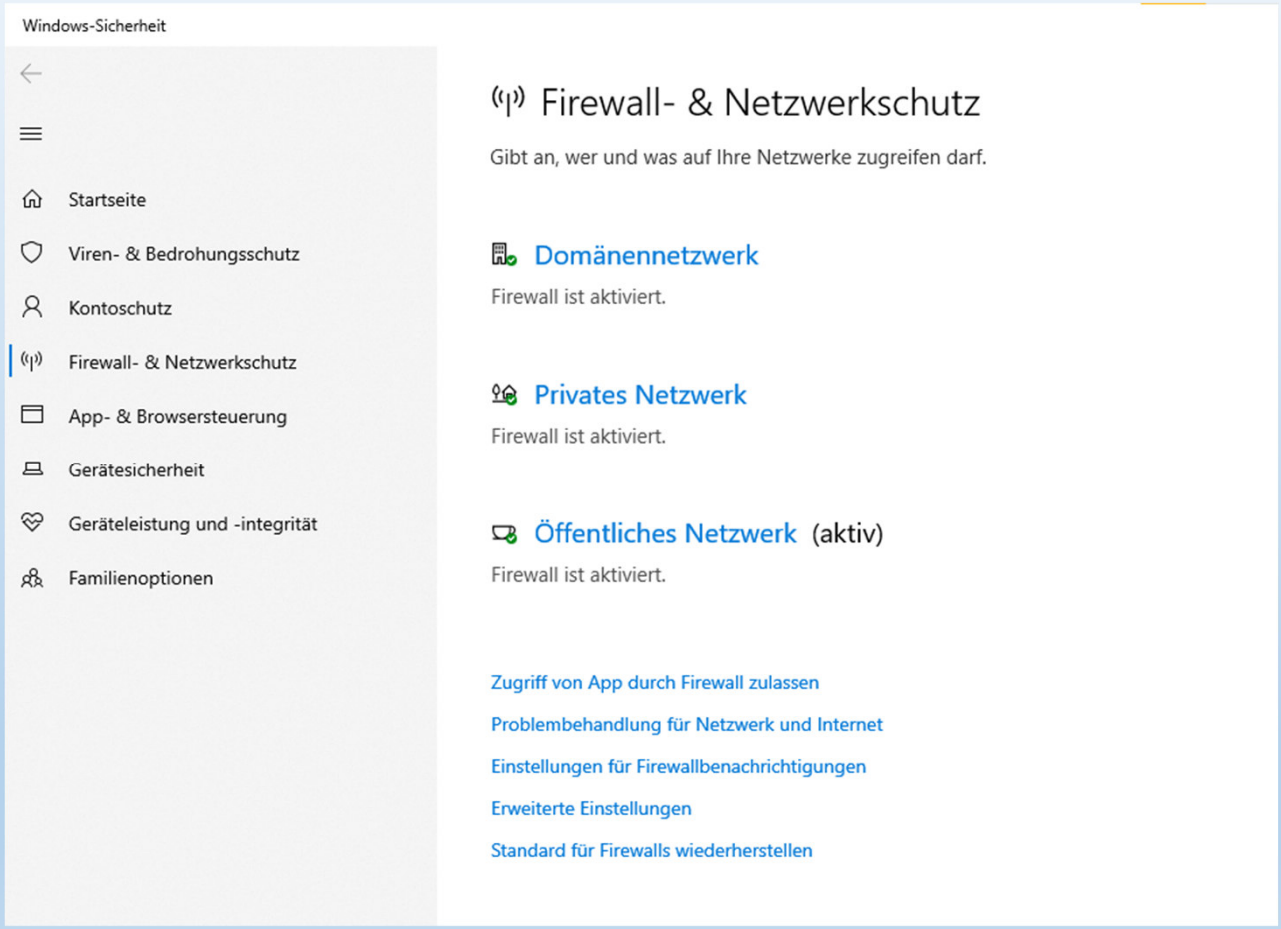



Beim Virenschutz vertraue ich Windows-Bordmitteln.

Aber immer drauf achten, wie bei jedem Virusscanner, dass die Virus-Signaturen aktuell sind.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik




Ebenso vertraue ich beim Firewall auf das, was Microsoft mitliefert.

Die Firewall Einstellungen werden bei der Installation neuer Programme nach den Vorgaben des Benutzers gemacht.

Wenn man hier etwas ändern möchte, muss man aber schon genau wissen, was man tut.
Der Rechner, oder Teile davon, lassen sich hier leicht lahmlegen.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

## SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR PHISHING

- Führen Sie Aktualisierungen von Software und Betriebssystemen auf allen Geräten immer sofort durch und installieren Sie Antivirenprogramme.
- Seien Sie skeptisch bei E-Mails unbekannter Absender. Ihre Bank, Diensteanbieter oder Behörden bitten niemals per E-Mail darum, persönliche Daten wie Passwörter über einen Link zu ändern.
- Bei Zweifeln lassen Sie sich die Echtheit einer E-Mail vom Absender telefonisch bestätigen. Nutzen Sie dafür nicht die Telefonnummer aus der E-Mail, sondern suchen Sie diese selbst heraus.
- Vorsicht bei Anhängen mit Formaten wie **.exe** oder **.scr**. Diese können Schadsoftware direkt auf Ihr Gerät laden. Manchmal werden Nutzer oder Nutzerinnen auch durch Doppelendungen wie Dokument **.pdf.exe** in die Irre geführt.
- Verwenden Sie für die diversen Account-Zugänge möglichst eine Zwei-Faktor-Authentisierung. Durch die zweite Stufe der Identifizierung können Kriminelle selbst dann nicht auf Ihre Daten zugreifen, wenn sie bereits Ihr Passwort erbeutet haben.

# Sicherheit in der Informationstechnik

**Kanuclub CJD Kaltenstein Kasse und Mitgliederverwaltung**

**Von:** Hermes <hermesdeutschland@foip2022.jp>
**Gesendet:** Donnerstag, 22. Juni 2023 20:16
**An:** Hermes
**Betreff:** Paket Hermes 982702454772 konnte nicht zugestellt werden

Sehr geehrte Kundin/Kunde,

leider konnten wir die Paketnummer 02137160000699 nicht zustellen.
Dies liegt daran, dass die von Ihnen angegebene Adresse unvollständig zu sein scheint. Daher benötigen wir weitere Angaben, um einen erneuten Versuch zur Zustellung dieses Pakets zu unternehmen.

Status: Nicht erfolgreiche Zustellung: Unzureichende oder fehlerhafte Adresse

Wie geht es weiter?
Ihr Paket wurde an unser lokales Lager zurückgeschickt, wo es für die nächsten zwei Werktage aufbewahrt wird.

Von hier aus können Sie uns eine aktualisierte oder vollständige Adresse für dieses Paket mitteilen, indem Sie <hier klicken>
Für die erneute Zustellung wird eine geringe Gebühr erhoben.
Sie können Ihr Paket auch in unserem Lager in **Bannwarthstraße 5, 22179** abholen.

Mit freundlichen Grüßen
Hermes

---

Wir hoffen, dass diese Nachricht nützlich für Sie war

Eine Emailadresse sieht immer so aus
lokaler Teil@Domänenteil

Der lokale Teil unterliegt bestimmten Konventionen ist aber mehr oder weniger frei wählbar.

Der Domänenteil muss ein gültiger Domänenname sein.

Laut Suchmaschine ist die Domäne des Hermes Paketdienstes myhermes.de

Der Domänenname in dem Mail foip2022.jp weist eindeutig darauf hin, dass dieses Mail nicht von Hermes stammt.

# Sicherheit in der Informationstechnik


Eine Überprüfung der Domäne führt daher auch nach Japan.
Wobei es die Domäne foip2022.jp, wie in der Mail verwendet, anscheinend gar nicht gibt.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

**michael.fischer@kanuclub-vaihingen.de**

**Von:** Zustellung und Gebuehren Service <unoil@tea.bg>
**Gesendet:** Montag, 26. Juni 2023 17:41
**An:** michael.fischer@kanuclub-vaihingen.de
**Betreff:** Sendung ist auf dem Weg: naechste Schritte

**EU-GB ZONE "CENTRAL", UNVERZOLLT**

Hallo,

**Ihre Bestellung aus dem Vereinigten Koenigreich erfordert die Zahlung von Zollgebuehren.**

Um Ihre Lieferung zu erhalten, ist die Zahlung notwendig. Klicken Sie unten, um auf die sichere Online-Zahlung zu gehen und die Berechnung Ihrer Zoelle zu bestaetigen und vorzubereiten. Bitte beachten Sie, dass die Liefertypen limitiert sind, so lange wie Zoelle ausstehen.

Zahlung durchfuehren

| | |
|---|---|
| **Lieferzeit:** | Ankommen bis 20 Uhr |
| **Absender:** | Amazon UK |
| **Zu zahlender Betrag:** | EUR 1.85 |

*Vielen Dank fuer die Nutzung von On Demand Delivery.*

**Express - Excellence. Simply delivered.**

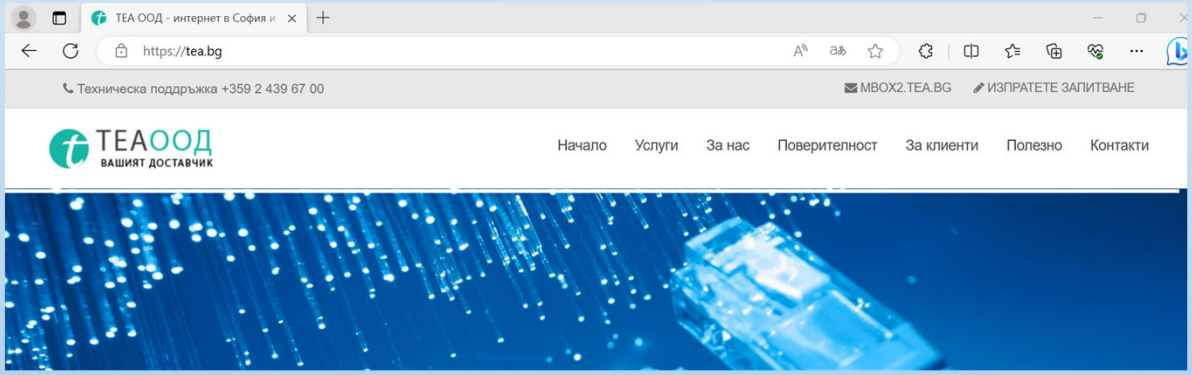
Express | Contact | Privacy Policy | Unsubscribe

2023 © International GmbH. All rights reserved.

1

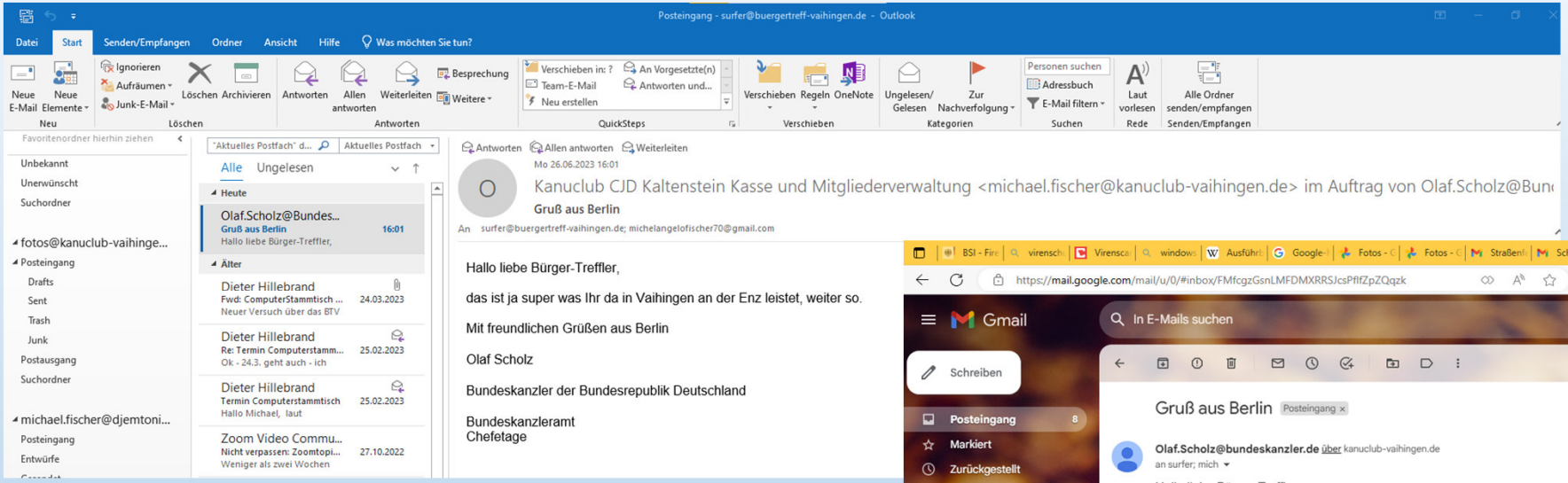
Ich erwarte keine Lieferung aus UK.

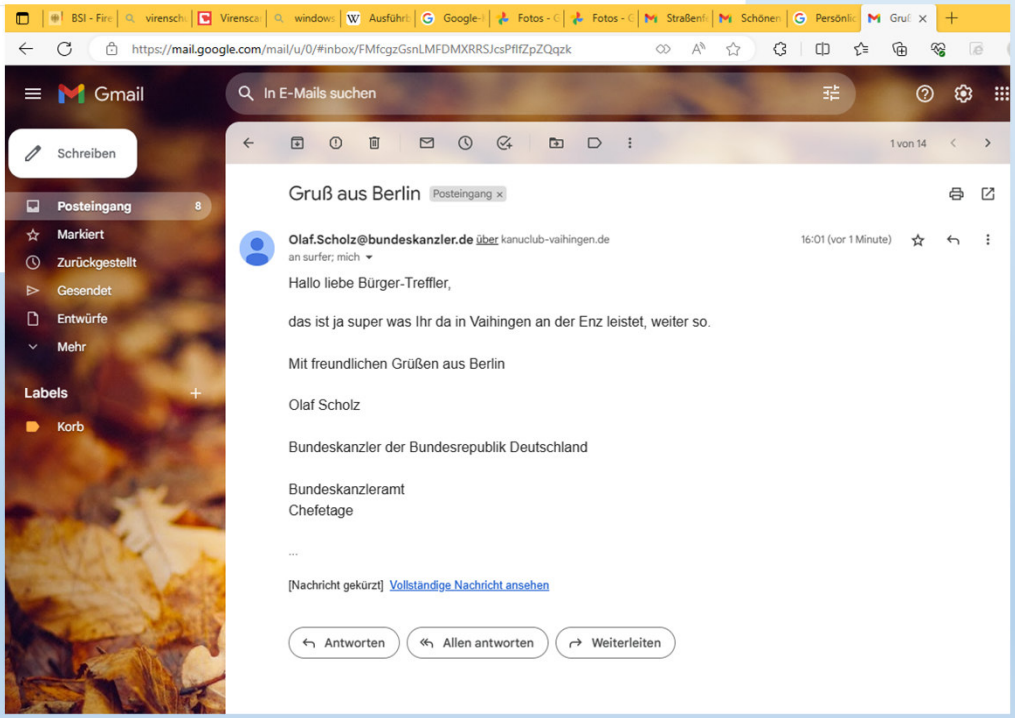
Wenn man die Domäne aus der Emailadresse überprüft, landet man erstaunlicherweise auf einer Internetseite mit kyrillischer Schrift, die in Bulgarien registriert ist.




Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik



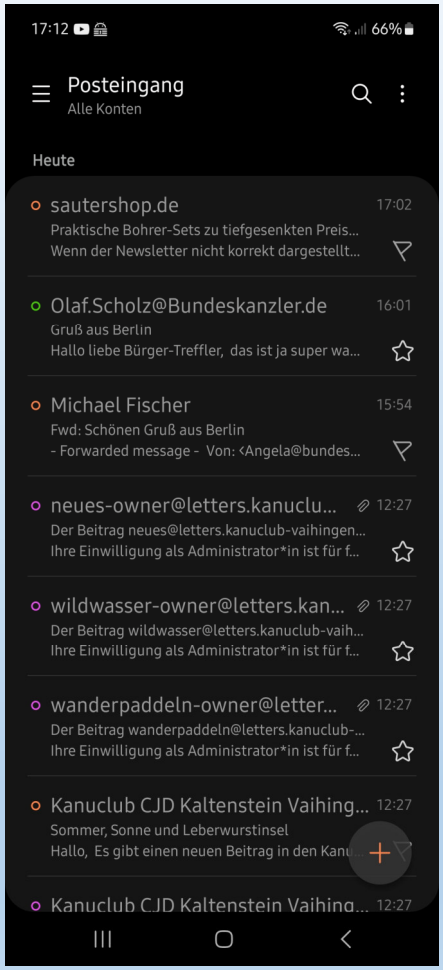



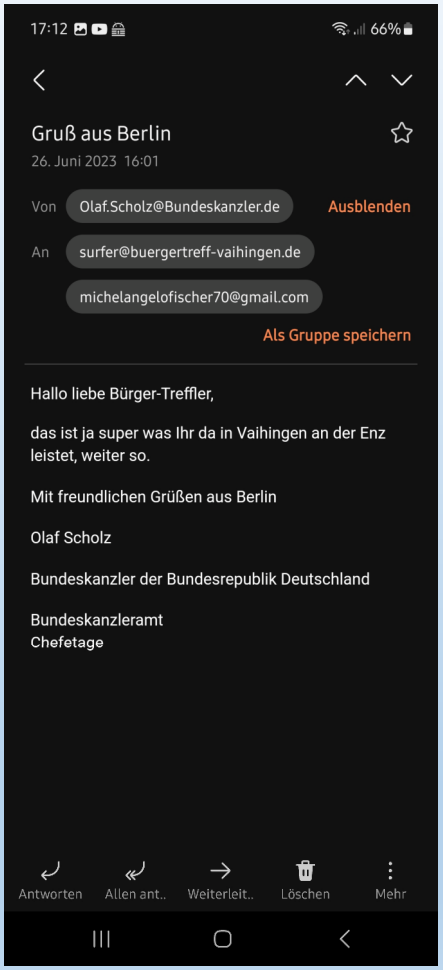

Absendereingaben in Emails sind nicht abgesichert. Sie lassen sich in vielen Mailprogrammen und Mailservern frei gestalten.

Manche Mailprogramme weisen auf diese Manipulation hin, andere dagegen nicht.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

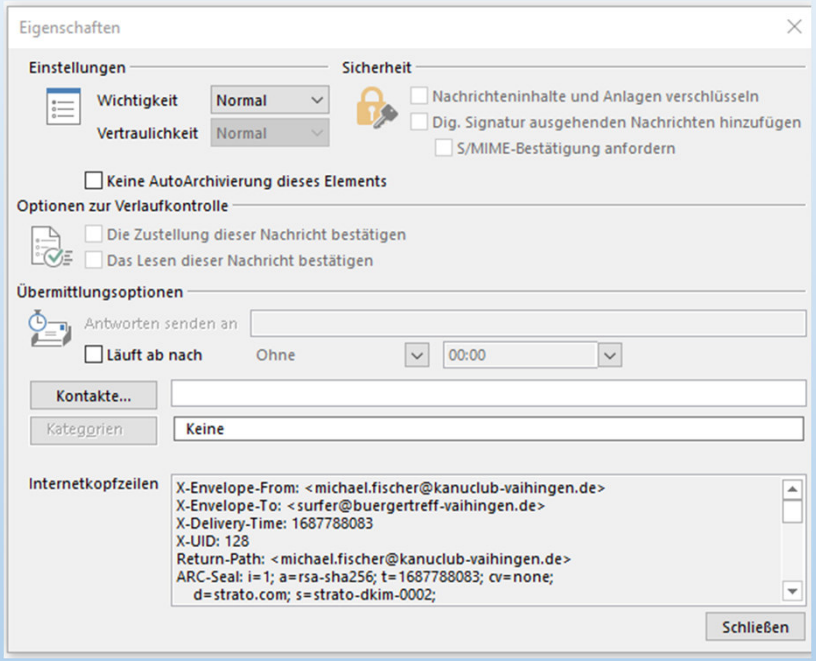


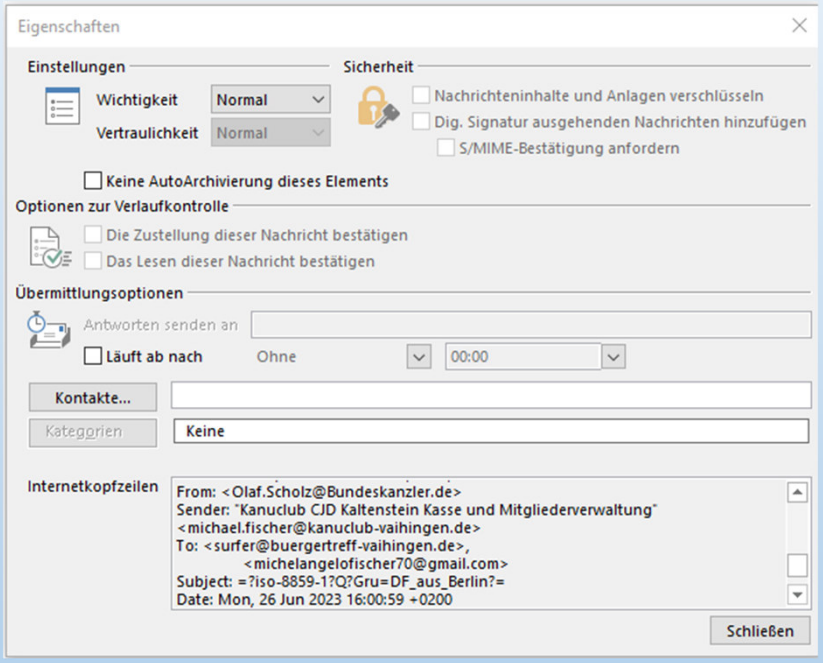




Auf dem Handy mit dem Samsung Mail Client kann man ebenfalls nichts von der Manipulation sehen.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik




Mit manchen Mailprogrammen, hier mit Outlook, kann man die Kopfzeilen einer Mail sichtbar machen, hier wird die Absendermanipulation immer angezeigt.

Michael Fischer, 25.06.2022

# Sicherheit in der Informationstechnik

Dateinamen bestehen aus zwei Teilen, die durch einen Punkt getrennt sind.

**Dateinamen.Erweiterung**

Die Erweiterung besteht, bei Windows, aus drei bis vier Zeichen und ist für die Zuordnung eines Programmes zu der Datei bei einem Doppelklick auf den Dateinamen zuständig ist.

Der . Ist als Zeichen im Dateinamen zulässig.

Windows interpretiert also die drei bis vier Zeichen hinter dem letzten Punkt als Erweiterung.

**Tun Sie das bitte auch.**

**Beispiel.pdf** ist eine Textdatei. Der Dateiname ist Beispiel.

**Beispiel.pdf.bat** ist eine ausführbare Datei, die Windows Befehle enthält und vom Windows Befehlsinterpreter ausgeführt wird. Der Dateiname ist Beispiel.pdf

Michael Fischer, 25.06.2022