GRUNDLAGEN SICHERHEIT IM INTERNET

Ein Leitfaden für einen sicheren Umgang im Netz

Autor und Referent: Klaus Grömminger

1. EINRICHTUNG DES PCs

Verwenden Sie ein sicheres Passwort für Windows oder Ihr Benutzerkonto.

Ein Passwort sollte immer aus mindestens 8 Zeichen mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie z.B. $,&,%,§,@ bestehen

- **Halten Sie Ihr Betriebssystem und Ihre Programme aktuell (Updates).**

  Wir empfehlen Windows so einzustellen das Updates automatisch installiert werden.

  Updates automatisieren
- **Nutzen Sie eine Firewall und ein Antivirenprogramm**.
- **Erstellen Sie regelmäßig Sicherungskopien (Backup).**

  Backup erstellen

2. SCHUTZ VOR VIREN

- Installieren Sie ein bekanntes Antivirenprogramm.

  Hier bieten einige Anbieter auch kostenlose Versionen für Privatanwender an.

  *hier eine kleine Auswahl. Avira, Total AV und Avast. Oder nutzen sie Windows Sicherheit von Microsoft

Führen Sie regelmäßige Scans durch. Beschreibung für Scann mit Windows Sicherheit

- Öffnen Sie keine unbekannten E-Mail-Anhänge.

- Laden Sie Programme nur von vertrauenswürdigen Quellen herunter.

* Die Anbieter sind nur Beispiele und keine Empfehlungen oder Vorgaben.
Für die Auswahl der Anbieter ist jeder selbst verantwortlich.

Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

3. PHISHING MAILS

- Achten Sie auf Absenderadressen in E-Mails und Herkunft von Webseiten.

  Wenn sie eine Mail mit die eine sehr lange Absenderadresse und Zusätze wie z.B. support@bankvonNürtingen-security/com.pw bekommen, oder sie durch hohe Dringlichkeit (z.B. „Handeln sie sofort“) unter Druck setzten, dann ist Vorsicht geboten

  Achten sie auf die Länderkennung von Webseiten, weitere Infos finden sie hier

- Klicken Sie niemals auf verdächtige Links

  Ein gutes Beispiel sind Mails von angeblichen Lieferdiensten mit dem Hinweis dass ein Paket nicht zugestellt werden konnte und auf einem Link der Abholort hinterlegt wurde.

  Oder Meldungen dass sie etwas gewonnen haben.

  Wenn sie mit der Maus auf einen Link gehen ohne zu klicken erscheint die echte URL wohin der Link führt

4. FAKE-WEBSEITEN

- Prüfen sie ob die Webadresse mit https:// beginnt, korrekt geschrieben und das Schloss-Symbol  vorhanden ist. Wenn man auf das Schloss-Symbol klickt wird das Sicherheitszertifikat angezeigt, das fehlt oft bei Fake-Seiten Seriöse Webseiten nutzen meist eine relativ kurze URL z.B. https://www.bahn.de

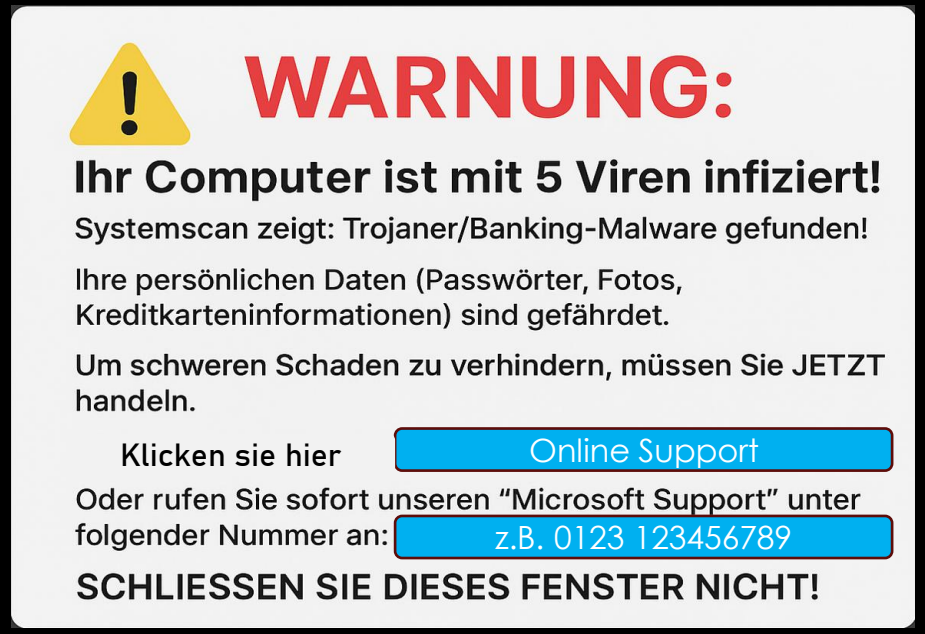
- Achten Sie auf Designmerkmale obwohl sich die Betrüger sehr viel Mühe geben sehen die Firmenlogos manchmal etwas anders aus als das Original

- Nutzen sie die Zwei-Faktor- Authentifizierung (2FA)

2-FAKTOR AUTHENTIFIZIERUNG (2FA)

- Die 2FA sollte für alle Aktionen auf Internetseiten verwendet werden, bei denen es um persönliche Daten und/oder Geld geht.
- Seriöse Anbieter bieten diese an und weisen auch immer darauf hin die 2FA zu verwenden.
- Sie funktioniert mittels eines Passwortes, dem Smartphones und SMS oder einer E-Mail, hierbei wird vor der eigentlichen Aktion an den Anwender eine SMS Nachricht oder eine E-Mail mit einem Code gesendet. Mit der Eingabe von diesem Code erfolgt dann die 2. Authentifizierung. Oder mit Biometrie (Gesichtserkennung/Fingerabdruck)
- Ein gutes Beispiel für so eine 2FA ist die Verwendung von SMS TAN Nummern bei Online-Banking.

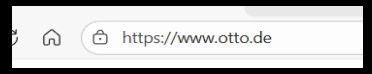
5. BETRÜGERISCHE MELDUNGEN



Für den Fall, dass sie eine solche oder ähnliche Meldung bekommen führen sie **keine** der gewünschten Aktionen aus sondern schließen sie die Webseite mit der Meldung mit dem X oben rechts oder fahren sie ihren Computer direkt am Ein- und Ausschalter herunter.

6. SICHERES EINKAUFEN IM NETZ

- Kaufen Sie nur bei bekannten oder geprüften Online-Shops.
  Und überprüfen Sie ggf. den Shop mit der Seite der Verbraucherzentrale oder Trusted Shops

- Achten Sie auf das Schloss-Symbol in der Adresszeile.
  Hier ein Beispiel von Otto.de 

- Nutzen Sie sichere Zahlungsarten (z. B. PayPal, Kreditkarte mit 2FA oder auf Rechnung).
  Bietet der Anbieter als Zahlungsart nur Vorkasse oder besteht auf Zahlungen mit Kryptowährung handelt es sich mit hoher Wahrscheinlichkeit um Betrug

- Ist ein Impressum vorhanden und sind darin Datenschutzrichtlinien, Telefon Nr. eine richtige Adresse(kein Postfach)und ein Name des Handlungsbevollmächtige angegeben
  Ob es diese Adresse überhaupt gibt kann z.B. auch mit Google Maps geprüft werden

- Bedenken sie, dass bei einem Einkauf aus dem Ausland die Chance im Falle ener Unregelmäßigkeit sein Geld zurückzubekommen gegen Null läuft.

Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

7. UMGANG MIT EIGENEN DATEN

- Geben Sie nur notwendige Informationen an.
- Überlegen Sie, was Sie in sozialen Netzwerken teilen.
- Nutzen Sie Datenschutzeinstellungen auf Websites.
- Löschen Sie alte oder nicht mehr benötigte Konten.

Wichtig:

Abgesehen von der Anmeldung wird sie keine Bank, keine seriöse Webseite und auch kein online-shop jemals auffordern ihr Passwort mitzuteilen oder per Mail zu verschicken.

8. ZUSAMMENFASSUNG

- Bleiben Sie wachsam – gesunder Menschenverstand schützt am besten.
- Aktualisieren Sie regelmäßig Ihre Geräte.
- Nutzen Sie sichere Passwörter und achten Sie auf verdächtige E- Mails.
- Ihre Daten sind wertvoll – gehen Sie sorgsam damit um.

HABEN SIE FRAGEN ODER ANREGUNGEN

Auf meiner Webseite http://www.klaus-g.de/ gibt es weitere Tipps und Informationen
Außerdem können sie dort unter Kontakt auch Fragen stellen.
Oder Anregungen für weitere interessante Themen formulieren auf die ich dann evtl. in weiteren Vorträgen oder auf meiner Webseite eingehen kann.

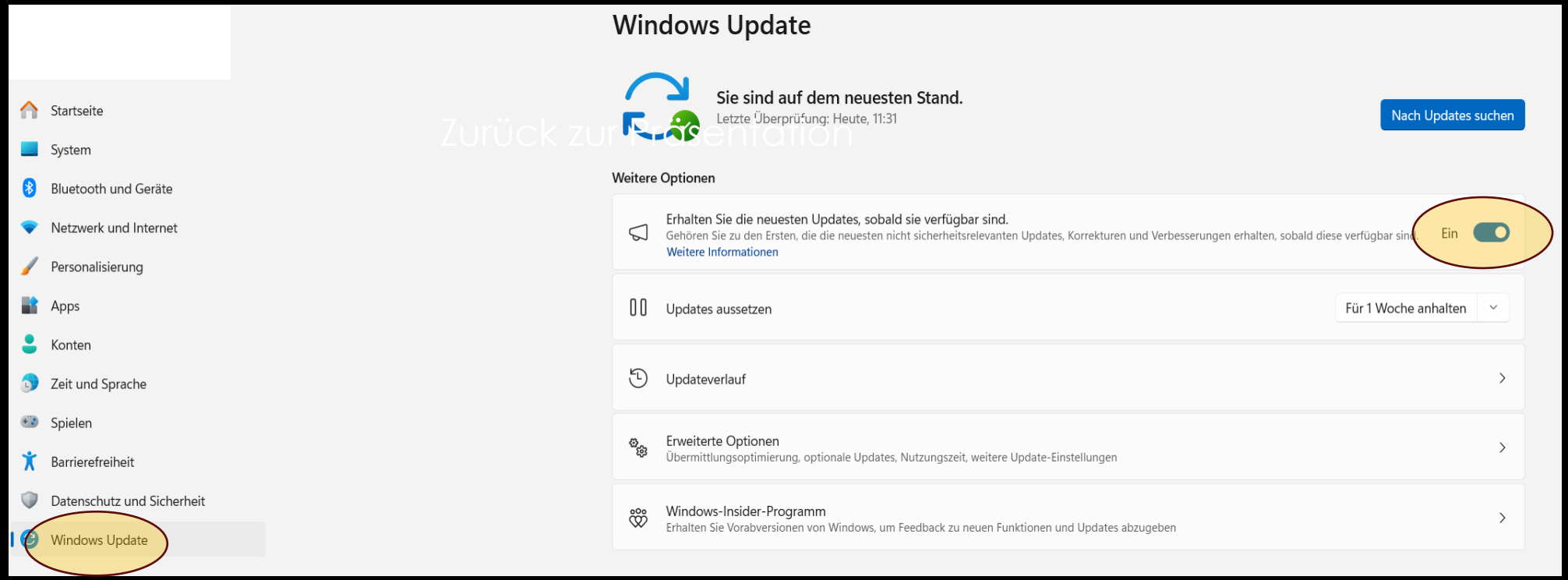
VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Bitte beachten sie das diese Ratschläge keine Garantie für absolute Sicherheit bedeutet und die von mir aufgeführten Vorschläge nur Empfehlungen sind die Ihnen helfen sollen sich sicherer im Internet zubewegen.

BACK UP

UPDATES AUTOMATISIEREN

- Klicken sie auf das Startsymbol unten in der Startleiste
- Jetzt öffnen sie Die Einstellungen
- Nun ganz unten Windows Update anklicken und den Schalter für Neuste Updates auf Ein schalten



Zurück zur Präsentation

Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

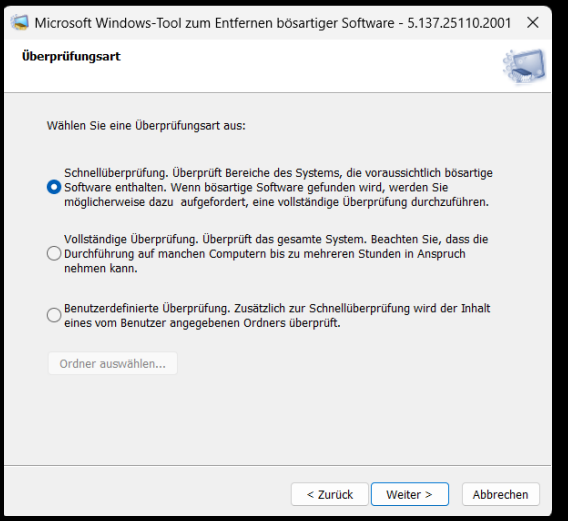
VIRENSCANN MIT DEM TOOL ZUR ENTFERNUNG BÖSARTIGER SOFTWARE MRT VON WINDOWS DURCHFÜHREN

In das Suchfeld der Startzeile unten MRT eingeben und anschließend im dem sich öffnenden Fenster rechts „Als Administrator ausführen“ anklicken. Danach müssen sie die Ausführung des Programms mit „Ja“ bestätigen und im sich öffnenden Fenster auf weiter drücken.

Jetzt können sie auswählen welche Prüfung sie machen wollen.

Sollten sie ihren PC noch nie überprüft haben empfiehlt sich eine vollständige Prüfung, danach genügt in der Regel die Schnellprüfung.

Wichtig das Programm MRT wird über Updates aktuell gehalten und deshalb ist die Einstellung der Automatischen Updates Voraussetzung



Zurück zur Präsentation

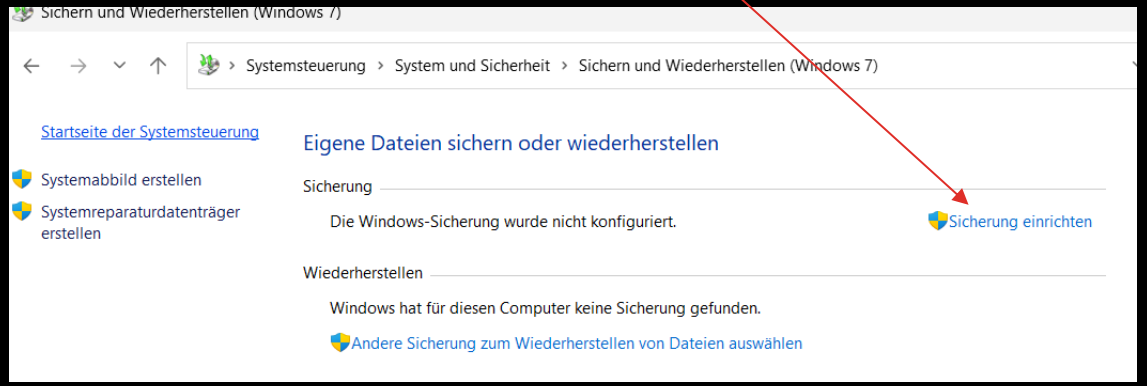
Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

10.01.2026

BACKUP ERSTELLEN

Geben sie in der Startleiste im Suchen Feld Systemsteuerung ein

Dann wählen sie unter dem Punkt System und Sicherheit ganz unten Sichern und Wiederherstellen aus. Anschließend Sicherung einrichten und folgen sie den weiteren Anweisungen (Am besten wird die Sicherung auf einer externen Festplatte gemacht)



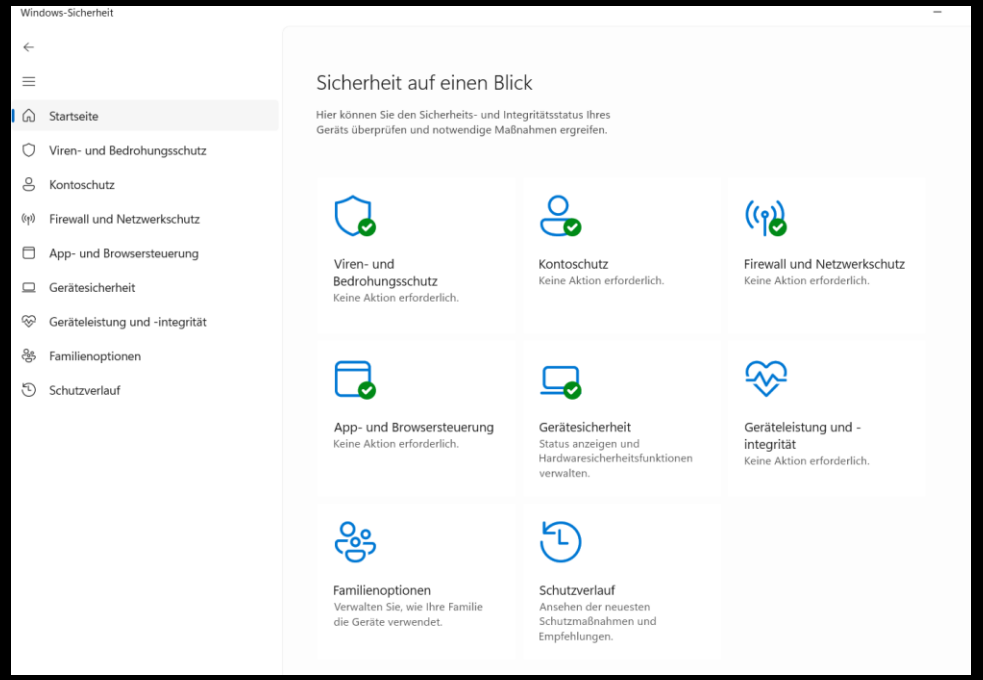
Zurück zur Präsentation

Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

WINDOWS SICHERHEIT

Symbol unten rechts öffnen und danach Windows-Sicherheit anklicken
(Symbol Schild mit hell- und dunkelblauer Farbe)

Hier können die Sicherheitseinstellungen konfiguriert werden



Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de

Zurück zur Päsentation

10.01.2026

INTERNETDOMAINS DIE GERNE FÜR BETRUG GENUTZT WERDEN

Einige **Länderkennungen (ccTLDs)** sind in der Vergangenheit besonders häufig in **Phishing-, Spam- oder Betrugsseiten** aufgetaucht.

Wichtig:
Diese Domains sind nicht grundsätzlich betrügerisch – sie werden nur wegen billiger oder kostenloser Registrierung überdurchschnittlich oft missbraucht.

Hier sind einige Domains die in den Missbrauchs-Statistiken oft weit oben stehen:
- **.tk** (Tokelau)
- **.ml** (Mali)
- **.ga** (Gabon)
- **.cf** (Zentralafrikanische Republik)
- **.gq** (Äquatorialguinea)
- **.cc** (Kokosinseln)
- **.pw** (Palau)

Warum diese oft missbraucht werden:
- Sehr geringe oder gar keine Registrierungskosten
- Weniger strenge Kontrollen bei Domainregistrierungen
- Leicht automatisierbare Massenregistrierungen

Hinweis: Auch Domains mit seriösen Endungen wie **.com**, **.net** oder **.de** werden regelmäßig für Betrug genutzt . Die Endung allein ist kein zuverlässiges Kriterium.

Zurück zur Präsentation

Erstellt von Klaus Grömminger Internet: http://www.klaus-g.de/ Mail: info@klaus-g.de