Computerwissen

Videosprechstunde

Tobias Tesch

COMPUTERWISSEN

Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

Justizminister gehen gegen heimliche Überwachung vor

Sie sind nicht größer als eine Münze und fallen nicht auf, wenn jemand sie in Ihre Jackentasche steckt oder in Ihr Auto legt.

Die Rede ist von Bluetooth-Trackern. Sie sind praktisch, um verlorene Gegenstände wie Koffer oder Schlüssel zu finden – und um Menschen zu überwachen.

Die Missbrauchsgefahr ist groß. Daher beraten die Justizminister der Länder nun über Maßnahmen gegen die heimliche Überwachung, um das Strafrecht anzupassen.

Meine Empfehlung: Warten Sie nicht auf die Änderung des Strafrechts. Das wirkt frühestens in ein paar Jahren. Nutzen Sie meine Anleitung zum Schutz gegen Bluetooth-Tracker aus der Dezember-Ausgabe Ihres PC-Sicherheits-Beraters. Damit erkennen Sie Überwachungsversuche sofort.

Viele Grüße, Ihr

Michael-Alexander Beisecker,
Deutschlands
PC-Sicherheitsexperte Nr. 1

Kostenlose Experten-Hilfe

Exklusiv für Sie als Abonnenten: Die Sofortauskunft mit zuverlässigen Antworten und professionellen Tipps direkt von der Redaktion.

Redaktions-Hotline:
Mittwoch 15:00 bis 18:00 Uhr,
Tel.: 02 08/6 90 79 77

Schützen Sie sich vor dem Missbrauch Ihrer Mobilfunknummer

Nutzen Sie Ihr Handy für das Online-Banking?

Ein Anruf kostete eine 35-jährige Anwältin aus Delhi in Indien die stolze Summe von 5 Millionen Rupien, das entspricht umgerechnet 56.250 €. Sie bemerkte 3 verpasste Anrufe einer unbekannten Rufnummer. Als sie zurückrief, erreichte sie einen vermeintlichen Paketkurier. Der „Kurier" fragte nach ihrer Adresse, um angeblich ein Paket zuzustellen. Einige Zeit danach fand die Frau auf ihren Kontoauszügen zwei große Abbuchungen. Ein Betrüger hatte auf die SIM-Karte ihres Handys zugegriffen. Der Diebstahl über die SIM-Karte passiert auch in Deutschland.

So kommen Betrüger über Ihre SIM-Karte an Ihre Ersparnisse

Der Zugang zu Ihrem Online-Banking-Konto ist doppelt abgesichert: Sie geben Ihre PIN (**P**ersönliche **I**dentifikations**n**ummer) und zusätzlich eine TAN (**T**rans**a**ktions**n**ummer) ein. Die TAN erzeugt ein TAN-Generator oder – und da wird es gefährlich – Sie bekommen diese per Kurznachricht (SMS) auf Ihr Handy gesendet.

Um dieses Sicherheitssystem zu überlisten und in den Besitz der TANs zu gelangen, gehen Betrüger in mehreren Schritten vor:

1. Die Betrüger bringen Ihre Kontonummer und PIN in Erfahrung. Das geht am einfachsten mit einer Betrugs-Mail. Die E-Mail enthält einen Link, der zu einer gefälschten Bankseite führt. Das Opfer gibt seine Anmeldedaten ein und schon haben die Gangster die benötigte Kontonummer und PIN.
2. Die TAN lässt sich am leichtesten über die SIM-Karte des Opfers besorgen. Dazu rufen die Täter bei dessen Telefongesellschaft an und fordern eine neue SIM-Karte an. Aus Sicherheitsgründen müssen sie dazu Fragen beantworten, wie zum Beispiel nach der Anschrift oder dem Geburtsdatum. Diese Informationen erhalten die Täter über einen Telefonanruf als „Kurier" oder sie suchen im Internet danach.
3. Haben die Kriminellen erst einmal Kontonummer, PIN und SIM-Karte, ist der Rest ganz einfach: Sie melden sich beim Online-Banking-Konto an und überweisen das Guthaben plus Überziehungsrahmen auf das eigene Konto.

Maßnahme 1: Stellen Sie sicher, dass Betrüger keine zweite SIM-Karte erhalten

Mobilfunk-Anbieter senden natürlich nicht einfach jedem Anrufer eine zweite SIM-Karte. Sie überprüfen die Berechtigung. Dazu haben Sie beim Abschluss Ihres Mobilfunk-Vertrags ein Passwort vereinbart. Doch wie sicher ist dieses Passwort? Kann ein

>>> Lesen Sie bitte weiter auf Seite 2

>>> Fortsetzung von Seite 1

Fremder das Passwort mit Informationen aus dem Internet erraten? Dann sollten Sie schnellstens ein neues, sicheres Passwort vereinbaren, das sich nicht so leicht knacken lässt.

Nehmen Sie außerdem Ihren Briefkasten unter die Lupe. Kann ein Unbefugter hier leicht Post stehlen? Eine zweite SIM-Karte wird an Ihre Anschrift gesendet. Kriminelle beobachten daher den Briefkasten und holen das Schreiben der Mobilfunkgesellschaft heraus, sobald der Postbote weg ist.

Maßnahme 2: Prüfen Sie die Sicherheit Ihres Online-Banking-Verfahrens

Erhalten Sie Ihre TAN per Nachricht auf Ihr Handy (mTAN/smsTAN)? Dann können Kriminelle über eine Kopie Ihrer E-Mail oder einen Trojaner wie „FakeToken“ auf Ihrem Android-Smartphone an Ihre TAN gelangen. Wechseln Sie schnellstmöglich zu einem dieser sicheren Online-Banking-Verfahren: BestSign, chipTAN, photoTAN oder pushTAN. Nutzen Sie immer zwei Geräte für das Online-Banking: PC und TAN-Generator oder PC und Smartphone.

Mein Tipp: Das pushTAN-Verfahren hat laut dem Landgericht Heilbronn ein „erhöhtes Gefährdungspotential“, wenn dazu ein Smartphone mit TAN-Generator-App und Online-Banking-App verwendet wird (Urteil vom 16.05.2023, Aktenzeichen Bm 6 O 10/23). Das gilt im Grunde auch für chipTAN und photoTAN ohne separaten TAN-Generator.

Maßnahme 3: Setzen Sie das Überweisungslimit pro Tag auf einen möglichst niedrigen Wert

Im Durchschnitt ist das Überweisungslimit für Girokonten auf 3.000 € pro Tag festgelegt. Senken Sie das Überweisungslimit zum Beispiel auf 1.000 €, dann kann ein Täter nicht mehr pro Tag entwenden.

Maßnahme 4: Lassen Sie keine großen Geldbeträge auf Ihrem Girokonto

Verlagern Sie nicht kurzfristig benötigte Geldbeträge auf ein Tagesgeld- oder Festgeldkonto. Sie erhöhen dadurch Ihre Zinseinnahmen und senken das Verlustrisiko.

Maßnahme 5: Überprüfen Sie täglich Ihren Kontostand, zum Beispiel durch E-Mail-Benachrichtigung

Viele Menschen sehen sich ihren Kontostand nur einmal pro Woche oder pro Monat an. Diebstähle bleiben dadurch lange Zeit unentdeckt und die Kriminellen haben viel Zeit, um das Konto leer zu räumen. Schauen Sie daher täglich in Ihr Konto oder richten Sie eine E-Mail-Benachrichtigung ein, damit Sie über Buchungen am Folgetag informiert werden.

Maßnahme 6: Geben Sie Fremden am Telefon keinerlei Auskünfte

Vermeintlich harmlos erscheinende Auskünfte wie die nach Ihrem Wohnsitz haben womöglich schlimme Folgen, wie im Fall der indischen Anwältin (siehe Seite 1). Geben Sie am Telefon insbesondere keine Auskunft zu Finanzdingen und schon gar nicht zu Zugangsdaten oder TANs.

Maßnahme 7: Geben Sie im Internet keine Informationen preis, die sich zum Hacken Ihrer Konten verwenden lassen

Je weniger Informationen Sie in Foren, sozialen Medien und auf Ihrer Webseite preisgeben, umso weniger liefern Sie Kriminellen Material, um Sie zu betrügen und Ihre Konten zu hacken. Achten Sie auch darauf, was auf Ihren Fotos und Videos im Internet zu sehen ist.

Meine Empfehlung: Verlassen Sie sich nicht allein auf die Sicherheitsvorkehrungen Ihres Bankinstituts, sondern treffen Sie die 7 vorstehenden Sicherheitsmaßnahmen zum Schutz Ihrer Ersparnisse.

Ihre Leserfragen

Sehen Sie sich die laufenden Windows-Prozesse an

„Was macht Windows 11 da heimlich auf meinem Rechner im Hintergrund?“

Frage: *„Nach dem Umstieg auf Windows 11 ist mir bei meinem älteren PC ein verdächtiges Verhalten aufgefallen: Nutze ich meinen PC eine Weile nicht, höre ich plötzlich laute Festplatten-Geräusche. Was macht Windows 11 auf meinem Rechner im Hintergrund oder ist da gar ein Schadprogramm aktiv?“, fragte Leser Gunter L. in der Redaktions-Hotline.*

Lösung: Hintergrundaktivitäten sind bei Windows 10 und 11 nicht ungewöhnlich. Windows nutzt Leerlaufzeiten für Systemaufgaben wie das Verwalten von Arbeitsspeicher und Auslagerungsdateien, das Aktualisieren des Suchindexes und das Defragmentieren der Festplatte, die Datensicherung und die Suche nach Schadprogrammen.

Mein Tipp: Haben Sie ein aktuelles Notebook mit SSD statt Festplatte, werden Sie die Hintergrundaktivitäten wahrscheinlich gar nicht bemerken. SSDs arbeiten im Unterschied zu Festplatten lautlos.

Können Hintergrundaktivitäten bösartig sein?

Natürlich kann auch ein Schadprogramm unsichtbar im Hintergrund arbeiten. Der Task-Manager zeigt Ihnen zur Kontrolle die aktiven Hintergrundprozesse an:

1. Klicken Sie die Taskleiste mit der rechten Maustaste an und wählen Sie **Task-Manager**.

2. Finden Sie auf dem Register **Prozesse** in der Liste der **Hintergrundprozesse** unbekannte Anwendungen, ist das äußerst verdächtig. Verlassen Sie den Task-Manager über das **X** rechts oben. Überprüfen Sie Ihr System auf heimlich installierte Werbeprogramme und mögliche Schadprogramme wie im Folgenden beschrieben.
3. Zur Prüfung auf Werbeprogramme öffnen Sie die **Einstellungen** (⊞ + I) und klicken auf **Apps**. Sehen Sie die Liste der Apps durch. Finden Sie hier unbekannte oder nicht benötigte Programme, klicken Sie diese Einträge an und wählen **Deinstallieren**.

Wie Sie eine Schadprogramm-Kontrolle durchführen

Führen Sie bei verdächtigen Hintergrundaktivitäten eine Prüfung mit dem installierten und eine mit einem externen Antiviren-Programm durch (Vier-Augen-Prinzip). Die externe Prüfung klappt mit dem Online-Virenscanner von ESET ganz einfach:

1. Öffnen Sie die Webseite des Online-Virenscanners: https://www.eset.com/de/home/online-scanner/
2. Klicken Sie auf **JETZT PRÜFEN**. Der Viren-Scanner **esetonlinescanner.exe** wird heruntergeladen.
3. Öffnen Sie Ihren Ordner **Downloads** und starten Sie **esetonlinescanner.exe** mit einem Doppelklick. Das Programm ist sofort lauffähig.
4. Klicken Sie auf **Computerscan** und bestätigen Sie die Sicherheitsabfrage der **Benutzerkontensteuerung** mit einem Klick auf **Ja**.
5. Klicken Sie auf **Vollständiger Scan** und wählen Sie **Erkennung und Verschieben von potenziell unerwünschten Anwendungen in die Quarantäne durch ESET aktivieren**.
6. Klicken Sie auf **Prüfung starten**. Ihr PC wird jetzt auf Schadprogramme untersucht und gefundene Schadprogramme werden in Quarantäne genommen.
7. Starten Sie Ihren PC nach dem Virenscan neu und prüfen Sie, ob weiterhin Hintergrundaktivitäten stattfinden.

Meine Empfehlung: Führen Sie die Schadprogramm-Kontrolle mit ESET regelmäßig einmal im Monat durch, auch wenn Sie keine Hintergrundaktivitäten feststellen. Das erhöht die Sicherheit Ihres PC-Systems für den Fall, dass Ihr installiertes Antiviren-Programm einmal ein Schadprogramm übersehen sollte.

Heben Sie die Sperre auf oder nutzen Sie zum Download Firefox

„Warum lädt der Edge-Browser empfohlene Tools nicht herunter?"

Frage: *„Ich wollte mit dem Edge-Browser ein Tool herunterladen. Als ich per Klick auf den Download-Pfeil in Edge in die Downloads-Übersicht geschaut habe, stand da: „XY kann nicht sicher heruntergeladen werden." Da habe ich das Tool mit dem Firefox-Browser geladen. Hier gab es keine Fehlermeldung. Woran liegt das und wie kann ich Tools auch mit Edge laden?", fragte Leser Peter T.*

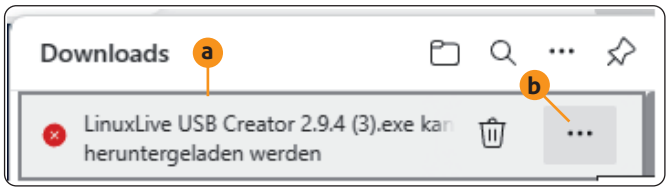
Lösung: Edge blockiert Downloads über unverschlüsselte Verbindungen. Sie erkennen dies daran, dass die Download-Adresse mit **http://** statt **https://** beginnt.

Die Sperrung erfolgt auch, wenn Sie ein Tool über eine Webseite mit verschlüsselter Verbindung herunterladen und von dort nach dem Klicken auf die Download-Schaltfläche auf eine unverschlüsselte Verbindung weitergeleitet werden.

Im Internet werden noch viele Tools über http:// angeboten. Sie stammen meist von privaten Entwicklern, die den Kostenaufwand für eine verschlüsselte Verbindung scheuen.

Sind Sie sich sicher, dass die betreffende Quelle vertrauenswürdig ist, umgehen Sie die Download-Sperre wie folgt:

1. Öffnen Sie Edge und drücken Sie die Tastenkombination Strg + J, um die **Downloads**-Übersicht anzuzeigen.



Edge meldet zuerst, dass es das gewünschte Tool nicht herunterladen kann – aber Sie haben eine Lösung.

2. Bewegen Sie den Mauszeiger auf den gesperrten Download **a**. Klicken Sie auf ··· **b** und wählen Sie **Beibehalten**.
3. Es erscheint eine Meldung, dass die Datei nicht sicher heruntergeladen werden könne. Beachten Sie diese Meldung nicht weiter und klicken Sie auf **Trotzdem behalten**.

Die Datei wird nun heruntergeladen und steht Ihnen zur Verfügung. Ist Ihnen dieses Verfahren zu umständlich, verwenden Sie für den Download den Browser Firefox. Er sperrt die Downloads bei http-Verbindungen nicht.

Meine Empfehlung: Laden Sie Tools nach Möglichkeit über verschlüsselte https-Verbindungen herunter. Ist das nicht möglich und die betreffende Webseite ist vertrauenswürdig, ist auch der unverschlüsselte Download sicher. Das gilt zum Beispiel für alle in Ihrem PC-Sicherheits-Berater empfohlenen Webseiten.

So verlieren Sie nach einem Windows-Totalausfall nicht Ihre Daten

Windows startet nicht mehr oder ist schwer beschädigt: Dieser USB-Stick rettet Ihre Daten

Leser Gert W. wollte weg von Windows, denn sein acht Jahre alter PC war nicht für den Umstieg auf Windows 11 geeignet. Daher installierte Gert W. testweise Linux. Auf seiner Festplatte war dafür noch reichlich Platz. Doch oh Schreck: Nach der Installation von Linux startete sein Windows 10 nicht mehr. Es machte ihm zwar nichts aus, jetzt ausschließlich mit Linux weiterzuarbeiten. Aber wie sollte er an seine Daten herankommen, die in der Partition mit Windows 10 gespeichert waren? Seine Datensicherung hatte er unter Windows erstellt und konnte sie unter Linux nicht wiederherstellen. Für solche Fälle, in denen Windows nicht mehr zur Verfügung steht, empfehle ich einen speziellen Rettungs-USB-Stick. Er half auch hier: Gert W. bootete seinen PC damit, kopierte seine Daten und speicherte sie anschließend unter Linux ab.

Es geht auch ohne Windows: Wie Sie an Ihre Daten kommen, wenn Windows nicht mehr startet

Früher wurde zur Rettung von Windows und der Daten eine Rettungs-CD oder -DVD verwendet. Heute ist in vielen PCs, vor allem Notebooks, kein optisches Laufwerk mehr enthalten.

Daher empfehle ich für Rettungseinsätze einen USB-Stick. Das Betriebssystem auf dem USB-Stick lässt sich zudem aktualisieren und Sie können auf dem USB-Stick Daten abspeichern.

Das sollten Sie beim USB-Stick beachten

Zur Installation des Rettungssystems reicht bereits ein USB-Stick mit 1 GB Speicherkapazität aus. Dann ist darauf aber kein Platz mehr für Ihre Daten frei.

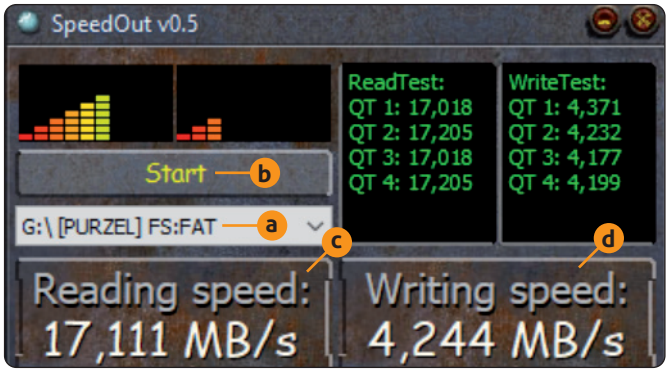
Je nach Umfang Ihrer Daten empfehle ich Ihnen daher einen USB-Stick mit 256 GB oder 512 GB. Die Preise liegen aktuell bei rund 20 € bzw. 45 €.

Testen Sie die Geschwindigkeit Ihres USB-Sticks

Damit die Datenrettung nicht zur Geduldsprobe wird, sollte Ihr USB-Stick für die Datenrettung eine hohe Schreib- und Lesegeschwindigkeit haben.

Messen Sie die Zugriffsgeschwindigkeit Ihrer vorhandenen USB-Sticks mit dem kostenlosen Tool SpeedOut:

1. Geben Sie folgende Adresse in Ihren Browser ein, um die aktuelle Version von SpeedOut herunterzuladen: https://pendriveapps.com/downloads/SpeedOut_0.5.zip
2. Öffnen Sie den Ordner **Downloads** und darin das heruntergeladene Archiv **SpeedOut_0.5.zip**. Starten Sie das enthaltene Programm **SpeedOut_0.5.exe** durch einen Doppelklick.
3. Stecken Sie den USB-Stick an den schnellsten USB-Anschluss (USB 3.0, USB 3.1 oder USB 3.2) Ihres PCs und wählen Sie das Laufwerk in SpeedOut aus (a).
4. Klicken Sie auf **Start** (b) und lesen Sie nach dem Ende des Tests die Lese- (c) und Schreibgeschwindigkeit (d) ab.



Wählen Sie in der Liste das Gerät aus und nehmen Sie die Einstellung per Klick auf den Schalter vor.

Aktuelle USB-Sticks erreichen nach Herstellerangaben Lesegeschwindigkeiten von bis zu 400 MB/s und Schreibgeschwindigkeiten von bis zu 60 MB/s.

In der Praxis lassen sich meist jedoch höchstens 100 MB/s beim Lesen und 40 MB/s beim Schreiben erreichen. Sind Ihre vorhandenen USB-Sticks deutlich langsamer, kaufen Sie sich für den Rettungs-USB-Stick einen neuen USB-Stick.

Installieren Sie „Linux Live USB Creator" auf Ihrem PC

Zum Einrichten Ihres bootfähigen USB-Sticks verwenden Sie das kostenlose OpenSource-Programm „LiLi" (**Li**nux **Li**ve USB Creator) mit deutscher Oberfläche:

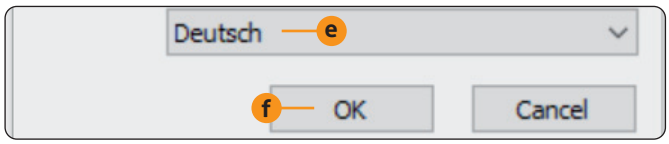
1. Laden Sie die aktuelle Version 2.9 von LiLi von dieser Webseite herunter:
   https://www.linuxliveusb.com/de/download
   Klicken Sie auf die rote Schaltfläche **Download LiLi**, um das 5,9 MB kleine Programm für Windows 10 und 11 herunterzuladen.

Mein Tipp: Verwenden Sie zum Download den Edge-Browser, erhalten Sie womöglich die Meldung: „LinuxLive USB Creator 2.9.4.exe kann nicht sicher heruntergeladen werden." Weichen Sie dann auf einen anderen Browser wie Firefox aus oder beachten Sie die Hinweise auf Seite 3, um das Tool zu erhalten.

2. Schließen Sie alle anderen Programme und starten Sie das heruntergeladene Programm **LinuxLive USB Creator 2.9.4.exe** als Administrator. Beachten Sie, dass der Dateiname die Versionsangabe enthält und daher in Ihrem Fall abweichen kann.

Mein Tipp: Erhalten Sie während der Installation eine Warnung von Ihrem Antiviren-Programm, dass das Programm 7z (Seven ZIP) installiert werden soll, dann blockieren Sie das Programm nicht. Es handelt sich dabei um das Archivprogramm, das LiLi zum Entpacken der Dateien auf dem USB-Stick benötigt. Ohne 7z wird der USB-Stick daher nicht korrekt erstellt und funktioniert nicht.

3. Es erscheint das Fenster zur Sprachauswahl. **Deutsch** (e) ist vorgewählt. Klicken Sie auf **OK** (f) und folgen Sie dem Assistenten. Am Ende der Installation startet LiLi automatisch.



Während der Installation ist die Oberfläche noch Englisch, nach dieser Auswahl wechselt sie automatisch zu Deutsch.

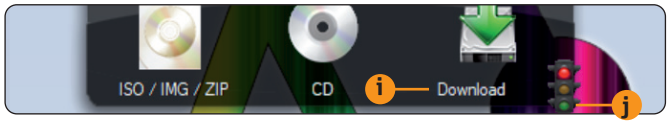
So richten Sie den Rettungs-USB-Stick mit Linux ein

Zum Einrichten des Rettungs-USB-Sticks sind 5 Schritte erforderlich, die Ihnen LiLi direkt anzeigt. Ich führe Sie durch den Vorgang und zeige Ihnen, auf was es ankommt:

1. Stecken Sie den USB-Stick ein und wählen Sie ihn bei **SCHRITT 1** aus (g). Die Ampel (h) springt auf **Grün**, wenn der ausgewählte USB-Stick verwendbar ist.

Achten Sie darauf, dass der USB-Stick an einem schnellen Anschluss mit USB 3.x steckt.

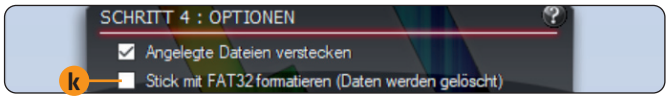
2. Klicken Sie auf **Download** (i) und wählen Sie **Linux Mint 17.2 „Rafaela" (Cinnamon) DVD**, denn die „Zimt"-Oberfläche (Cinnamon) sieht so ähnlich aus wie die von Windows 10 und 11. Starten Sie den Download mit einem Klick auf **Automatisch** und wählen Sie einen Ordner auf der Festplatte für den Download aus. Warten Sie mit dem nächsten Schritt, bis die Ampel (j) **Grün** zeigt.



Wählen Sie das Linux für Ihren USB-Stick.

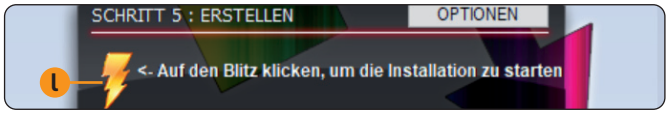
3. Unter **SCHRITT 3** sehen Sie jetzt einen Schieberegler. Ziehen Sie diesen Regler nach rechts, bis Sie ausreichend Platzbedarf für Ihre Daten ausgewählt haben. Lassen Sie den Schalter auf 0 MB, können Sie im Rettungseinsatz keine Daten speichern!

4. Ihr USB-Stick muss für Linux mit dem Dateisystem FAT32 formatiert sein. Dazu aktivieren Sie bei **SCHRITT 4** die Formatieroption (k). Auf dem USB-Stick vorhandene Daten werden beim Formatieren gelöscht!



Aktivieren Sie das Formatieren des USB-Sticks mit FAT32.

5. Klicken Sie auf das **Blitz**-Symbol (l). Linux wird nun auf dem USB-Stick eingerichtet. Die einzelnen Schritte werden Ihnen angezeigt. Es dauert rund 10 Minuten, bis der USB-Stick fertig ist.



Noch ein Klick, dann ist Ihr Rettungs-USB-Stick eingerichtet.

Wie Sie Ihre Daten mit dem neuen USB-Stick retten

So retten Sie im Ernstfall Ihre Daten mit Ihrem neuen USB-Stick:

1. Fahren Sie Ihren nicht mehr reagierenden PC herunter bzw. schalten Sie diesen aus. Dann stecken Sie den Rettungs-USB-Stick an einen USB-Steckplatz Ihres PCs.
2. Schalten Sie den PC ein und drücken Sie unmittelbar danach die Taste zum Aufruf des Boot-Menüs mehrfach schnell hintereinander. Das ist meist F11 oder F12.
3. Erscheint kein Boot-Menü, rufen Sie stattdessen die BIOS-/UEFI-Einstellungen auf. Über welche Taste das geht, steht auf dem Bildschirm und im Handbuch zu Ihrem PC, meist ist es Entf, Esc oder F2. Verschwindet der Bildschirm so schnell, dass Sie ihn nicht lesen können, starten Sie den PC erneut und drücken die Taste Pause, sobald das erste sichtbare Bild erscheint. Jetzt können Sie die Anzeige in Ruhe lesen und dort nach Hinweisen zur Funktionstaste suchen.
4. Stellen Sie die Boot-Reihenfolge um, sodass Ihr Rechner beim nächsten Start vom USB-Stick bootet. Dann speichern Sie die neuen Einstellungen ab und verlassen das Boot-Menü oder die BIOS-Oberfläche. Ihr Rechner bootet jetzt vom Rettungs-USB-Stick mit Linux.
5. Nachdem die grafische Oberfläche angezeigt wird, greifen Sie über das Ordner-Symbol mit der Bezeichnung **home** auf die Daten auf Ihrem Rechner zu.
6. Wählen Sie alle gewünschten Datendateien aus und kopieren Sie diese auf Ihren USB-Stick. Dann fahren Sie Ihren PC herunter. Jetzt ist Ihr Rettungs-USB-Stick komplett und enthält Ihr Windows und Ihre Daten.

Meine Empfehlung: Warten Sie nicht bis zum Absturz Ihres Windows, sondern erstellen Sie den Rettungs-USB-Stick jetzt. Dann haben Sie ihn im Notfall griffbereit. Wir können Sie auch bei der Datenrettung unterstützen, wenn Sie den PC-Notruf-Support gebucht haben und unter Linux die Fernwartung Anydesk installieren.

Geben Sie die Adresse der PayPal-Webseite manuell ein und klicken Sie dazu nie auf E-Mail-Links

Die 7 Arten des PayPal-Betrugs und wie Sie sich von jetzt an 100 Prozent sicher davor schützen

Der Bezahldienst PayPal (wörtlich übersetzt „Bezahlfreund") birgt Risiken, wie Leser Karl-Heinz F. feststellte. Ein vermeintlich harmloser Klick in eine gefälschte PayPal-E-Mail und sein Guthaben war weg. Normalerweise hatte er nur wenig Geld auf seinem PayPal-Konto, aber diesmal waren es über 1.000 €. Er hatte das Geld auf das PayPal-Konto überwiesen, um online einen neuen Fernseher zu kaufen. Damit Sie kein Geld bei PayPal verlieren oder sensible Daten preisgeben, nehmen Sie bei E-Mails mit PayPal-Absender die folgende Checkliste zur Hand. Überprüfen Sie die E-Mail Frage für Frage nach Betrugsanzeichen. Denn bei „PayPal"-E-Mails geht es nur selten mit rechten Dingen zu.

1. **Werden Sie in der PayPal-Mail aufgefordert, Ihr Passwort zurückzusetzen?**
   - ☐ **Ja:** Haben Sie das Zurücksetzen Ihres Passwortes nicht tatsächlich angefordert, handelt es sich um einen Betrugsversuch oder Hacker versuchen, Ihr PayPal-Konto zu übernehmen. Ändern Sie das Passwort Ihres E-Mail-Kontos und löschen Sie die E-Mail.
   - ☐ **Nein**

2. **Hat die PayPal-E-Mail einen Betreff wie: „Ihr Konto wird demnächst gesperrt", oder: „PayPal hat Ihre Finanzen eingefroren"?**
   - ☐ **Ja:** Betrüger wollen Sie über einen Link in der E-Mail auf eine gefälschte PayPal-Seite leiten, um an Ihre PayPal-Zugangsdaten, Kreditkarten-Daten und Bankdaten zu gelangen. Löschen Sie die E-Mail.
   - ☐ **Nein**

3. **Werden Sie auf eine angeblich eingegangene oder erforderliche Zahlung hingewiesen?**
   - ☐ **Ja:** Betrüger wollen Sie dazu bringen, Geld auf deren Konto zu überweisen. Dazu wird teilweise auch eine gefälschte Rechnung angehängt. Achtung: Das Öffnen des Anhangs kann zur Installation eines Schadprogramms führen. Löschen Sie die E-Mail, sie ist Betrug!
   - ☐ **Nein**

4. **Sollen Sie eine angebliche Bestellung bestätigen?**
   - ☐ **Ja:** Die Bestellung existiert nicht. Betrüger wollen Sie über einen Link in der E-Mail auf eine gefälschte PayPal-Webseite leiten, um dann Ihre PayPal-Zugangsdaten zu erhalten. Löschen Sie die E-Mail unverzüglich.
   - ☐ **Nein**

5. **Meldet sich ein angeblicher Käufer, weil ein Paket nicht angekommen sein soll?**
   - ☐ **Ja:** Betrüger behaupten, ein bereits bezahltes Paket von Ihnen sei nicht angekommen, und Sie sollen den Kaufbetrag nun per PayPal zurückerstatten. Dieser Betrugsversuch ist gefährlich, wenn Sie privat Waren über Amazon oder eBay verkaufen. Löschen Sie die E-Mail und bezahlen Sie nicht.
   - ☐ **Nein**

6. **Haben Sie eine SMS (Kurznachricht) mit einer angeblichen Betrugswarnung von PayPal erhalten?**
   - ☐ **Ja:** Solche Kurznachrichten stammen von Kriminellen. Sie behaupten darin, es hätte verdächtige Aktivitäten bei Ihrem PayPal-Konto oder einen unbefugten Zugriffsversuch gegeben. Die Kurznachrichten enthalten einen Link, der zu einer gefälschten PayPal-Webseite führt. Gibt ein Empfänger der SMS dort seine Zugangsdaten ein, hacken die Betrüger damit sein PayPal-Konto und räumen es leer. Löschen Sie solche Kurznachrichten sofort.
   - ☐ **Nein**

7. **Erhalten Sie von fremden Personen Nachrichten, dass sie E-Mails von Ihrem PayPal-Konto erhalten haben, oder meldet sich deswegen die Polizei?**
   - ☐ **Ja:** Kriminelle haben Ihr PayPal-Konto gehackt und missbrauchen es für den Versand der Nachrichten. Ändern Sie sofort das Passwort Ihres PayPal-Kontos und richten Sie die 2-Faktor-Authentifizierung zum Schutz Ihres Kontos ein. Erstatten Sie wegen des Hackens Ihres PayPal-Kontos Anzeige bei der örtlichen Polizeiwache oder bei https://online-strafanzeige.de/.
   - ☐ **Nein**

Auswertung: Haben Sie eine Frage mit **Ja** beantwortet, ist die betreffende E-Mail ein Betrugsversuch (Fragen 1 bis 6) oder es wurde Ihr PayPal-Konto gehackt (Frage 7). Löschen Sie Betrugs-Mails, ohne darauf zu reagieren. Sie erhalten sonst noch mehr solcher Mails. Klicken Sie in keinem Fall auf einen Link in einer PayPal-E-Mail, öffnen Sie keinen Anhang und befolgen Sie keine Anweisung. Erscheint Ihnen eine E-Mail echt, melden Sie sich manuell bei PayPal an. Zur Anmeldeseite gelangen Sie über die Adresse www.paypal.com. Im Falle eines **Neins** müssen Sie nichts weiter unternehmen.

Ihr sicherer Schutz: Prüfen Sie jede eingegangene E-Mail vor dem Öffnen

3 Sekunden reichen: So erkennen Sie Betrugs-E-Mails endlich sicher, ohne viel Zeit zu verlieren

Der Bericht des Bundesamts für die Sicherheit in der Informationstechnik (BSI) spricht Bände: Von den 616.000 täglich in der Bundesverwaltung eingehenden E-Mails im August 2023 waren 290.000 Spam-E-Mails, also unerwünschte E-Mails. Neben Werbung gehören dazu Betrugsversuche und E-Mails mit schädlichen Inhalten. Die meisten dieser E-Mails wurden automatisch ausgefiltert (265.000), übrig blieben 25.000 unerwünschte E-Mails täglich. Zum schnellen und trotzdem sicheren Aussortieren dieser E-Mails wenden die Behörden die nachstehende 3-Sekunden-Prüfung an, die ich auch Ihnen wärmstens empfehle. Sie sparen damit viel Zeit und sind gut vor Erpresser-Trojanern und Datenmissbrauch geschützt.

Die 3-Sekunden-Prüfung ist im Grunde ganz einfach: Achten Sie auf die 3 wichtigsten Punkte zum Erkennen von Betrugs-Mails. Das sind Absender, Betreff und Anhang.

Berücksichtigen Sie dabei, dass Sie den Absenderangaben und Inhalten von Betrugs-Mails nicht trauen dürfen. Hier wird gefälscht und gelogen, dass sich die Balken biegen!

Checkpunkt 1: Kennen Sie den Absender?

Blicken Sie zuerst auf den Absender a. Ist der Absender eine Privatperson, sollten Sie ihn kennen.

Bei einem Unternehmen: Haben Sie eine Geschäftsbeziehung mit dem Unternehmen?

Kennen Sie den Absender nicht oder haben keine Geschäftsbeziehung, ist die Sache einfach: Löschen Sie die E-Mail sofort.

Mein Tipp: Erhalten Sie ständig E-Mails von neuen Kontakten, löschen Sie die E-Mails unbekannter Absender nicht einfach, sondern prüfen Sie sie mit den weiteren Checkpunkten.

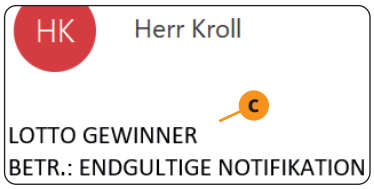
Kennen Sie den Absender, prüfen Sie die Absenderadresse b ganz genau. Sie wird entweder direkt in der E-Mail angezeigt oder Sie lassen den Mauszeiger über dem Absender schweben, damit die Adresse erscheint.

Betrug entlarvt: Die echte Volksbank verwendet Adressen wie info@vr.de oder info@bvr.de, nicht info@diskclick.com.

Fragen Sie sich: Passt die E-Mail-Adresse des Absenders zu der Person oder dem Unternehmen? Lautet die Antwort nein, handelt es sich um einen Betrugsversuch. Löschen Sie die E-Mail.

Checkpunkt 2: Erscheint Ihnen der Text in der Betreffzeile und in der E-Mail sinnvoll und vertrauenswürdig?

Prüfen Sie den Betreff-Text kritisch. Ist der Absender ein Bekannter, wird er Sie zum Beispiel nicht über einen Lotteriegewinn informieren c oder Ihnen eine Mahnung, einen Lieferschein oder eine Rechnung schicken.



Sie kennen einen Herrn Kroll, aber er ist nicht bei einer Lottogesellschaft beschäftigt? Dann löschen Sie diese Mail sofort!

Checkpunkt 3: Erwarten Sie einen Anhang, enthält die E-Mail einen oder mehrere Links?

Die größte Gefahr geht von E-Mails mit Anhang aus, denn im Fall einer Betrugs-Mail erwartet Sie im Anhang meist ein Schadprogramm wie ein Erpresser-Trojaner. Dabei sind die Schadprogramme oft getarnt, zum Beispiel als Office-Dokument, PDF-Datei oder Bilder junger, attraktiver Damen.

Eine weitere Gefahr sind Links in E-Mails, denn sie führen im Betrugsfall zu gefälschten Bankseiten, kostenpflichtigen Online-Angeboten oder gefährlichen Webseiten mit Schadprogrammen.

E-Mails mit Anhang und Links sind verdächtig. Löschen Sie die E-Mails, wenn Sie diese, den Anhang oder den oder die Links nicht erwartet haben.

Meine Empfehlung: Löschen Sie lieber eine E-Mail zu viel, als eine gefährliche Webseite oder ein Schadprogramm zu riskieren. Lassen Sie sich durch alarmierende Begriffe wie „Mahnung“, „Rechnung“ oder „Kontosperrung“ nicht verunsichern und lassen Sie sich auch von angebotenen Geldbeträgen nicht locken. Damit wollen Betrüger erreichen, dass Sie unüberlegt handeln. Aber nicht mit Ihnen!

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Computerwissen, ein Verlagsbereich der VNR Verlag für die Deutsche Wirtschaft AG
Vorstand: Richard Rentrop, Bonn
Redaktionell Verantwortlicher: Sven Udert, VNR Verlag für die deutsche Wirtschaft AG, Adresse siehe nebenstehend

Chefredakteur: Michael-Alexander Beisecker
Gutachter: Rudolf Ring, Mülheim; Ute Samenfink, Freiburg
Druck und Belichtung: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim
Adresse: VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, 53177 Bonn
Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165
Dieses Produkt besteht aus FSC®-zertifiziertem Papier.
Die Beiträge in „Ihr PC-Sicherheits-Berater“ wurden mit Sorgfalt recherchiert und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Daher ist eine Haftung, auch für telefonische Auskünfte, ausgeschlossen.

Seien Sie bei der Suche nach diesen 10 Promis vorsichtig

Suchen Sie im Internet nach Promis? Gefährlich!

Nach dem Kinofilm „Barbie" fragte Ute B. ihren Mann Stefan nach weiteren Filmen des Hauptdarstellers Ryan Gosling. Stefan fand Meldungen zu einer neuen Kinoversion von „Ein Colt für alle Fälle". Doch als er eine der Meldungen anklickte, erschien eine betrügerische Viren-Warnung. Kein Einzelfall, denn die Suche nach Prominenten im Internet ist riskant.

Eine aktuelle Studie des Sicherheitsunternehmens McAfee zeigt, dass die Suche nach Ryan Gosling am häufigsten für Online-Betrugsversuche verwendet wird. Doch auch die Namen weiterer Prominenten werden ohne deren Wissen von Kriminellen missbraucht.

Die Top 10 der Promis, deren Namen für Betrugs-Attacken verwendet werden

	Name	Bekannt durch
1.	Ryan Gosling	Kinofilm „Barbie"
2.	Emily Blunt	Kinofilm „Oppenheimer"
3.	Jennifer Lopez	Musikerin & Schauspielerin
4.	Zendaya	Musikerin & Schauspielerin
5.	Kevin Costner	Schauspieler & Regisseur
6.	Elon Musk	Tech-Unternehmer
7.	Al Roker	Autor, Journalist, US-Wetter-Moderator
8.	Margot Robbie	Kinofilm „Barbie"
9.	Bad Bunny	Sänger, Spotify-Megastar
10.	America Ferrera	Kinofilm „Barbie"

Die Suche nach diesen Prominenten führt am häufigsten zu Schadprogrammen und gefährlichen Webseiten.

Ihr Schutz: So suchen Sie gefahrlos

Seien Sie bei der Suche nach Prominenten also vorsichtig beim Klicken, insbesondere auf Links angeblicher Audio- und Videodateien. Laden Sie solche Inhalte nur von offiziellen Musik- und Video-Streaming-Plattformen herunter.

Bei anderen Anbietern kann Ihr PC mit Adware (Werbeprogrammen) oder Schadprogrammen infiziert werden oder Ihnen werden betrügerische Anzeigen eingeblendet.

Meine Empfehlung: Seien Sie bei jeglicher Promi-Suche auf der Hut und nicht nur bei den 10 obigen Namen. Die Tabelle gibt zudem die Situation in den USA wieder und muss nicht mit der Situation in Europa übereinstimmen.

Lassen Sie sich nicht auf gefährliche Webseiten leiten

Prüfen Sie E-Mails mit QR-Code kritisch

„Was ist denn das?", fragte mich Leser Bernd M. während einer Fernwartung im Rahmen unseres PC-Notruf-Dienstes. Er hatte eine E-Mail mit einem QR-Code erhalten. „Ein Betrugsversuch", antwortete ich. Beachten Sie beim Verwalten Ihres elektronischen Postfachs die folgenden Tipps, damit Sie nicht in die QR-Code-Falle tappen.

QR-Codes (**Q**uick **R**esponse, schnelle Antwort) wurden ursprünglich für die Automobilindustrie entwickelt, um Baugruppen und Komponenten zu kennzeichnen. Es handelt sich um quadratische Grafiken aus schwarzen und weißen Quadraten oder Punkten.

Mit QR-Codes lassen sich aber auch Internet-Adressen verschlüsseln. Durch das Einscannen eines QR-Codes sparen Sie das Eingeben einer Internet-Adresse. Doch das ist riskant. Sie sehen einem QR-Code nicht an, wohin er führt!

Die Gefahr: Den Umstand, dass die Zieladresse nicht sichtbar ist, nutzen Kriminelle aus: Sie erstellen QR-Codes, die zu Betrugsseiten führen. Dort werden Sie nach sensiblen Daten gefragt, es werden Ihnen Schadprogramme angeboten oder solche auch automatisch auf Ihr Gerät geladen.

Der Betrug mit QR-Codes lauert überall

In Amerika begegnen Sie betrügerischen QR-Codes quasi auf Schritt und Tritt: Kriminelle kleben sie auf Automaten, Parkuhren, Plakate, Masten und viele andere öffentlich zugängliche Stellen, an denen viele Menschen vorbeikommen.

In Deutschland werden Sie beim Spaziergang selten auf betrügerische QR-Codes stoßen, aber sie können in Ihrem E-Mail-Postfach auf Sie lauern. Denn Betrugs-Mails mit QR-Codes sind auf dem Vormarsch, auch wenn diese am PC kaum nutzbar sind.

QR-Codes vorwiegend für Smartphones gefährlich

Zum Scannen eines QR-Codes benötigen Sie eine gute Kamera und geeignete Programme. QR-Codes werden daher überwiegend mit Smartphones und teilweise auch mit Tablets über die Kamera-App gescannt.

Erhalten Sie einen QR-Code per E-Mail, macht das am PC wenig Sinn und ist ein Alarmzeichen. Denn bislang werden QR-Codes fast nur in Betrugs-Mails verwendet.

Meine Empfehlung: Scannen Sie unterwegs keine QR-Codes auf Aufklebern. Löschen Sie alle E-Mails mit QR-Code sofort. Scannen Sie den QR-Code aus einer E-Mail nicht ein, klicken Sie auf keine Links und öffnen Sie keinen Anhang.

Computerwissen Live-Sendungen

Seien Sie auch bei der nächsten, interessanten Online-Live-Sendung von Computerwissen mit dabei!

In unserer **„Video-Sprechstunde“** beantwortet Tobias Tesch live die Fragen unserer Leser – Hier klicken und zur „Video-Sprechstunde“ anmelden.

In **„Wissen macht Klick!“** stelle ich, Kaner Etem, Ihnen brandaktuelle Computer- und Technikthemen vor – Hier klicken und gleich zur nächsten Sendung „Wissen macht Klick!“ anmelden.

PS: Jeder Teilnehmer erhält am Ende der Live-Sendung immer ein **Dankeschön-Sofort-Download** im Ratgeber-Format. Dies kann eine Zusammenfassung der Inhalte der Sendung ein, oder Inhalte, die die Informationen der Sendung sinnvoll ergänzen. Hier gleich anmelden und Dankeschön sichern.

Impressum: Computerwissen, ein Unternehmensbereich der VNR Verlag für die deutsche Wirtschaft AG, Theodor-Heuss-Straße 2-4, 53177 Bonn, Vorstand: Richard Rentrop, Bonn, redaktionell Verantwortliche: Patricia Sparacio, VNR Verlag für die Deutsche Wirtschaft AG, Adresse s.o.