Liebe Kursteilnehmerinnen und -teilnehmer,

die Sicherheit Ihrer Geräte und Ihrer persönlichen Daten liegt uns bei Levato ganz besonders am Herzen. Deshalb möchten wir Ihnen an diesem letzten Bonus-Tag zusätzlich zu unseren bisherigen Lerneinheiten, die sich vor allem auf die tägliche Bedienung konzentrierten, noch einige wichtige Sicherheitshinweise mitgeben, die Sie vor aktuellen Betrugsversuchen, Gaunern und digitalen Fallen schützen. In dieser PDF, die Sie ausdrucken können und dürfen, haben wir die typischen (und leider sehr erfolgreichen) Methoden der Betrüger zusammengestellt, die gerade am Smartphone immer wieder auftreten und bei denen ein wenig Wissen schon den entscheidenden Unterschied macht.

Solche Sicherheitsthemen greifen wir übrigens auch regelmäßig in unserer Levato-Mitgliedschaft auf, damit unsere Mitglieder über neue Entwicklungen und Betrugsversuche informiert bleiben. Wir wünschen Ihnen eine hilfreiche Lektüre – und vor allem weiterhin einen sicheren und entspannten Umgang mit Smartphone und Internet.

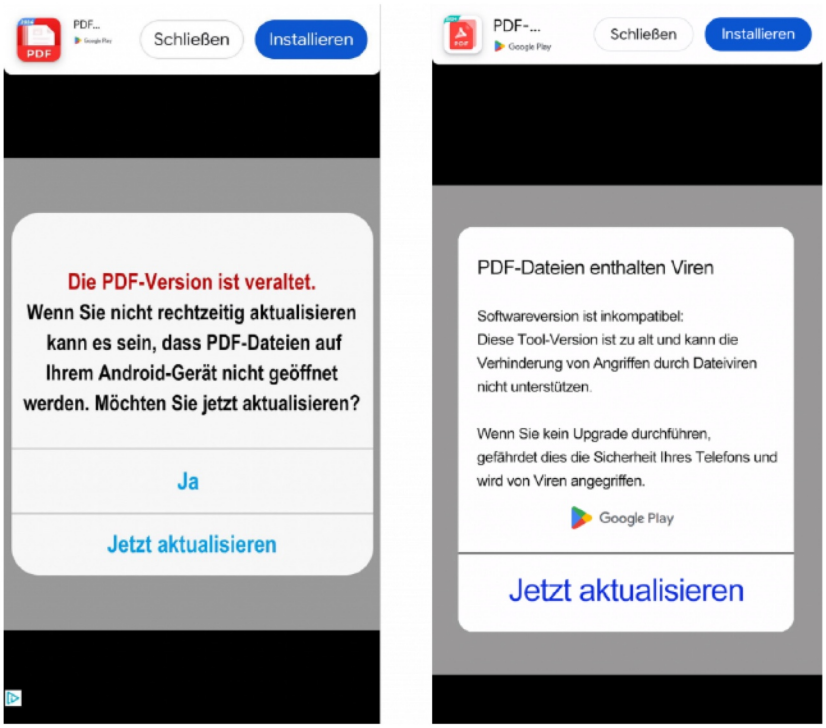
Andreas Dautermann und Kristoffer Braun

www.levato.de

Inhaltsverzeichnis

1. Der Trick mit den Browser-Benachrichtigungen

Browser-Benachrichtigungen wurden für sinnvolle Hinweise entwickelt. Heute werden sie jedoch häufig missbraucht, um Werbung, erfundene Virenwarnungen und andere Betrugsversuche direkt auf Computer und Smartphones zu schicken.



Beispiel für erfundene Meldungen, die wie echte Systemhinweise wirken.

Wie funktionieren diese Benachrichtigungen?

Internetseiten fragen beim Besuch häufig, ob sie Benachrichtigungen senden dürfen. Wer zustimmt, erlaubt der Seite dauerhaft Meldungen an den Browser zu schicken - auch dann, wenn die betreffende Internetseite längst geschlossen ist.

Weil die Meldungen über das Benachrichtigungssystem von Windows, macOS oder Android erscheinen, wirken sie oft wie echte Hinweise des Geräts. Genau das macht die Masche so gefährlich.

Wie sieht der Missbrauch aus?

Die häufigsten Beispiele sind gefälschte Warnungen vor Viren, einem gehackten Konto oder angeblichen Sicherheitsproblemen. Ein Klick führt dann häufig zu einer unseriösen Support-Seite, einem kostenpflichtigen Programm oder einer schädlichen App.

Solche Warnmeldungen sind keine Diagnose des Computers. Nicht auf „Scannen“, „Bereinigen“, „Aktualisieren“ oder ähnliche Schaltflächen klicken.

So schützen Sie sich

Lehnen Sie Benachrichtigungsanfragen unbekannter Internetseiten grundsätzlich ab. In den Einstellungen des Browsers können bereits erteilte Berechtigungen wieder entfernt werden.

- Edge: Drei Punkte > Einstellungen > Cookies und Websiteberechtigungen > Benachrichtigungen. Unbekannte Einträge entfernen.
- Chrome: Drei Punkte > Einstellungen > Datenschutz und Sicherheit > Website-Einstellungen > Benachrichtigungen. Einträge entfernen und auf Wunsch Benachrichtigungen generell blockieren.
- Firefox: Drei Striche > Einstellungen > Datenschutz und Sicherheit beziehungsweise Berechtigungen und Daten > Benachrichtigungen. Unbekannte Seiten entfernen und neue Anfragen blockieren.

Auch am Smartphone

Auf Smartphones ist die gleiche Masche besonders verbreitet. Die Meldungen wirken dort häufig wie Hinweise des Handys. Prüfen Sie deshalb in den Einstellungen der Browser-Apps, welche Internetseiten Benachrichtigungen senden dürfen, und entfernen Sie unbekannte Einträge.

2. Der Betrug mit der Hitze

Bei großer Hitze suchen viele Menschen nach einer schnellen und günstigen Möglichkeit, ihre Wohnung abzukühlen. Unseriöse Händler nutzen diese Situation und bewerben kleine Verdunstungskühler als angebliche vollwertige Klimaanlagen.

Kleine Geräte - große Versprechen

Viele Produkte werden mit Aussagen wie „eiskalte Luft in wenigen Sekunden“, „kühlt den ganzen Raum“ oder „ersetzt jede Klimaanlage“ beworben. Tatsächlich handelt es sich oft nur um einen kleinen Ventilator mit Wassertank. Direkt vor dem Gerät kann sich die Luft angenehmer anfühlen; einen ganzen Raum kann ein solches Gerät aber nicht wie eine Klimaanlage herunterkühlen.

Warnzeichen auf der Verkaufsseite

- Riesige Rabatte von 70 oder 80 Prozent
- ständig ablaufende Countdown-Uhren
- Hinweise wie „nur noch wenige Stück verfügbar“
- fehlende technische Daten oder unklare Herstellerangaben
- keine nachvollziehbare Unternehmensadresse

Physik lässt sich nicht überlisten

Eine echte Klimaanlage arbeitet mit einem Kompressor oder einer Wärmepumpe und muss die entstehende Wärme nach draußen ableiten - über einen Abluftschlauch oder fest verlegte Leitungen. Fehlt diese Ableitung, kann das Gerät einen Raum nicht stark abkühlen.

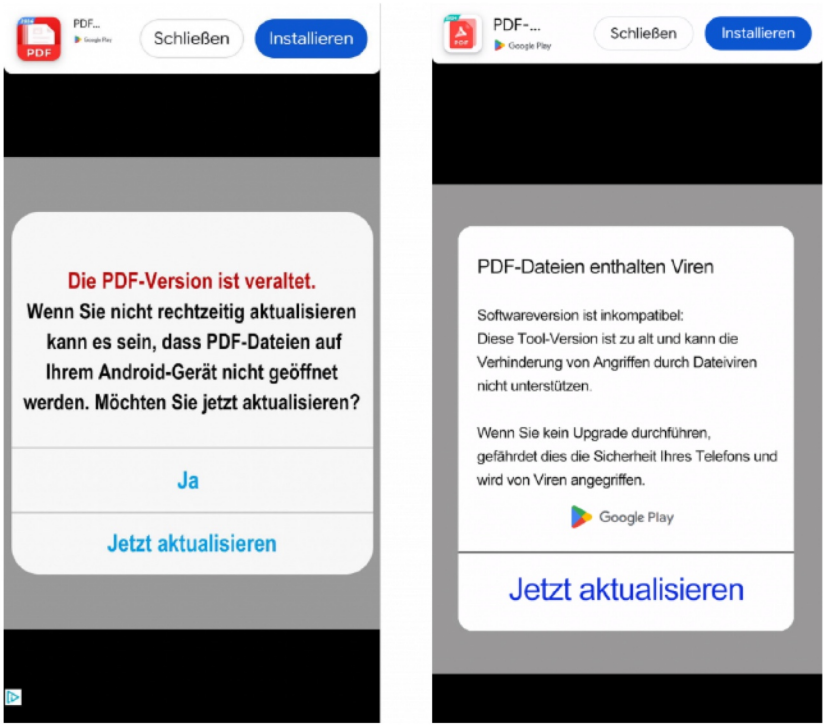
Behauptet ein Anbieter, ein kleines Gerät könne ohne Abluftschlauch einen ganzen Raum deutlich herunterkühlen, ist dieses Versprechen technisch nicht glaubwürdig.

Fazit

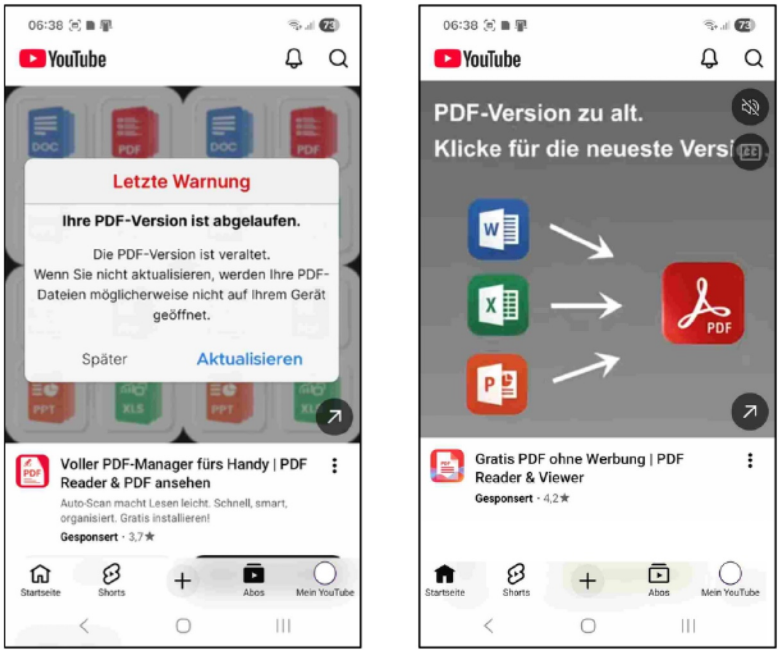
Einfache Verdunstungskühler sind außerhalb von Hitzewellen oft für etwa 30 bis 50 Euro erhältlich. Preise von 100 Euro oder mehr sind bei solchen Geräten häufig deutlich überhöht. Eine echte mobile Klimaanlage kostet mehr, verbraucht mehr Strom und benötigt einen Abluftschlauch.

3. PDF-Betrug weitet sich aus

Auf Smartphones erscheinen immer wieder Werbeanzeigen, die wie echte Systemmeldungen aussehen. In der aktuellen Variante wird behauptet, eine PDF-App sei veraltet oder PDF-Dateien enthielten Viren.



Gefälschte PDF-Warnungen: Hier wird keine bestehende App aktualisiert.



Auch gewöhnliche Werbeanzeigen in YouTube können wie Systemmeldungen aussehen.

Bisherige Varianten

In einer Meldung wird behauptet, die PDF-Version sei veraltet und müsse sofort aktualisiert werden. Eine andere warnt, PDF-Dateien enthielten Viren. Häufig fehlt eine klare Möglichkeit zum Abbrechen.

Dabei wird keine vorhandene App aktualisiert. Stattdessen soll eine ganz neue App installiert werden. Die angebliche Warnung ist lediglich eine besonders aggressiv gestaltete Werbeanzeige.

Auch Werbung in YouTube kann so aussehen

Solche Anzeigen können sogar innerhalb seriöser Apps wie YouTube auftauchen. Die App selbst ist dann nicht zwingend unsicher; die eingeblendete Werbung wurde nur so gestaltet, dass sie wie eine Meldung des Smartphones wirkt.

Was ist zu tun?

- Nicht auf „Installieren“ oder „Aktualisieren“ tippen.
- Die verwendete App schließen oder mit der Zurück-Taste die Anzeige verlassen.
- Nach einem kleinen X oder dem Wort „Schließen“ suchen; es erscheint manchmal erst nach einigen Sekunden.
- Falls nötig, das Smartphone vollständig ausschalten und neu starten.
- Kürzlich installierte, unbekannte Apps prüfen und verdächtige Anwendungen deinstallieren.
- Apps nur selbstständig im offiziellen App-Store suchen und installieren - niemals über eine eingeblendete Werbung.

Was kann nach einer Installation passieren?

- Die App zeigt sehr viel Werbung.
- Sie fordert unnötige Berechtigungen für Kontakte, Nachrichten, Standort oder Kamera.
- Sie kann persönliche Daten ausspähen oder Schadsoftware enthalten.
- Sie kann unerwartete Kosten verursachen.

Bei Android vor der Installation Bewertungen, Anbieter und angeforderte Berechtigungen prüfen. Unbekannte Apps mit wenigen oder schlechten Bewertungen besser nicht installieren.

4. Erfundene Virenmeldung: „Bedrohung erkannt!“

Eine besonders hartnäckige Meldung füllt den gesamten Bildschirm und behauptet, ein Trojaner sei gefunden worden. Sie ähnelt einer echten Windows-Sicherheitswarnung und lässt sich teilweise nicht auf dem üblichen Weg schließen.

Meldung lässt sich nicht schließen

Die Warnung kann von einer problematischen Browser-Erweiterung ausgelöst werden. Nach einem Neustart taucht sie häufig erneut auf. Das Ziel ist, ein kostenpflichtiges oder unerwünschtes Programm zu installieren.

Die Meldung ist frei erfunden. Keine angebotene Software installieren und keine Zahlungsdaten eingeben.

Hilfreiche Tastenkombinationen

Alt + F4 schließt das aktuelle Fenster.

Windows-Taste + D zeigt den Desktop an.

Strg + Alt + Entf öffnet einen Sicherheitsbildschirm, über den der Task-Manager gestartet werden kann.

Browser-Erweiterungen kontrollieren

Browser-Erweiterungen sind kleine Zusatzprogramme. Prüfen Sie nach einer solchen Meldung, welche Erweiterungen installiert sind. Bei Chrome und Edge öffnen Sie über die drei Punkte den Bereich „Erweiterungen“ und danach „Erweiterungen verwalten“. Bei Firefox finden Sie den Bereich über die drei Striche unter „Erweiterungen und Themes“.

Entfernen Sie Erweiterungen, die Sie nicht kennen oder nicht bewusst installiert haben. Verdächtig sind häufig allgemeine Namen wie „Video Downloader“, „PDF Converter“ oder „Search Tool“.

Zusätzliche Bereinigung

Wenn weiterhin ungewöhnliche Werbung oder Warnmeldungen erscheinen, kann ein zusätzliches Prüfprogramm wie Malwarebytes helfen, unerwünschte Programme und Werbesoftware zu finden. Die kostenfreie Version wird bei Bedarf manuell gestartet und ersetzt keinen dauerhaft aktiven Virenschutz.

5. Neue Betrugsmasche auf Verkaufsplattformen

Kriminelle versuchen bei Kleinanzeigen, Online-Marktplätzen und Buchungsportalen, Nutzer aus der geschützten Umgebung der Plattform herauszulocken.

Das erste Ziel der Kriminellen

Solange Kommunikation und Zahlung innerhalb der ursprünglichen Plattform stattfinden, greifen deren Schutzmechanismen. Wird der Kontakt plötzlich per E-Mail, SMS oder WhatsApp fortgesetzt, steigt das Risiko deutlich.

Typischer Ablauf

Kurz nach einer Anzeige, einem Kauf oder einer Buchung meldet sich eine freundlich wirkende Person. Sie schlägt vor, „der Einfachheit halber“ außerhalb der Plattform weiterzuschreiben oder sendet eine angebliche Zahlungsbestätigung über einen externen Link. Diese Bestätigung kann vollständig erfunden sein.

Der wichtigste Tipp

Bleiben Sie innerhalb der Plattform und verwenden Sie deren Nachrichten- und Bezahlsysteme. Bei PayPal sollte für Waren die Funktion „Waren und Dienstleistungen“ genutzt werden. Vorkasse und Kreditkartenzahlungen außerhalb der Plattform sind deutlich riskanter.

- Aufforderung, einen externen Link anzuklicken
- Bitte um persönliche Daten oder Kontoinformationen
- ungewöhnlich günstiger Preis
- Druck, sehr schnell zu handeln

Bildschirmfoto als Beweis

Fertigen Sie bei verdächtigen Nachrichten sofort ein Bildschirmfoto an. Es dokumentiert die Situation und erleichtert später die Beratung oder eine Anzeige. Der Filmhinweis zur Erstellung von Bildschirmfotos wurde in dieser schriftlichen Fassung entfernt; die Empfehlung selbst bleibt wichtig.

6. Betrug mit angeblichen Cloud-Mails

Betrügerische E-Mails behaupten, der Cloud-Speicher sei voll, eine Zahlung sei fehlgeschlagen oder sämtliche Daten würden gelöscht, wenn man nicht sofort handelt.

In den meisten Fällen ist es Phishing

Die Nachrichten werden massenhaft versendet und sollen Angst auslösen. Typisch sind dramatische Formulierungen, sehr kurze Fristen, auffällige Schaltflächen wie „Jetzt handeln“ und eine unpersönliche Anrede. Ziel ist meist, Passwörter oder Zahlungsdaten abzugreifen.

Wie erkennt man echte Nachrichten?

Echte Anbieter informieren in der Regel ruhig und sachlich. Ein Cloud-Speicher kann tatsächlich voll sein, und eine hinterlegte Kreditkarte kann ablaufen. Seriöse Anbieter verlangen aber nicht, Passwörter oder Zahlungsdaten unmittelbar über einen Link in einer E-Mail einzugeben.

Eine echte Nachricht enthält häufig eine persönliche Anrede und verweist darauf, die Angaben direkt im eigenen Kundenkonto zu prüfen.

Warum die Masche funktioniert

Die E-Mails nennen oft gar keinen konkreten Anbieter. Dadurch fühlen sich Nutzer von Apple, Microsoft, Google oder anderen Diensten gleichermaßen angesprochen.

Der wichtigste Rat

Klicken Sie nicht auf den Link in der E-Mail. Öffnen Sie stattdessen die bekannte App des Cloud-Dienstes oder geben Sie die offizielle Internetadresse selbst in den Browser ein. Im Kundenkonto lässt sich zuverlässig prüfen, ob der Speicher tatsächlich voll ist oder Zahlungsdaten aktualisiert werden müssen.

Angstmachende E-Mails mit Zeitdruck und Löschdrohungen sind fast immer ein starkes Betrugszeichen.