

# Inhalt

1. WhatsApp-Aus! Messenger beendet Support für alte iPhones und Android-Handys
2. Betrügerische Phishing-Mails Von Sparkassen, Volksbanken oder Mastercard: Diese Mails sollten Sie sofort löschen
3. Vorsicht vor "Abzock"-SMS im Namen von DHL: Diese Nachricht lockt Sie in teure Abofalle
4. Microsoft stellt ab 14. Januar 2020 die kostenlosen Updates für Windows 7 ein

Quellen: [FOCUS.de](https://www.focus.de), [verbraucherzentrale.de](https://www.verbraucherzentrale.de)

**1.**

## **WhatsApp-Aus! Messenger beendet Support für alte iPhones und Android-Handys**



dpa/Martin Gerten

**Donnerstag, 16.01.2020**

**WhatsApp zieht auf mehreren alten Smartphones den Stecker - und zwar schon Ende Januar. Auf vielen alten iPhones und Android-Smartphones endet mit dem Monatswechsel der Support und WhatsApp wird nicht mehr wie gewohnt funktionieren. Was Nutzer jetzt wissen müssen.**

**Millionen Deutsche nutzen WhatsApp täglich, um mit Freunden und Bekannten zu chatten. Der zu Facebook gehörende Messenger ist seit Jahren der meistgenutzte Chat-Dienst in Deutschland.**

**Doch einige Nutzer müssen sich ab Anfang Februar von WhatsApp verabschieden. Ab 1. Februar 2020 kann der Messenger auf einigen Smartphones mit veralteten Android- und iOS-Betriebssystemen nicht mehr**

installiert bzw. ohne Einschränkungen genutzt werden. Der Grund: WhatsApp beendet den Support.

## WhatsApp beendet Support für iPhones und Android-Handys

Schon vor Monaten hatte der Dienst das Support-Aus für iOS 8 ab 1. Februar 2020 angekündigt. iOS 8 ist im Herbst 2014 erschienen und spielt bei Apple-Geräten heute praktisch keine Rolle mehr, da iPhones wesentlich schneller aktualisiert werden als Android-Smartphones. Aktuell ist bereits seit Herbst 2019 iOS 13 für iPhones verfügbar.

Und auch für Android Gingerbread (Android 2.3.7 und älter) – so der Name der Version – wird WhatsApp ab 1. Februar 2020 nicht mehr unterstützt. Allerdings dürften auch die Nutzerzahlen der Android-Variante eher überschaubar sein: Besagte Android-Version erschien im Dezember 2010, wird zum Support-Aus also über 9 Jahre alt sein.

Das Support-Aus trifft:

- Android-Version 2.3.7 und älter nach dem 1. Februar 2020
- iPhone iOS 8 und älter nach dem 1. Februar 2020
- zudem alle Windows-Phone-Betriebssysteme nach dem 31. Dezember 2019

*Auch interessant: [Gefährliche Android-Apps: 3 Anwendungen sollten Nutzer jetzt schnell löschen](#)*

Wer WhatsApp auf einem der oben genannten Betriebssysteme weiter nutzen will, kann ab Februar 2020 kein neues Konto mehr erstellen; auch das erneute Verifizieren eines bestehenden WhatsApp-Accounts wird dann nicht mehr möglich sein.

Da die App-Betreiber für diese Betriebssysteme nicht mehr aktiv entwickeln, können außerdem einige Funktionen möglicherweise nicht mehr genutzt werden. WhatsApp selbst kann zwar weiterhin genutzt werden; dennoch sollten sich betroffene User perspektivisch nach einem neuen Handy mit aktuellem Betriebssystem umsehen - auch aus Sicherheitsgründen.

Gar nicht mehr unterstützt wird WhatsApp seit kurzem auch [auf Windows](#) Phones: Stichtag für alle Windows Phones war der 31. Dezember 2019. Seitdem ist der Messenger auf Windows Phones nicht mehr nutzbar.

## Support-Aus: Was betroffene WhatsApp-User wissen sollten

**WhatsApp stellt die Unterstützung für alte Versionen von Android und iOS ein. Nutzer, die betroffene Geräte mit veralteten Versionen nutzen, sollten - sofern möglich - eine aktuelle Betriebssystem-Version installieren oder sich nach einem neueren Smartphone umsehen.**

**Grund dafür ist nicht nur das WhatsApp-Aus – auch sonst stellen die veralteten Betriebssysteme ein Sicherheitsrisiko dar, da sie über viele bekannte Schwachstellen angegriffen werden können.**

Quelle: [FOCUS.de](https://www.focus.de)

## 2.

### **Betrügerische Phishing-Mails Von Sparkassen, Volksbanken oder Mastercard: Diese Mails sollten Sie sofort löschen**



dpa/Daniel Karmann

**Donnerstag, 16.01.2020**

Sie haben eine E-Mail erhalten, die auf den ersten Blick von Ihrer Sparkasse, der Volksbank oder Mastercard stammt? Dann ist Vorsicht geboten, in Wirklichkeit könnten Kriminelle hinter den E-Mails stecken. Die Verbraucherzentrale Nordrhein-Westfalen warnt Bankkunden derzeit vor einer Betrugswelle. Wie Sie nicht auf die Masche hereinfallen.

- Derzeit kursieren wieder vermehrt Phishing-Mails, die Daten von Kunden abgreifen wollen.
- Der vermeintliche Sender der Mails sind Sparkassen, Volksbanken und Mastercard, doch in Wirklichkeit handelt es sich um unbekannte Kriminelle.
- Die Verbraucherzentralen erklären, wie sie reagieren sollten, wenn sie eine Phishing-Mail erhalten.

Die Verbraucherzentrale Nordrhein-Westfalen warnt Bankkunden auf ihrer Webseite vor vermeintlichen E-Mails der Sparkassen, Volksbanken und von Mastercard. Wie die Verbraucherschützer schreiben, versenden Unbekannte derzeit in allen Fällen Phishing-Mails an Verbraucher und versuchen, Kunden unter einem falschen Vorwand auf eine gefälschte Website zu locken. Dort fragen sie Nutzerdaten ab. Doch Vorsicht: Wer dieser Aufforderung nachkommt, übergibt die Daten an Kriminelle.

## **Sparkasse, Volksbank, Mastercard: So sehen die Phishing-Mails aus**

Sparkasse: Kunden der Sparkassen erhalten beispielsweise Nachrichten mit dem Betreff "Überprüfung Ihrer Daten". Darin informieren die Betrüger über "neue Bestimmungen für den Online-Zahlungsverkehr". Im Rahmen dieser "neuen Bestimmungen" sei ab sofort jeder Kunde der Sparkasse dazu verpflichtet, regelmäßige Datenabgleiche durchzuführen, fassen die Verbraucherschützer den Inhalt der Mail zusammen. Komme man der Aufforderung nicht nach, so bleibe das Konto angeblich vorerst gesperrt.

Mastercard: Kunden von Mastercard erhalten derzeit Mails mit ähnlichem Inhalt, auch die Betreffzeile "Überprüfung Ihrer Daten" ist identisch. Wie die Verbraucherzentrale NRW schreibt, fordert der unbekannte Mail-Versender Kunden auf, "die Daten Ihres Kundenstammes zu überprüfen" – dazu seien sie verpflichtet. Der E-Mail-Empfänger habe diese Überprüfung aber noch nicht durchgeführt, weswegen nun seine Karte gesperrt sei. Kunden, die der Überprüfung innerhalb von zwei Tagen nicht nachkommen, könnten ferner ihre Karte nur gegen eine Bearbeitungsgebühr von 29,95 Euro entsperren.

Die Verbraucherzentralen betonen vor diesem Hintergrund: Insbesondere, "wenn Sie via E-Mail aufgefordert werden, ganz dringend und innerhalb einer bestimmten (kurzen) Frist zu handeln, sollten Sie ebenfalls stutzig werden. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist - beispielsweise, dass sonst Ihre Kreditkarte oder Ihr Online-Zugang gesperrt werden."

*Mehr zum Thema: [Kontodaten und Passwörter im Visier - Phishing-Falle: So schützen Sie sich vor Internet-Betrügern](#)*

Volksbanken: Auch Kunden der Volksbank sind Ziel von Betrügern. Der aktuellste Phishing-Versuch wurde sowohl unter dem Betreff "Authentifizierung erforderlich" als auch "Authentifizierung notwendig" verschickt, warnt die Verbraucherzentrale. Im Zuge der neuen Zahlungsdienstrichtlinie PSD2 sei es notwendig, das Geburtsdatum und die Mobilfunknummer über den beigefügten Link anzugeben. Damit wolle die Bank angeblich "die Sicherheit im Zahlungsverkehr" erhöhen.

## Sie haben eine Phishing-Mail erhalten? Das sollten Sie jetzt tun

Die Verbraucherschützer aus NRW betonen, dass die Inhalte dieser E-Mails frei erfunden sind und es sich um Phishing-Versuche handelt. Sieht eine E-Mail nach einem Betrugsversuch aus, sollten Verbraucher weder auf Links klicken noch Dateianhänge öffnen oder auf die E-Mail antworten. Betroffene sollten die Mail am besten in den Spam-Ordner verschieben oder gleich löschen, raten die Verbraucherschützer weiter.

Wer auf Nummer sicher gehen möchte, kann die verdächtige E-Mail auch direkt an die Verbraucherzentrale in Nordrhein-Westfalen weiterleiten. Die Verbraucherschützer sind unter [phishing@verbraucherzentrale.nrw](mailto:phishing@verbraucherzentrale.nrw) zu erreichen.

Quelle: [FOCUS.de](https://www.focus.de)

- Signale, woran Sie eine [Phishing-Mail erkennen](#),
- Hinweise, wie Sie den [E-Mail-Header](#) lesen
- Informationen über andere [Abzocker im Internet](#)

Darüber hinaus finden Sie tägliche Warnungen auch auf Twitter ([@vznrw\\_phishing](#)) und in der [Facebook-Gruppe Phishing-Radar](#).

Quelle: [verbraucherzentrale.de](https://www.verbraucherzentrale.de)

### 3.

## Vorsicht vor "Abzock"-SMS im Namen von DHL: Diese Nachricht lockt Sie in teure Abofalle



picture-alliancet/dpa/D. Bockwoldt

Mittwoch, 15.01.2020

Phishing-Attacken kommen nicht nur per Mail, sondern über jegliche digitale Kommunikationskanäle – darunter auch SMS. Derzeit verschicken Unbekannte angeblich im Namen von DHL Textnachrichten mit der Ankündigung, dass ein Paket im Verteilerzentrum liegt.

Für zwei Euro könne das Paket seinen Weg fortsetzen, schreiben die Betrüger darin. Über einen Link sollen die Empfänger der SMS dann ihre Daten eingeben und die zwei Euro bezahlen. Doch wer dieser Aufforderung nachkommt, landet direkt in einer Abofalle.

Über die Betrugsmasche berichtet "[Onlinewarnungen.de](http://www.onlinewarnungen.de)" in seinem Warnungsticker. Auch ein Leser kommentierte den Beitrag unterdessen und berichtet von seiner Erfahrung. So habe er eine Phishing-SMS von DHL mit folgendem Inhalt bekommen: „AT-HKM32013: Unzustellbares Paket! Status: Ihre Sendung ist im Verteilerzentrum angehalten worden. verfolgen Sie Ihre Sendung: : <http://8xad.vip/Y...>“

### **DHL: „Fragliche Meldungen nicht von uns“**

Auch die Bonner Polizei warnt inzwischen ausdrücklich vor der Betrugsmasche. „In den letzten Tagen wurden gleich mehrere Fälle dieser Masche bei der Bonner Polizei



zur Anzeige gebracht“, erklärt Polizeisprecher Michael Beyer. Die Betrugsmasche liefe derzeit bundesweit, die Täter hätten ihre Fake-SMS gleich massenweise verschickt.

Achim Gahr von der Pressestelle der "Deutsche Post DHL Group" stellt klar: „Die fraglichen Meldungen werden nicht von DHL verschickt. Wir versenden weder Paket-Statusmeldungen per SMS, noch fordern wir unsere Kunden in der Online-Sendungsverfolgung dazu auf, Geld nachzuzahlen.“ Man rate den Kunden daher, Links in solch dubiosen Mitteilungen nicht anzuklicken.

## **SMS-Phishing: Abzock-Methode ist nicht neu**

Wie der Online-Dienst von "onlinewarnungen.de" zudem schreibt, kommt die Masche mit den angekündigten Sendungen auch im Namen von anderen Logistikunternehmen vor. Die Betrüger würden jedoch vor allem auf E-Mails setzen.

Besonders gerne haben Kriminelle in jüngster Vergangenheit mit einer Sendung, die ein Samsung Galaxy S9 ankündigt, gelockt. Per Link soll die Lieferung bestätigt werden. Absender waren in diesem Fall angeblich etwa DHL, TNT und DB Schenker.

"Onlinewarnungen.de" hat unterdessen eine Liste mit dubiösen Absendern erstellt. Bei folgenden Nummern sollten Sie auf der Hut sein:

- TrackInfo
- Info13Text
- Info21Text
- Info42Text
- Info 65Text
- Info75Text
- +447851536620
- +43872254636
- +263711105879
- +50494052848
- .....

Die vollständige Liste finden Sie [hier](#).

## 4.

### Microsoft stellt ab 14. Januar 2020 die kostenlosen Updates für Windows 7 ein

Dienstag, 07.01.2020

Microsoft stellt ab 14. Januar 2020 die kostenlosen Updates für Windows 7 ein. Das Betriebssystem ist immer noch weit verbreitet, wird aber zum Sicherheitsrisiko. Was Sie nun tun sollten.

Das Wichtigste in Kürze:

- Neue Sicherheitslücken in Windows 7 werden nicht mehr kostenlos geschlossen.
- Das bedeutet: Upgrade oder neuer PC – das sind aber nicht die einzigen Möglichkeiten, die Sie nun haben.
- Beim aktuellen Betriebssystem Windows 10 raten wir zu den richtigen Datenschutz-Einstellungen.



Foto:

Verbraucherzentrale

Nach rund 10 Jahren stellt Microsoft den Support für sein Betriebssystem Windows 7 ein. Weltweit liegt der Marktanteil wohl noch bei rund 25 Prozent. Für alle, die Windows 7 nutzen, steigt ab dem 14. Januar 2020 aber das Risiko: Werden neue Sicherheitslücken entdeckt, kann es sein, dass Microsoft sie nicht mehr per kostenlosem Update schließt.

Das bedeutet unter anderem: Vom zukünftigen Homebanking mit Windows 7 ist dringend abzuraten, da im Schadenfall die Bank eine Haftung ablehnen könnte.

Wer Windows 7 auf einem PC installiert hat, sollte sich darum kümmern. Einige Möglichkeiten:

1. Trennen Sie den PC dauerhaft vom Internetanschluss. Bei Sicherheitslücken in Windows 7 wäre das sonst ein großes Risiko. Seien Sie ebenso vorsichtig, wenn Sie etwa per USB-Stick, externer Festplatte, Handy, DVD oder einer anderen externen Quelle Daten übertragen. Auch dabei besteht ein steigendes Risiko, dass Schadsoftware Sicherheitslücken ausnutzt.
2. Für einige Versionen von Windows 7 bietet Microsoft einen kostenpflichtigen Update-Service bis 2023 an. Das richtet sich vor allem an Unternehmen, für die ein Umstieg mit vielen Geräten teurer werden kann. Für Privatleute mit einem PC lohnt sich das wohl nicht.
3. Rüsten Sie Ihren PC mit einem aktuellen Betriebssystem aus und achten Sie darauf, dass Ihre Soft- und Hardware damit kompatibel sind. Als kostenloses alternatives Betriebssystem ist zum Beispiel Linux bekannt.
4. Kaufen Sie einen neuen PC und entscheiden Sie sich dabei für ein aktuelles Betriebssystem.

Microsoft empfiehlt offensiv die vierte Möglichkeit – den Kauf eines ganz neuen PCs mit Windows 10. Für Besitzer von Windows 7 gibt es aber immer noch eine weitere Möglichkeit: Der Wechsel aufs aktuelle Betriebssystem kann auch noch über ein kostenloses Upgrade funktionieren. Sie müssen dann nichts neu kaufen. Wie Sie von Windows 7 auf Windows 10 upgraden können, [beschreibt z.B. die Stiftung Warentest](#).

Windows 10 haben wir als datenhungrig kritisiert. Wer es installiert, sollte sich mit den Einstellungen beschäftigen, sodass möglichst wenige Nutzerdaten an Microsoft übertragen werden. Wichtige Einstellungen haben wir [hier für Sie zusammengefasst](#).

Ein weiterer Knackpunkt kann bei älteren Geräten außerdem sein, dass einige Programme und Geräte nicht mit Windows 10 kompatibel sind. Haben Sie solche Anwendungen installiert, kann es sein, dass sie nach dem Upgrade nicht mehr funktionieren. Oder es kommt z.B. kein Ton mehr, weil die Soundkarte des PCs keine Treiber für Windows 10 bekommen hat.

Windows 10 hat etwas höhere Anforderungen an den PC als Windows 7. Das Gerät kann also nach einem Upgrade durchaus langsamer laufen und weniger freien Speicherplatz auf der Festplatte haben.

Wer hier unsicher ist und das Upgrade erst einmal ausprobieren möchte, sollte sich mit den Möglichkeiten der Systemwiederherstellung beschäftigen. Dann könnten Sie Ihr Gerät, sollte Windows 10 nicht wie gewünscht laufen, noch einmal auf Windows 7 zurückstellen.

*Dieser Inhalt wurde von der Gemeinschaftsredaktion in Zusammenarbeit mit den Verbraucherzentralen [Nordrhein-Westfalen](#) und [Bremen](#) für das Netzwerk der Verbraucherzentralen in Deutschland erstellt.*

Quelle: [verbraucherzentrale.de](http://verbraucherzentrale.de)