DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Microsoft-Support-Scam mit neuer Masche

Seit Jahren ziehen Betrüger PC-Nutzern mit dem Microsoft-Support-Scam Geld aus der Tasche. Jetzt sind sie mit einer neuen Masche zurück!
Inhaltsverzeichnis

Internet-Betrüger nutzen zahlreiche Methoden, mit denen sie leichtgläubige Menschen um ihr Geld bringen. Eine der beliebtesten ist die seit Jahren grassierende Microsoft-Masche. Dabei versuchen angebliche Microsoft-Mitarbeiter, ihren Opfern per Telefon überteuerte und völlig überflüssige Hilfsmaßnahmen anzudrehen oder sogar Schadsoftware auf deren PC zu installieren. Aktuell häufen sich die betrügerischen Anrufe in Deutschland wieder. Was dahintersteckt, verrät COMPUTER BILD.

Microsoft-Support-Scam: Neue Masche mit Defender-Meldungen

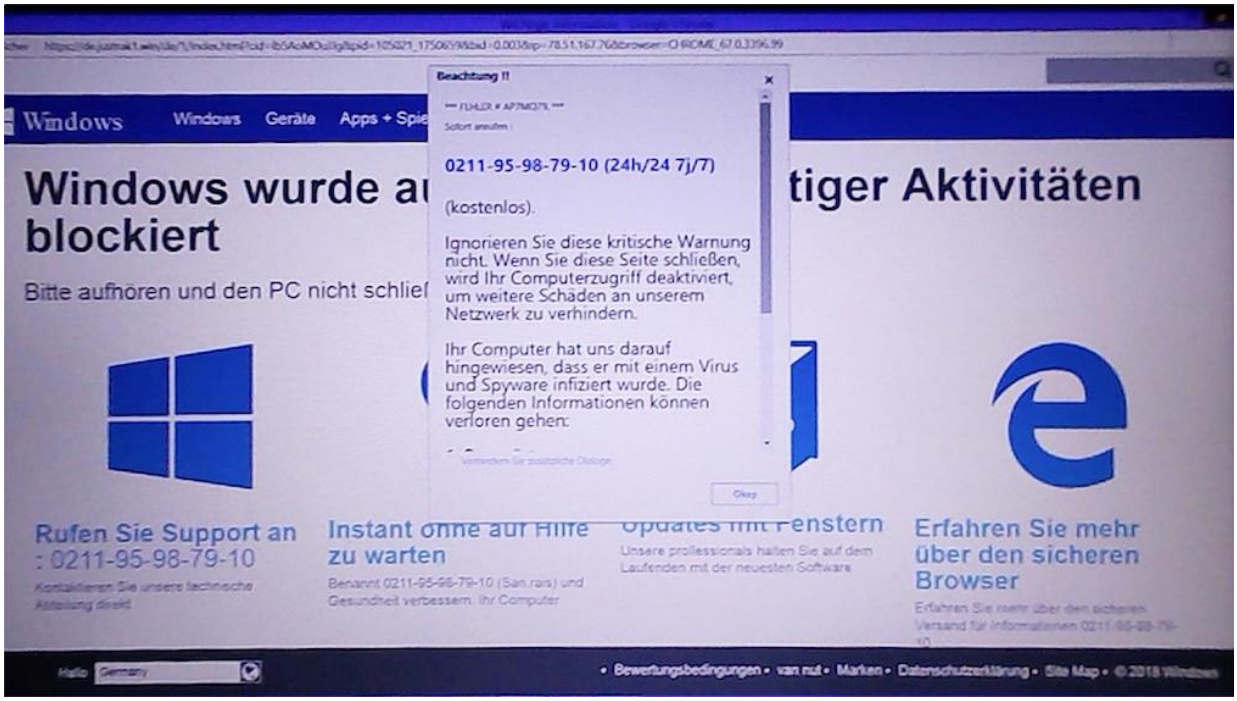
Wie die Seite Watchlist Internet berichtet, gibt es aktuell vermehrt Betrugsversuche mit einer leicht abgewandelten Form des Support-Scams: Die Täter ahmen Microsoft-Defender-Meldungen nach und zeigen diese per Pop-up oder als Werbung auf verschiedenen Internetseiten an. So soll der Eindruck entstehen, dass ein Virus auf dem PC ist. Um den zu entfernen, sollen Nutzerinnen und Nutzer eine Telefonnummer anrufen und landen dann in den klassischen Callcentern, wo die Betrüger versuchen, Geld und Daten zu stehlen. Ignorieren Sie diese Meldungen!

Microsoft-Scam: Klassische Support-Masche

Seit Jahren weist die Verbraucherzentrale auf die fiese Microsoft-Masche hin und erinnert hartnäckig daran, dass die Anrufe oder Support-Nummern nicht von echten Microsoft-Mitarbeitern stammen. Aktuell sind die Betrüger wieder besonders aktiv und zielen auf ahnungslose Menschen in Deutschland. Die Kriminellen verwickeln ihre zumeist älteren Opfer oftmals in lange Telefonate und drängen sie zur Installation einer Fernwartungs-Software – etwa TeamViewer. Damit ist es ihnen dann möglich, sensible Daten wie Passwörter und Kontodaten auszuspähen sowie Schadsoftware zu installieren. Wie Mimikama berichtet, ist erst kürzlich wieder ein älterer Herr auf die Masche hereingefallen und hat 2.000 Euro in Google-Play-Karten bezahlt.

Betrug mit Microsoft-Anrufen: So wehren Sie sich!

Sollten Sie einen derartigen Anruf erhalten, legen Sie am besten sofort auf! In einem Blog-Eintrag stellte Microsoft vor einiger Zeit klar, dass kein Support-Mitarbeiter des Unternehmens jemals ungefragt anrufen oder E-Mails schicken und persönliche Daten abfragen würde. Auch Hinweise auf Internetseiten, dass Ihr PC virenverseucht ist und Sie eine Support-Nummer von Microsoft anrufen sollen, ignorieren Sie am besten. Haben Sie trotzdem bereits auf solch einen Betrugsversuch reagiert, sollten Sie dadurch installierte Software sofort wieder entfernen, alle übermittelten Kennwörter ändern und den PC mit einem Virenschutzprogramm untersuchen. Und: Bringen Sie den Vorfall bei Ihrem örtlichen Polizeirevier zur Anzeige! Weitere Verhaltenstipps nennt die Verbraucherzentrale.



Eine Webseite fordert zum Anruf einer vermeintlichen Microsoft-Support-Rufnummer auf. Dahinter steckt Betrug.

Microsoft-Masche: Ein alter Trick

Die sogenannte Microsoft-Masche ist eigentlich ein alter Hut. Schon seit 2014 sind entsprechende Betrugsfälle vermehrt bei den Verbraucherzentralen aktenkundig. Dabei erhielten PC-Nutzer zunächst vor allem eine Viruswarnung, die dazu auffordert, eine gefälschte Kundendienstnummer des Windows-Herstellers anzurufen, siehe Bild oben. Hatten sie bereits Telefonnummern erbeutet, klingelten die vermeintlichen Microsoft-Mitarbeiter auch gern selbst mal durch und zogen den PC-Nutzern das Geld aus der Tasche. Ein gemeiner Trick, mit dem die Kriminellen einer Studie zufolge Millionen verdienen. Auch Microsoft weiß von der Problematik, erhält eigenen Angaben zufolge monatlich etwa 11.000 Beschwerden wegen derartiger Betrugsversuche. Laut einem Report von Microsoft Security meldeten sich allein 2017 mehr als 153.000 Opfer beim Windows-Hersteller; die Dunkelziffer liegt deutlich höher.

Immer raffiniertere Methoden

Die Kriminellen hinter dem Tech-Support-Scam nutzen immer mehr Tricks, um Opfer in die Falle zu locken. So kommen die gefälschten Meldungen nicht nur als Anzeige oder Pop-up auf

Internetseiten, sondern auch als Mail, Anruf oder SMS, tauchen in den Edge-Favoriten auf oder imitieren sogar bekannte Seiten, um dann auf die Scam-Adressen zu verlinken. Seien Sie daher grundsätzlich auf der Hut und behalten Sie immer im Hinterkopf, dass alle Virenwarnungen, die Sie auffordern, eine Nummer anzurufen, Betrug sind!

Google-Play-Karten kein seriöses Zahlungsmittel!

Wenn Sie etwas im Google Play Store kaufen oder Guthaben verschenken wollen, ist das natürlich in Ordnung. Aber keine seriöse Firma akzeptiert Google-Play-Karten als Zahlungsmittel. Sollte Sie jemand dazu auffordern, damit zu bezahlen, dann ist das sehr sicher Betrug! Tun Sie das nicht und beenden Sie am besten sofort das Gespräch!

Fake-Callcenter: Über 50 Festnahmen in Indien

Microsoft ist nicht untätig. Ende 2018 ließ der Konzern in Zusammenarbeit mit den örtlichen Sicherheitsbehörden 16 Callcenter in der indischen Hauptstadt Neu-Delhi durchsuchen. Dabei kam es zu über 50 Festnahmen. Die festgenommenen Callcenter-Agenten hatten sich zuvor am Telefon als Microsoft-Mitarbeiter ausgegeben und arglose Menschen um ihr Geld betrogen. Microsofts Einsatz war ein erster wichtiger Schritt in der Bekämpfung dieser Abzockmasche, der vorerst aber wohl nur Erleichterung im englischsprachigen Raum bringt. Die meisten Opfer der inhaftierten Betrüger stammen aus den USA und Kanada. Dass die Microsoft-Masche in Deutschland weiter auftritt, zeigen die aktuellen Fälle.

Offizielle Liste von Microsoft-Adressen

Haben Sie eine E-Mail von Microsoft bekommen und sind nicht sicher, ob die echt oder gefälscht ist, gleichen Sie den Absender mit der offiziellen Liste mit Microsoft-Adressen ab. Ist die Absender-Domain dort nicht enthalten, stammt die Mail nicht von Microsoft! Ist sie enthalten, ist das ein gutes Zeichen. Seien Sie aber trotzdem skeptisch und geben Sie keine Daten raus. Gewähren Sie vor allem keinen Fernzugriff. Die Absender-Adresse lässt sich nämlich mit etwas mehr Aufwand auch fälschen.

Weitere Phishing-Maschen

Die Microsoft-Support-Scam-Masche ist bei Weitem nicht die einzige, mit der Betrüger versuchen, an Ihr Geld und Ihre Daten zu kommen. Egal ob falsche Gewinnspiele, Erbschaften, angebliche Probleme in Ihren Konten, falsche Mahnungen oder Pakete, die irgendwo auf Sie warten sollen: Die Betrüger versuchen mit allen Tricks, Ihre Aufmerksamkeit zu bekommen und Sie zu schnellem und unüberlegtem Handeln zu verleiten. Welche anderen Maschen es gibt und wie Sie sich schützen, wehren und am besten reagieren, hat COMPUTER BILD in einem Phishing-Ratgeber zusammengefasst.

Quelle: https://www.computerbild.de/artikel/cb-News-Sicherheit-Microsoft-Support-Scam-16616433.html