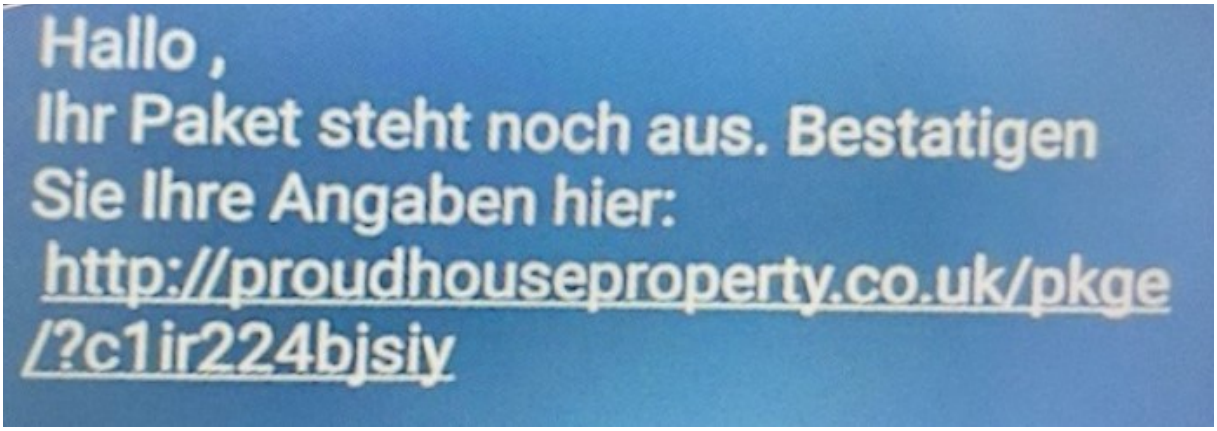
Vorsicht !

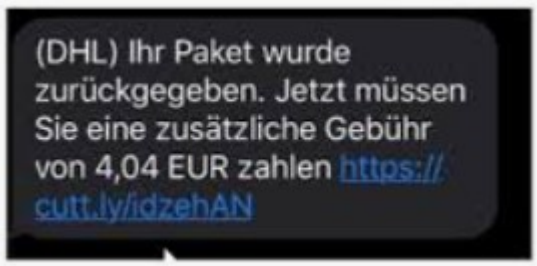
Gefährliche SMS Nachrichten – Empfehlungen für den sicheren mobilen Betrieb

Der sichere Betrieb mit mobilen Endgeräten wird seit längerer Zeit durch eine gefährliche Phishing-Welle bedroht. Dabei kommen die mit einem Link versehenen Lockbotschaften aber nicht per Mail, sondern per SMS und enthaltenen Links.



Wie Betroffene damit umgehen sollten.

Falsche Paket-SMS: Wer aktuell solche oder ähnliche u.a. SMS bekommt, löscht sie besser sofort und klickt keinesfalls auf Links.



"Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es." Diese leicht holprige, mit einem Link versehene SMS kursiert schon seit Jänner dieses Jahres und verbreitet mitunter eine gefährliche Android und iOS Schadsoftware namens FluBot.

Neben Fake-Nachrichten von Fedex erhalten Anwender nun auch ähnliche Benachrichtigungen von DHL und anderen Dienstleistern wie von unterschiedlichen Rufnummern von A1, Drei oder Magenta und enthalten verschiedene Inhalte zur Paketzustellung mit dubiosen Links.

Aktuell ist der Nutzen für Kriminelle deshalb so erfolgreich, weil der Onlinehandel in der Corona-Krise boomt und viele Nutzer tatsächlich eine Lieferung erwarten. Gerade jetzt, mitten im Weihnachtsgeschäft, nimmt die Gefahr noch einmal zu.

Ist der Empfang der SMS gefährlich?

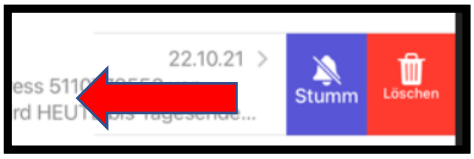
Nein. Wer die Phishing-Nachricht erhalten und ignoriert hat, muss sich keine Sorgen machen, dass sich die Schadsoftware bereits auf dem Handy eingenistet hat.

Der Trojaner wird nicht unmittelbar installiert, sobald man auf den Link klickt. Stattdessen landen Nutzer zunächst auf einer Phishing-Seite, wo sie den Download selbst anstoßen müssen. Die Schadsoftware ist zum Beispiel als Paket-App getarnt.

Absender blockieren:

(siehe manuelles bzw. direktes blockieren von SMS Absendern, Seite 4)

Löschen der SMS:



Nachricht nach links verschieben, dann erscheint die o.a. Löschfunktion

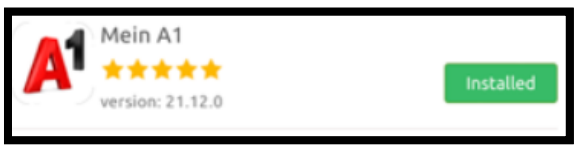
Vorgehensweise wenn Schadsoftware bereits installiert ist.

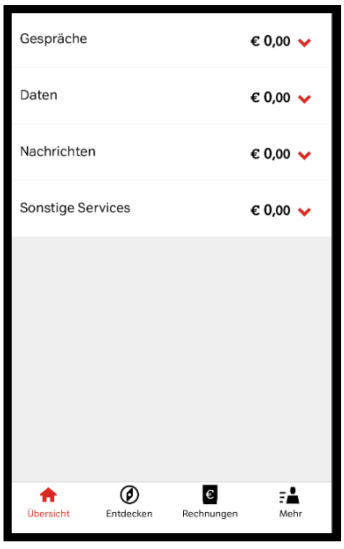
Betroffene schalten ihr mobiles Endgerät (Smartphones und Tablets) am besten sofort in den Flugmodus (abgesicherter Zustand).

Falls noch nicht feststeht, ob Kosten entstanden sind, gilt es, das als nächstes zu prüfen.

Auf allen dienstlichen Endgräten steht die App „Mein A1“ zur Verfügung. Ist die App nicht bereits installiert, so kann diese über die App „Catalog“ manuell installiert werden.

Die App „Mein A1“ öffnen und „Verbindungsentgelte“ auswählen, danach erscheint die u.a Übersicht.





Bei Kostenbestand oder Verdacht unverzüglich mit der zuständigen Logistikabteilung bzw. BMI Helpdesk Kontakt aufnehmen, do werden dann erforderliche Schritte wie zB. Sperre der SIM etc. vorgenommen. Zur Übersicht kann ebenso via zuständiger Logistikabteilung ein Kostennachweis beim Provider (A1) angefordert werden.

Manuelles löschen von schadhaften Apps (Flugmodus):

Im abgesicherten Modus sucht man jene Apps, die zuletzt und nicht bewusst selbst installiert wurden. Diese Apps entfernt man und startet das Smartphone neu. Im schlimmsten Fall hilft aber nur das Zurücksetzen in den Auslieferungszustand.

Bevor dies geschieht, nicht vergessen, die Daten auf dem Gerät in einem Onlinespeicher (Cloud) oder auf einer Speicherkarte zu sichern. Dann geht man in den Einstellungen zum Punkt "Allgemein“ – „iPhone übertragen/zurücksetzen" – „Alle Inhalte & Einstellungen löschen“.

Achtung: Bumerangeffekt bedenken (Wenn das Endgerät nicht in den Auslieferungszustand gesetzt wird und verdächtige Apps einzeln gelöscht werden)

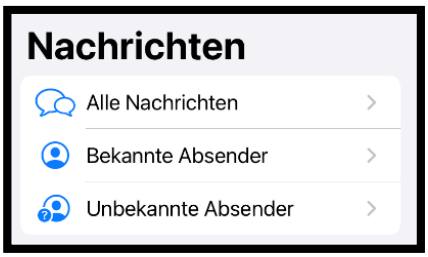
Wer anschließend seine Daten wieder aus einer Cloud-Sicherung aufs Gerät installieren möchte, sollte unbedingt darauf achten, dass in dem Cloud-Speicher keine schadhaften Apps darunter sind. Sonst befindet sich der Trojaner gleich wieder auf dem mobilen Endgerät ! Dahingehend wird eine einzelne manuelle Installation aus dem App Store empfohlen.

So schützen Sie sich vor Spam-SMS

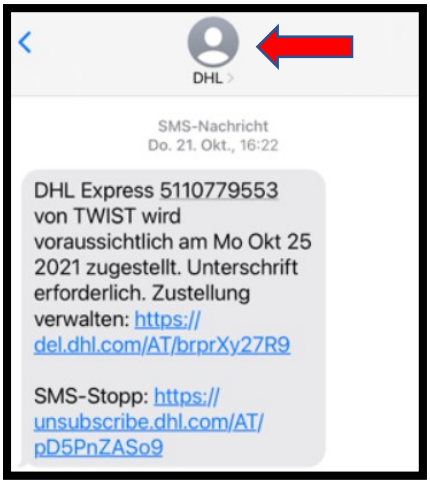
Smartphones verfügen bereits über einen generellen eingebauten Spam-Filter für SMS.

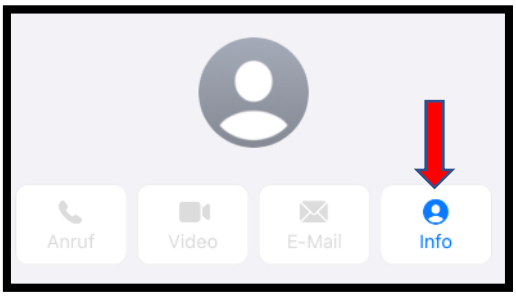
Zukünftig werden Nachrichten von Absendern, die nicht in den Kontakten gespeichert sind in eine eigene Liste abgelegt bzw. gefiltert. Dadurch kann ein versehentliches öffnen unter den sicheren Nachrichten verhindert werden.

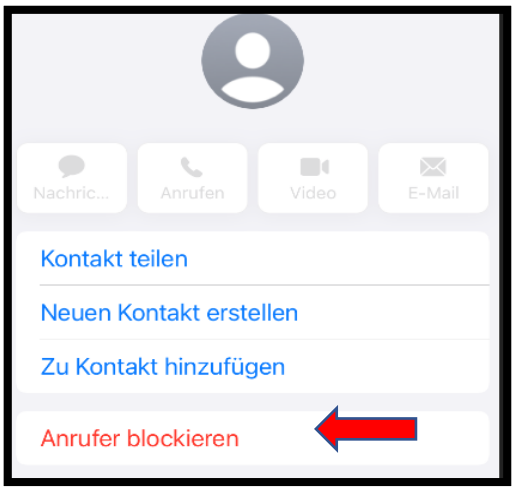
Danach können nicht erwünschte oder verdächtige Nachrichten über die Funktion „Filter“ aufgerufen und aus der Liste „unbekannte Absender“ gelöscht werden.



Manuelles bzw. direktes blockieren von SMS Absendern (nach Erhalt einer SMS Nachricht):







Versehentlich blockierte Absender können wieder von der Blockade entfernt werden.

Einstellungen-Nachrichten-Blockierte Kontakte-Bearbeiten-Deaktivieren