Phishingversuch mit angeblichen Telekom-Mails

Martin Himmelheber (him)
21. Mai 2020
Mit teilweise sehr gut nachgemachten Mails, die aussehen wie von der Telekom oder auch anderer Unternehmen, versuchen Betrüger Computernutzer auszunehmen. Die Polizei rät, solche Mails zu löschen und keinesfalls irgendwelche Schaltflächen auf den Mails anzuklicken.

„Das sind klassische Phishing-Versuche“, erläutert Jörg Dieter Kluge vom Polizeipräsidium Konstanz. Das Phishing ist eine verbreitete Methode von Internetbetrüger an vertrauliche Daten zu gelangen.

Was ist der Zweck dieser Mails?

Bei den „Telekom-Mails“ und ähnlichen Mails geht es den Gaunern laut Kluge darum, herauszufinden, ob hinter einer E-Mail-Adresse eine reale Person steckt. „Wenn man antwortet durch einen Click, erkennt das Programm des Absenders: ‚den gibt es‘. Und dann geht es los.“

Es gibt für die E-Mailversender zwei Möglichkeiten, was sie mit der Information anstellen können: Sie können die Internetadresse verkaufen. Oder es stecken direkt Betrügerbanden dahinter.

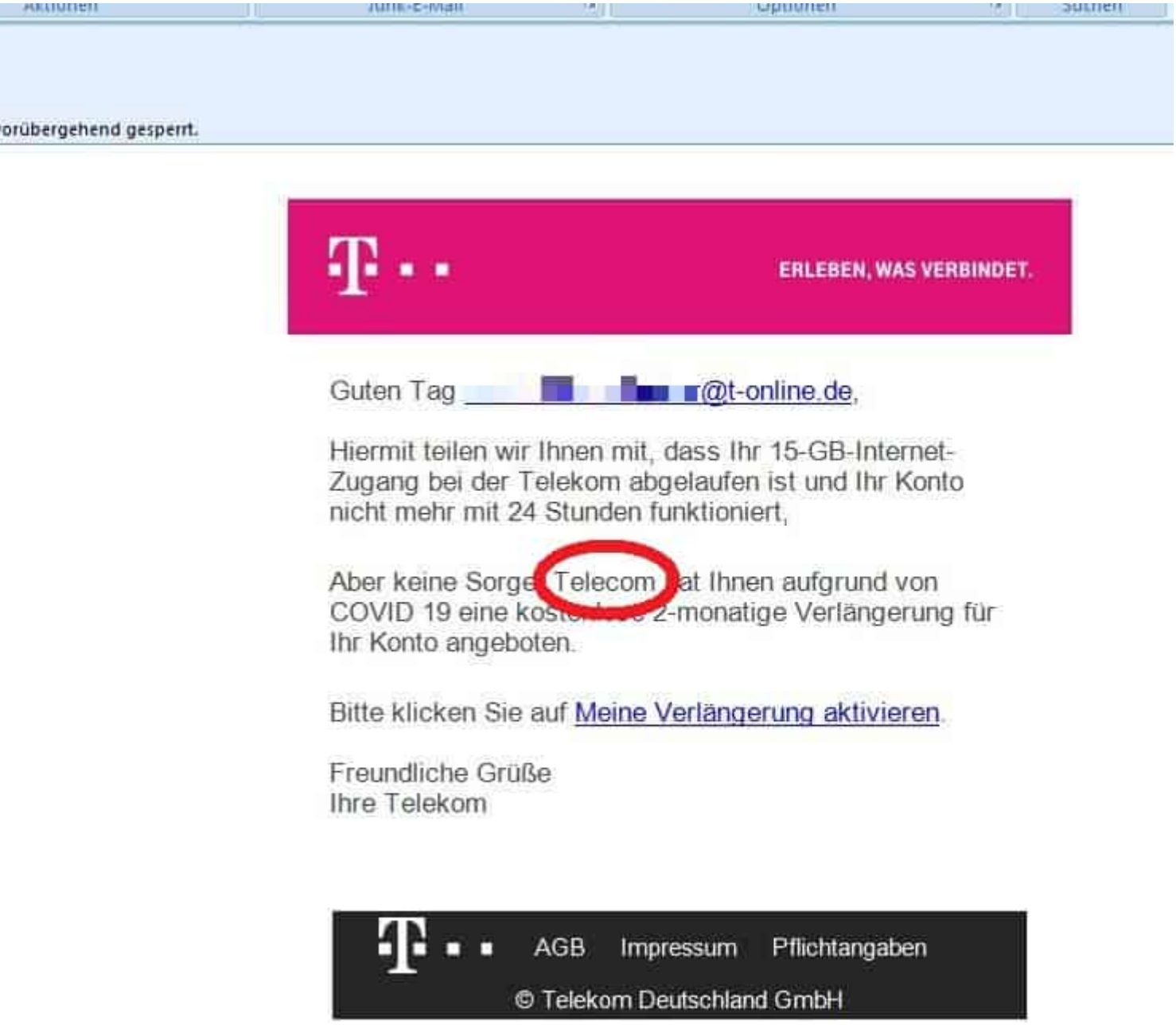
Bei Adressverkauf melden sich anschließend alle möglichen Anbieter bis hin zu Online-Casinos und Schmuddeligerem, die ihre Dienste anbieten. Solche bestätigten Adressen sind teuer zu verkaufen.

Und was passiert bei Betrügerbanden?

Diese versuchen über weitere Mails an Bankdaten zu kommen, versuchen, ob sie Zugriff auf die Konten bekommen, die TAN erfragen oder über den Enkeltrick und ähnliches ihre Opfer auszunehmen.

Wie kann es sein, dass die Mails dem Original so täuschend ähnlich sehen?

„Das ist sehr leicht zu fälschen“, sagt Kluge. Erkennen kann man die plumperen Fälschungen an krummem Deutsch, Rechtschreibfehlern beispielsweise. Aufschlussreich sind auch die E-Mail-Absender.



ürde sich durchgehend richtig schreiben. Screenshot him

Oft stehen dort Allerweltsnamen wie Thomas Maier, Bernd Müller. Auch ausländische Absender finden sich gelegentlich noch. Die Absender nennen in der Anrede den Empfängernamen selten, in unserem Beispiel haben sie die E-Mailadresse als Namen eingefügt. Ein seriöser Absender würde das sicher nicht tun.

Wieso werden solche Mails nicht verhindert?

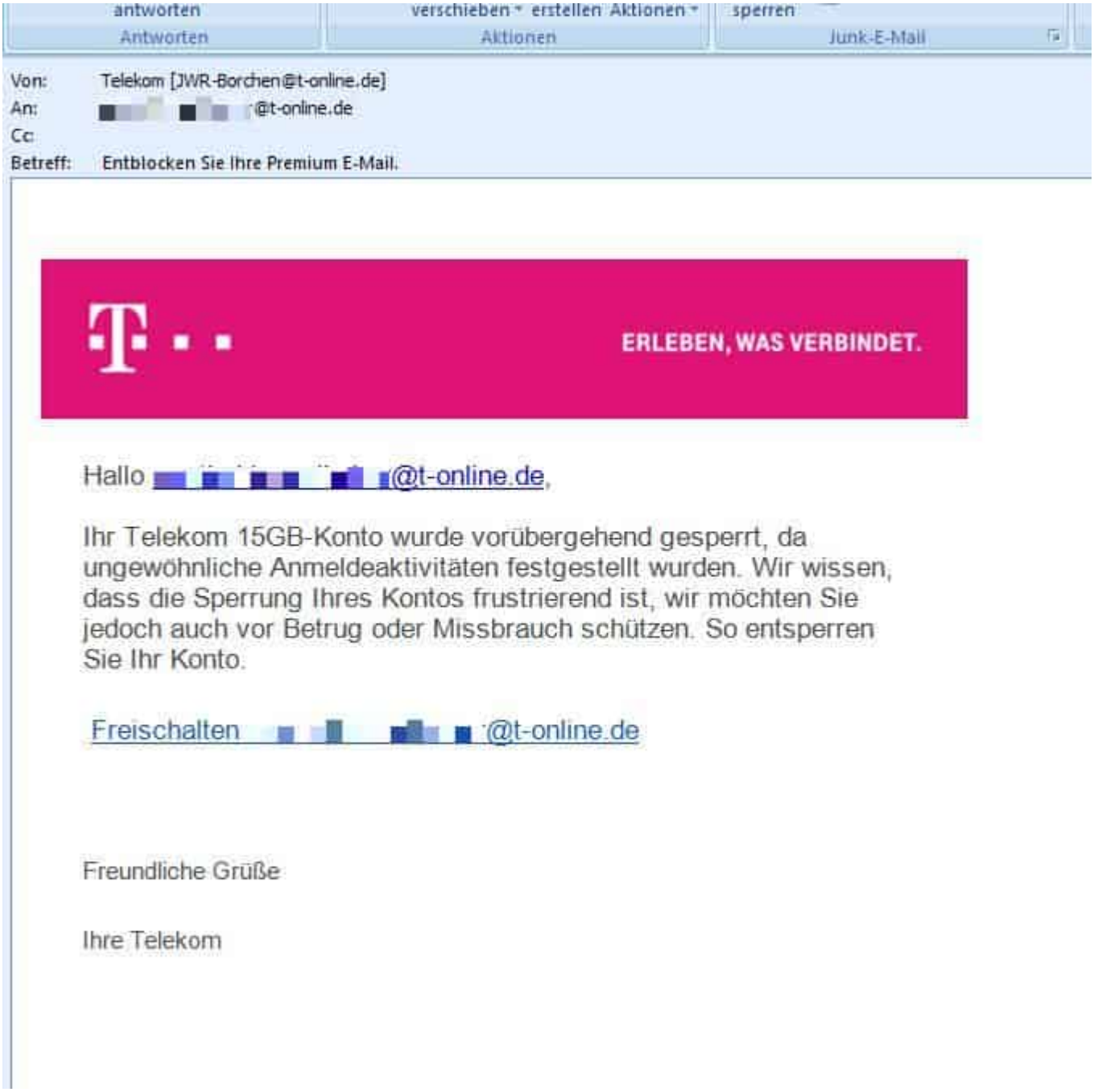
Nur der Versand einer solchen Mail ist laut Kluge nicht strafbar. Erst wenn später daraus ein Betrugsdelikt folgt, wird dieses strafbar.

Was sollte man als Empfänger tun?

Kluge rät: Sofort löschen. Man kann auch versuchen, den Spamfilter so einzustellen, dass diese Mails gar nicht im Posteingang landen. Aber mit neuen Namen und Adressen umgehen die Gauner das. Solche Mails stammen in aller Regel nicht von den „echten“ Dienstleistern. Wichtige Informationen schicken die Unternehmen immer noch per normaler Post in Papierform, weil das nicht so leicht zu fälschen ist. „Lieber drei Mal löschen als einmal versehentlich öffnen“, so Kluges Rat. „War es ein ehrlicher Anbieter, dann wird er sich nochmals melden.“

Wer fällt auf solche Mails herein?

Niemand ist davor gefeit, so die Beobachtung der Polizei. „Wir hatten schon Rechtsanwälte, Vorstandsvorsitzende von Firmen, intelligente Menschen, die hinterher sagen: ‚Wie konnte ich so blöd sein?‘“ Die Tricks der Betrüger sind raffiniert. Und die Menge macht’s: Wenn bei 100 ausgesandten Mails einer reinfliegt, hat es sich schon gelohnt.



Besonders nett: Die Gauner wollen in dieser Mail den Empfänger vor Betrügern schützen. Danke, aber Nein Danke! Screenshot: him

Nachtrag: Prüft man die E-Mailadre