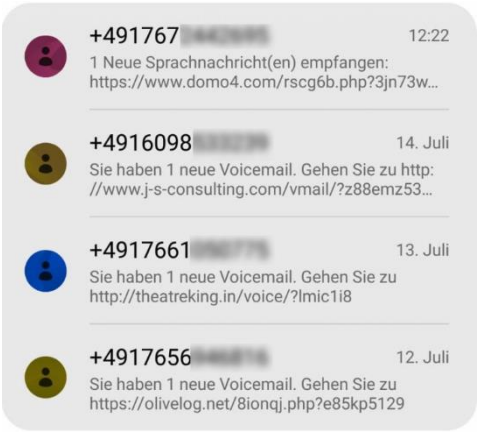
Neue betrügerische SMS im Umlauf

Wie sieht der Betrug aus?
Der Betrug per SMS-Nachricht nimmt zu. Vor einiger Zeit waren es noch Nachrichten mit gefälschten Paket-Benachrichtigungen *(lesen Sie hier den ausführlichen Beitrag)*, nun gibt es eine neue Welle. Aktuell sind nämlich vermehrt SMS mit der Nachricht über eine angebliche *Voicemail* (oft auch Sprachnachricht oder Mailbox-Nachricht genannt) im Umlauf. Solche SMS werden tatsächlich auch in seriösen Fällen vom Mobilfunkanbieter verschickt, wenn man einen Anruf verpasst hat und jemand eine Nachricht hinterlassen hat. Man kennt solche Benachrichtigungen als Handy-Besitzer entsprechend bereits. Das machen sich die Betrüger nun zunutze und versenden gefälschte SMS, in denen ein Link enthalten ist. Diesen Link soll man anklicken, um die angebliche Sprachnachricht (Voicemail) abzuhören. Und genau hier wird es gefährlich, denn durch ein Anklicken öffnet sich **nicht** die vermeintliche Sprachnachricht, sondern eine betrügerische Internetseite. Hier können jetzt verschiedene Dinge passieren. Es ist zum Beispiel möglich, dass eine neue Anwendung auf das Handy heruntergeladen wird, die Schaden anrichtet. Es können aber auch automatische kostenpflichtige Anrufe passieren (von Ihrem Handy aus, ungewollte) oder die App versendet im Hintergrund und unbemerkt durch den/die Nutzer/in Nachrichten an das gesamte Adressbuch.
Manchmal kommt dieser Betrug nicht per SMS auf dem Smartphone an, sondern per E-Mail. Denn die Betrüger können leichter und schneller und viel mehr Menschen anschreiben, wenn Sie den Weg über die E-Mail gehen. Für den Betrug macht das im Weiteren keinen Unterschied: Viele Menschen sehen nur die Benachrichtigung oben im Handy, dass eine Voicemail/Sprachnachricht angekommen ist, und entdecken gar nicht erst, dass es keine SMS war, sondern eine E-Mail, die darüber informiert. Auch bei dem Weg über die E-Mail führt ein Antippen/Anklicken des Links ins Verderben. **Und auch wie bei der SMS ist das reine Anschauen der E-Mail noch nicht problematisch.** Erst das Antippen des Links startet das Unheil und bringt die Probleme mit sich.

Was ist zu tun?



Bitte tippen Sie auf keinen Fall den Link in der SMS an, falls Sie eine solche Nachricht erhalten. Löschen Sie solche Nachrichten sofort. Das Lesen einer Nachricht ist noch nicht problematisch, nur das Antippen des Links sorgt für den Schaden auf dem Handy. Sollten Sie angetippt haben, so bestätigen Sie bitte keinesfalls das Herunterladen oder Installieren von irgendwelchen Anwendungen, falls eine solche Nachfrage erscheint. Es kann aber auch sein, dass ohne Bestätigung etwas installiert wird. Wenn Sie sich nicht sicher sind, kontrollieren Sie die zuletzt installierten Apps und löschen Sie zuletzt installierte, unbekannte Anwendungen. Es ist auch möglich, die Nummern, von denen die betrügerischen SMS kommen, zu blockieren. Vermutlich wird dies aber kaum etwas helfen, da diese SMS fast jedes Mal von einer anderen Nummer verschickt werden. Eine “dicke Haut” gegen solche Betrugsversuche zu entwickeln, ist der beste Weg damit umzugehen. Auch ein Gang zur Polizei ist nicht erfolgsversprechend; es sei denn, Sie haben den Link angetippt, wurden wahrhaftig und vollständig ein Opfer des Betrugs. Wenn finanzielle Schäden, Datendiebstahl oder andere Schäden auf dem Gerät entstanden sind, dann sollten die Behörden informiert werden.

Kosten verhindern

Um Kosten zu verhindern, können Sie außerdem die sogenannte Drittanbietersperre bei Ihrem Mobilfunkanbieter aktivieren, über die wir schon häufig gesprochen haben. Sie verhindert, dass Unternehmen (oder Betrüger) über Ihre Handyrechnung Beträge abbuchen können. Das bringt eine gewisse Absicherung gegen bestimmte Betrugsverfahren. Lesen Sie hierzu auch unseren ausführlichen Beitrag zum Thema Drittanbietersperre:

Schutz vor Abofallen und Handybetrug (nur verfügbar für Mitglieder)

Grundsätzlich muss man außerdem sagen, dass die Gefahr bei Nutzerinnen und Nutzern von Android-Geräten deutlich höher ist, als bei Menschen, die ein iPhone verwenden. Denn beim iPhone können nicht einfach so neue Anwendungen heruntergeladen und installiert werden. Bei Android ist dies eher möglich, auch weil hier Installationen vorbei am Play Store möglich sind. Solche Installationen sind nicht durch die Sicherheitskontrollen des Play Store gelaufen und können solche betrügerische Programmfunktionen enthalten. Das iPhone erlaubt generell nur Installationen aus dem App Store, einen Weg daran vorbei gibt es nicht. Unter dem Aspekt der Sicherheit ist dies ein Vorteil für die Apple-Welt.

Quelle: https://levato.de/betruegerische-sms-im-umlauf/