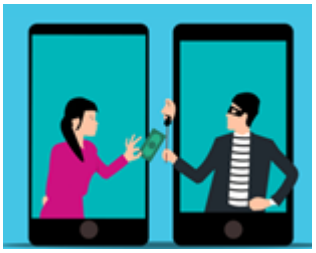
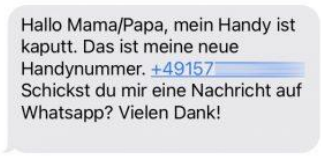
Betrug im großen Stil über SMS und WhatsApp

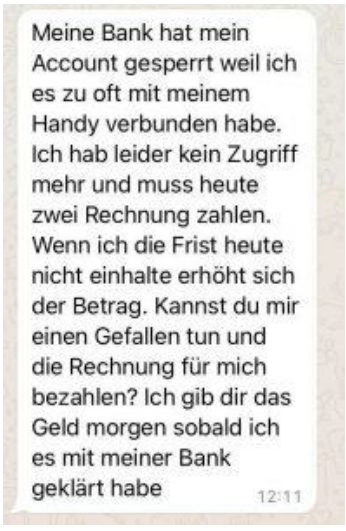


Schon im letzten Jahr haben wir darüber berichtet, wie der Enkeltrick zum Kindertrick wurde. Die Masche in Kurzform: Betrüger nehmen per SMS oder WhatsApp Kontakt auf und behaupten, sie seien das Kind der Betroffenen und hätten jetzt eine neue Telefonnummer. Sie bitten darum, die Nummer abzuspeichern. Danach bitten die Betrüger (die sich als die Kinder ausgeben) um finanzielle Hilfe. Zum Beispiel soll Geld vorgelegt und auf ein Konto überwiesen werden. Dafür nennen die Betrüger seriöse Kontodaten einer deutschen Bankverbindung und bauen Druck auf: Es müsse sehr schnell gehen! Diese Masche wird wieder vermehrt angewendet, auch wir haben auf unseren privaten Smartphones die Nachricht zur Kontaktaufnahme in den letzten Wochen und Monaten erhalten.
Für diesen Beitrag sind wir auf den Betrugsversuch eingegangen und **haben mit den Betrügern geschrieben**, um genau zu sehen, wie die Masche funktioniert. Im Anschluss haben wir mit der **Deutschen Bank** und mit der **Kriminalpolizei** gesprochen, um zu erfahren, wie man sich in so einem Fall am besten verhält.

Das sagen die Betrüger



Die erste Kontaktaufnahme der Kriminellen erfolgte in unserem Fall per SMS. Woher die Betrüger unsere Handynummer haben, ist dabei unklar. Entweder wurde sie einfach erraten (die Computerprogramme der Betrüger schreiben tausendfach zufällig erstellte Handynummer an) oder sie ist durch ein Datenleck bekannt geworden und im Internet veröffentlicht worden. Der Wortlaut der SMS: ***"Hallo Mama/Papa, mein Handy ist kaputt. Das ist meine neue Handynummer: +49157…… . Schickst du mir eine Nachricht auf WhatsApp? Vielen Dank!"***
Die Betrüger wissen dabei nicht, ob die Empfänger der SMS tatsächlich Kinder haben. Sie senden die Nachricht an unzählige Handynutzer und hoffen dabei einfach, dass jemand darauf hereinfällt, der *(erwachsene)* Kinder hat und die Nachricht für echt hält. Und das funktioniert leider sehr oft.
INTERESSANT: Warum erfolgt die Kontaktaufnahme eigentlich per SMS, wenn die Unterhaltung danach bei WhatsApp stattfinden soll? Das hat vermutlich folgenden Hintergrund: Wird man über WhatsApp von einer fremden Nummer angeschrieben, so erhält man von WhatsApp direkt den Hinweis, dass es sich um Spam handeln könnte, mit der Möglichkeit, die Nummer sofort zu blockieren. Per SMS gibt es solche Warnungen in der Regel nicht. Startet man nun selbst aktiv bei WhatsApp einen Chat und beginnt auf Eigeninitiative hin, der Person bei WhatsApp zu schreiben, so taucht der Hinweis dort dann nämlich nicht auf!
Wir sind auf die Kontaktaufnahme eingegangen und haben den Betrügern geantwortet, um zu sehen, was passiert. Wir haben zuerst gefragt, was denn mit dem Handy unseres angeblichen Kindes passiert sei und mit "Mama" unterschrieben. Die Betrüger haben daraufhin geantwortet, das Handy sei heruntergefallen und dabei kaputt gegangen. Daraufhin haben die Kriminellen uns direkt gefragt, ob wir kurz Zeit hätten und ob wir ihnen einen Gefallen tun könnten. Natürlich haben wir "ja" gesagt. Es wurde behauptet, es müsse dringend eine Rechnung bezahlt werden, man könne aber gerade nicht auf das Online-Banking zugreifen. Wir wurden gefragt, ob wir die Überweisung schnell durchführen könnten. Wir haben wieder "ja"



gesagt. Danach wurde uns eine Kontoverbindung bei der Deutschen Bank genannt, an die ein Betrag in Höhe von 1862,76 Euro überwiesen werden sollte. Als wir nicht zeitnah reagiert haben, wurde direkt Druck ausgeübt. Daraufhin haben wir die Unterhaltung abgebrochen und die Nummer blockiert. Von der Unterhaltung haben wir Bildschirmfotos als Beweis angefertigt.

Das sagt die Deutsche Bank

Verwundert hat uns, dass die Betrüger ein Konto bei der Deutschen Bank für den Trick verwendet haben. Denn darüber müsste der Kontoinhaber ja sehr leicht zu finden und zu schnappen sein. Daher haben wir mit dem **Kundendienst der Deutschen Bank** gesprochen und gefragt, wie das sein kann. Dort war der Trick selbstverständlich gut bekannt. Man sagte uns, dass unter anderem gekaperte/gehackte Konten verwendet werden. Die eigentlichen Kontoinhaber wissen oft gar nichts davon, dass ihr Konto von den Betrügern missbraucht wird. Man hat uns dazu geraten, die betroffenen Kontodaten an die Deutsche Bank zu übermitteln. Fast jedes Bankunternehmen hat für solche Fälle eine eigene Phishing-/Betrugsabteilung. Die Bank kann dann die Aktivitäten auf dem für den Betrug genutzten Konto überwachen und es bei ungewöhnlichen Vorgängen vorübergehend sperren. Außerdem riet man uns dazu, Anzeige gegen unbekannt zu erstatten.

Das sagt die Polizei

Danach haben wir uns an die Polizei gewendet, genauer gesagt an die Abteilung **Cybercrime des LKA Rheinland-Pfalz**. Wir wollten wissen, wie man sich in solch einem Fall am besten zu verhalten hat, was die Polizei tun kann und ob eine Anzeige überhaupt erfolgsversprechend ist. Man hat uns erklärt, dass die Betrüger ausgesprochen professionell vorgehen und sogar in Teams arbeiten, wobei manche Personen für die Kontaktaufnahme zuständig sind, andere für die Verwaltung der gekaperten Konten und das Abschöpfen der erbeuteten Gelder. Für die verwendeten Konten werden sogar dritte Personen als angebliche Minijobber geködert, die unter einem Vorwand darum gebeten werden, ein Konto bei einer Deutschen Bank zu eröffnen. Über diese Konten laufen dann die Zahlungen, ohne dass die eigentlichen Kontoinhaber überhaupt wissen, dass sie Teil einer Betrugsmasche sind. Um gegen die Betrüger vorzugehen, sammelt die Polizei so viele Daten wie möglich. Daher ist es ratsam, wenn man selbst Opfer wurde, Anzeige zu erstatten. Das gilt auch, wenn noch kein finanzieller Schaden ist, weil man den Betrug rechtzeitig bemerkt hat. Die Polizei kann erstens die verwendeten Handynummern sperren und zweitens die verwendeten Bankkonten überprüfen und einfrieren lassen. Dafür kann man sich an die örtliche Polizeidienststelle wenden oder aber die sogenannte **Onlinewache** verwenden, über die man über das Internet und ein entsprechendes Formular Hinweise an die Polizei geben und Anzeige erstatten kann. Diese Onlinewache gibt es für jedes Bundesland, hier finden Sie eine Übersicht: *https://www.bka.de/DE/KontaktAufnehmen/Onlinewachen/onlinewachen_node.html*
Die Polizei rät dazu, Bildschirmfotos anzufertigen, um die betrügerischen Aktivitäten zu belegen.

Hier zeigen wir, wie man Bildschirmfotos auf allen Geräten anfertigen kann: www.levato.de/hilfe
INTERESSANT: Die reine Kontaktaufnahme ist trotz des Schwindels rechtlich gesehen noch keine Straftat! Erst dann, wenn die Betrüger zur Zahlung auffordern, handelt es sich rechtlich gesehen um eine Straftat.