Tatort WhatsApp

Seit über einem Jahrzehnt treiben sich Cyber-Kriminelle auf der beliebten Messaging-Plattform herum. Was genau sie dort tun, enthüllen wir hier und präsentieren die zehn häufigsten Betrugsmaschen auf WhatsApp.

Von Claudia Holzer

Allein in Österreich werden jährlich rund 60.000 Cybercrimes gemeldet

So mancher mag sich noch an die Zeit erinnern, als das Versenden von „SMS" limitiert war, Nachrichten, Bilder oder Videos außerhalb Österreichs zu verschicken, gar nicht in Frage kam und eine Nachricht gleich mehre Cents wert war. Getrieben von genau diesen Spesen sowie der zunehmenden Ineffizienz der SMS-Kommunikation nahmen sich zwei US-amerikanische Studenten gemeinsam vor, eine Lösung zu entwickeln. Ihr Ziel war es, die internationale digitale Kommunikation auf revolutionäre Weise zu verändern. Im Jahr 2009 präsentierten Jan Koum und Brian Acton schließlich ihr Ergebnis: WhatsApp.

Mit der Verbreitung von WhatsApp öffneten sich bislang unvorstellbare Möglichkeiten für die Art und Weise, wie Menschen miteinander kommunizieren. Nachrichten, Fotos und Videos konnten plötzlich innerhalb von Sekunden über große Entfernungen hinweg verschickt werden. Und das Beste daran? Das alles, ohne einen weiteren Cent zu zahlen.

Nach den Anfängen in Amerika, schaffte es WhatsApp auch nach Europa. Nicht mal zehn Jahre später – in 2017 und 2018 – erreichte die Plattform ihren Höhepunkt. Zu dieser Zeit hatte die SMS-Alternative mehr als eine Milliarde monatlich aktive Nutzer weltweit und gehörte zu den am weitesten verbreiteten Messaging-Apps auf dem Markt.

Die Schatten des Erfolges

Aber – wie bei jeder Erfolgstory – gibt es auch bei dieser eine Schattenseite: Die App überzeugte nicht nur ehrliche User, sondern auch – aufgrund der enormen Nutzerzahl – den ein oder anderen „Scammer". Bereits Mitte der 2010er Jahre tummelten sich die ersten Kriminellen auf der Plattform. Mit dem Ausbruch der Corona-Pandemie erreichte die Problematik dann einen Höhepunkt. Kriminelle nutzen geschickt den zunehmenden Fokus auf digitale Kommunikation, um so ihre eigenen Taschen zu füllen. Dies war der Zeitpunkt, wo Mag. Roman Taudes – nach langjähriger Erfahrung im Anlegerschutz – seine eigene Anwaltskanzlei gründete. Sein Schwerpunkt: Cyberkriminalität – ein Gebiet, das für viele Polizisten noch Neuland ist. Kryptowährungen- und

Adobe Stock

Anlagenbetrug rückten so in den Fokus.
Heute klingelt das Telefon im Minutentackt. Bis zu zehn Hilfesuchende täglich sehen in Taudes und seinem Team ihre letzte Rettung. Der Grund: Internet-Scams. Schäden ab 10.000 Euro bis hin in den Millionenbereich sind an der Tagesordnung.

Dunkelziffer und Aufklärungsquote

Laut dem jährlich veröffentlichten Cybercrime Report des Bundeskriminalamts gab es in 2022 über 60.000 gemeldete Fällen allein in Österreich. Ein Plus von 30,4 Prozent im Vergleich zum Vorjahr. Abgesehen von der niedrigen Aufklärungsquote von 33,9%, wird besonders auf die außerordentlich hohe Dunkelziffer hingewiesen, welche diesen Bereich betrifft.
Grund dafür seien die exorbitanten Summen, wie Taudes im Interview erklärt. Viele Opfer mit Schäden von „nur ein paar hundert Euro“ , scheuen sich aus zeitlichen und wirtschaftlichen Gründen, überhaupt eine Anzeige zu machen und werden dementsprechend auch nicht in der Statistik berücksichtigt. Zusätzlich wird dieses Verhalten von der weitverbreiteten Annahme gefördert, dass die Polizei sich „eh nicht auskennt“ und deswegen „sowieso nichts machen kann“. Tatsächlich trägt diese Aussage, so der Cybercrime-Spezialist, auch ein Fünkchen Wahrheit.
Denn hier spricht man nicht vom Einbruch über die Balkontür. Vom Love-Scamming über Gewinnspielfallen bis hin zum Anlagebetrug: Die Tricks und Maschen der Internet-Betrüger sind mittlerweile perfide komplex und ändern sich – wie man es von der digitalen Welt kennt – täglich. Ohne Knowhow, langjähriger Erfahrung und entsprechendem Programm sind den Helfern schnell die Hände gebunden.
Und obwohl jede Geschichte anders ist, erfreuen sich bestimmte Maschen über besonderen Erfolg. Das sind die zehn Bekanntesten, die man als Nutzer kennen sollte:

1. Der Enkeltrick

„Hey Papa! Ich brauche unbedingt deine Hilfe!“, schreibt eine unbekannte Nummer. Man ist sofort alarmiert, gibt so schnell wie möglich den Handy-Pin ein und drückt auf das grün-leuchtende Symbol. Komisch. Plötzlich ist das Profilbild der Tochter weg. Und die Nummer ist auch ganz anders.
„Ich habe mein Handy, meine Daten, sogar meine Telefonnummer verloren. Die ist jetzt neu. Die alte kannst du gleich löschen!“ Sowas kann passieren. „Aber Papa! Ich habe auch den Zugriff meines Bankkontos verloren und brauche jetzt unbedingt das Geld für meine Wohnungsmiete. Sonst werfen die mich gleich wieder raus, du weißt doch wie die sind! Bitte überweis es mir sofort auf das Bankkonto!“
So fing in den vergangenen Jahren nicht zu selten ein WhatsApp-Gespräch an. Und endete mit einer erfolglosen Anzeige bei der Polizei und ein paar tausenden Euro weniger in der Tasche.
Und so funktionierts: Hinter der verzweifelten Tochter, dem Sohn, dem Enkel oder dem Freund steckt in Wahrheit ein Unbekannter, der die Nummer des Opfers in den Tiefen des Internets gefunden hat.
Während manche Betrüger gezielt nach Personen suchen, machen es sich die meisten dann doch eher einfach. So bekommt auch der 21-jährige Student nicht selten eine Nachricht von seiner vermeintlichen Tochter, mit der Bitte, die Monatsmiete des Wiener WG-Zimmers auf ein unbekanntes Konto zu überweisen.
Aber – hin und wieder – ist das Glück auf der Seite der Betrüger und sie treffen genau ins Schwarze. Meistens lassen sie den Opfern auch nicht mal die Zeit zum Nachdenken, nutzen den sensiblen emotionalen Zustand aus, sei der Notfall ja „so dringend“. Wenn dann das Geld erstmal überwiesen ist, stehen die Chancen schlecht, dieses jemals wiederzusehen.

Empfohlene Vorgehensweise:

Das Stichwort ist hier: Prävention. Wenn eine unbekannte Nummer schreibt, sollte sofort Misstrauen geweckt sein. Ganz besonders wenn sich diese als Angehörige ausgibt. Kurz durchatmen und nachdenken! Dann reicht auch schon ein Anruf an den Unbekannten – der nicht abheben wird, oder noch besser: an den Angehörigen selbst – natürlich über seine „alte“ Nummer. Und wenn dieser von nichts weiß, sollte die Situation jedem klar sein. Nicht antworten und Nummer blockieren reicht dann auch schon, damit der Fall erledigt ist.

2. Love Scamming

Und emotional geht es auch weiter. Wieder mit einer Nachricht einer unbekannten Nummer. Aber Vorsicht: Meistens startet diese Masche schon viel früher. Auf einer Dating-App wie Tinder beispielsweise. Dabei lernen sich Betrüger und Betrogener kennen, tauschen Nummern aus und wechseln auf einen Messaging-Dienst.
Daraus wird dann ein wochen- oder gar monatelanges Hin- und Her. Dabei wird auf das Aufbauen von Vertrauen abgezielt, um dieses anschließend dreist auszunutzen.
Es beginnt wieder ein ähnliches Spiel wie beim „Enkeltrick“. Die Vertrauensperson ist in einer unerwarteten Notlage. Das kann die verlorene Kreditkarte auf der Geschäftsreise bis hin zur lebensnotwendigen Operation des Vaters

Kryptowährungen- und Anlagenbetrug stehen häufig im Fokus

sein. Egal welche Geschichte, Ziel ist immer eines: Geld. Davon viel. So schnell wie möglich. Und so unglaublich es jetzt klingen mag: Die Masche funktioniert.
„MeinBezirk.at" berichtete im vergangenen Jahr von einer 37-jährigen Niederösterreicherin und einer 29-jährigen Kärntnerin, die sich gleich beide in denselben „Chirurg", der zu Besuch aus den USA war, verliebten und dabei insgesamt mehrere zehntausende Euro verloren. Durch die Spitzenarbeit des Landeskriminalamts Kärnten gemeinsam mit der Staatsanwaltschaft Klagenfurt wurde dieser Täter überführt und festgenommen.
Nicht so viel Glück hatte ein 29-jährigen Linzer, der von einer derzeit noch unbekannten „jungen Damen" um eine Gesamtsumme im sechsstelligen Bereich betrogen wurde. Der Fall ist bis heute ungelöst.

Empfohlene Vorgehensweise:

Die Suchmaschinen-Funktion „Bilder der Suche" ist hier des Opfers bester Freund. Vor allem auf Dating-Websites: Um „echt" zu wirken, müssen die Täter gleich mehrere Bilder anbieten. Mit „Reverse-Searching" lässt sich herausfinden, in welchem Kontext diese noch genutzt wurden. Auch das Eingeben des Namens mit dem Zusatz „Scammer" in der Suchleiste, verhilft in manchen – seltenen – Fällen zur Aufklärung.
Ein weiterer Hinweis sind Fragen nach der finanziellen Situation, dem Lebenslauf oder den Lebensumständen sowie eine ungewöhnliche Lebensgeschichte mit Bezug zum Ausland. Aber auch eine sprachliche Barriere, welche sich oft in überdurchschnittlich vielen Grammatikfehlern oder fehlenden Deutschkenntnissen äußert, sollte hellhörig machen.
Und auch hier wieder der Rat zum Telefonanruf. Wenn sich die Person nicht zeigen oder reden will, steckt oft ein Betrüger dahinter.

3. Geschenkkartenbetrug

Hier erhält der Nutzer eine plötzliche Textnachricht von einem „seriösen" Unternehmen mit einem Link. Dieser führt meist zu einer infizierten Website, die ohne dem Wissen des Opfers eine Malware installiert.
Dabei handelt es sich um eine „bösartige" Software, welche entweder das Telefon-System extrem verlangsamt oder Bewegungen auf dem Gerät ausspioniert, dabei persönliche Daten sammelt und diese an Dritte weiterverkauft. Bei der „Ransomware" verlieren die Besitzer sogar ihren eigenen Zugang zu diesen und müssen sie erst zurückkaufen in Form von „Lösegeld". Bis dahin werden die Informationen als „Geiseln" gehalten.
Weniger technisch, aber gleich fatal sind „Gewinnspiele", die das Opfer dazu verleiten, persönliche Informationen preiszugeben, um den vermeintlichen Gewinn zu erhalten.

Empfohlene Vorgehensweise:

Auf das Öffnen von unerwarteten Links sollte immer (!) verzichtet werden. Bei Geübten empfiehlt sich ein kurzer Blick auf die URL, um dessen Authentizität zu überprüfen. Ist es dafür zu spät, sollte auf Zeichen einer Malware geachtet werden: Das Smartphone verlangsamt sich, es öffnen sich unerwartete Pop-ups oder ungewöhnliche Systemmeldungen scheinen auf. Auch die Datennutzung sollte beobachtet werden.
Im Falle einer Infektion sollte man das Handy umgehend vom Netzwerk trennen, sich ein Antiviren-Programm installieren und sich gegebenenfalls an einen IT-Experten wenden.

4. QR-Code Betrug

Ähnlich wie beim Geschenkkartenbetrug werden hier statt Links QR-Codes auf WhatsApp versendet. Dahinter verstecken sich gefälschte Seiten von Banken oder Online-Shops. Ziel ist das Sammeln von persönlichen Daten, Login-Daten oder gar Kreditkartennummern.
Damit kann Identitätsdiebstahl be-

unsplash

Mag. Roman Taudes ist für viele Opfer die letzte Rettung

gangen, Einkäufe mit der eigenen Kreditkarte getätigt oder auch Geld vom Bankkonto abgezogen werden.

Empfohlene Vorgehensweise:

Auch unbekannte QR-Codes sollten nicht angeklickt werden. Aber Achtung! Solche Nachrichten können auch von Freunden und Familie zugeschickt werden, die selbst Opfer der Aktion wurden und den Zugriff auf ihr Konto verloren haben.
In diesem Fall sollte auf ein QR-Code-Scanner zurückgegriffen werden. Dabei handelt es sich um eine App mit integrierter Sicherheitsfunktion, welche dazu konzipiert wurde, die Echtheit von QR-Codes zu prüfen.

5. Job-Annoncen-Betrug

Für Jobsuchende sind Online-Jobbörsen oft die erste Anlaufstelle. Wer nicht nur suchen, sondern auch gefunden werden will, kann dafür einen Account erstellen. Und mit viel Glück schreibt einen das Wunsch-Unternehmen sogleich von selbst an. Solche Anfragen erhalten täglich tausende von Personen allein in Österreich. Doch nicht alle sind echt. Dass ein – via WhatsApp versendetes – Jobangebot, tatsächlich „zu schön, um wahr zu sein" ist, musste ein Mandant von Herrn Taudes erst auf die harte Tour lernen.
Nachdem dieser den, für den juristischen Laien, vermeintlich „echten" Arbeitsvertrag unterschieben hatte, begann er auch schon den neuen Traumjob. Die Aufgabe: Online-Registrierungsprozesse bei Partnerbanken testen und darüber berichten. Nutzen sollte er – der Einfachheit halber –die eigenen Daten, welche natürlich auch im „Bericht" anschließend angegeben werden mussten.
Eine Arbeit, die pro Bank nicht mehr als eine halbe Stunde dauern und mit bis zu 200 Euro vergütet werden sollte. Statt dem Superlohn, standen dann aber zwei Männer an der Tür. In Polizeiuniform, bereit den Österreicher für die Einvernahme mitzunehmen.
Und so fand sich das Opfer plötzlich in der Rolle des „Täters" wieder. Die Konten, die er „testweise" angelegt hatte, existierten in Wahrheit tatsächlich. Und wurden für Geldwäsche verwendet. Das Geld darauf stammte von anderen Opfern derselben Täter. Als diese das wahre Ausmaß der Machenschaften erkannten, wandten sie sich natürlich an die Polizei. Die Ermittlungen führten jedoch nicht zu den eigentlichen Straftätern, sondern zu Taudes' Mandanten, der plötzlich mit der ernsten Möglichkeit einer Haftstrafe konfrontiert war.
In diesem Fall konnte das Fiasko zwar geklärt werden, den fehlenden Lohn und das traumatisierenden Erlebnis blieb aber trotzdem.

Empfohlene Vorgehensweise:

Wenn etwas „zu schön, um wahr zu sein" klingt, ist es in den meisten Fällen leider tatsächlich so. Seriöse Unternehmen melden sich zudem auch nur selten über WhatsApp. Dementsprechend sollte auf eine ausreichende Recherche, ein Treffen oder Telefonat mit den Arbeitgebern sowie die professionelle Überprüfung des Arbeitsvertrages nicht verzichtet werden.

6. Kryptowährung-Betrug

Eine unbekannte Nummer benachrichtigt ein Opfer mit der Aussicht auf eine „lukrative Investitionsmöglichkeit" mit hohen Renditen. Ist das Geld erstmal in den Händen des Täters, macht sich dieser aus dem Staub, ohne auch nur einen Cent anzulegen.

Empfohlene Vorgehensweise:

In solchen Fällen sollte sofort die Bank kontaktiert und die eigenen Accounts gesperrt werden. Wenn das Geld bereits weg ist, sollte man sich weiters an die Polizei wenden. Ebenso empfiehlt sich ein Rechtsanwalt, welcher sich insbesondere mit dieser Art von Fällen beschäftigt. Dieser besitzt meist über das geeignete Knowhow sowie dementsprechende Programme, welche eine Nachverfolgung ermöglichen.

Rene Hundertpfund

7.Verifizierungs-code-Betrug

Hier behauptet der Scammer, fälschlicherweise die Telefonnummer der Zielperson für den Erhalt des WhatsApp-Verifizierungscode angegeben zu haben. Der Code soll dann von ihr geschickt werden. Fällt der Betroffene darauf rein, kann er sich nach kurzer Zeit auch schon von seinem Konto verabschieden, da dieses dann in den Händen des Kriminellen liegt. Eine positive Nachricht: Da WhatsApp „Ende-zu-Ende-verschlüsselt" ist, können bereits bestehende nach der Übernahme des Kontos nicht gelesen werden. Er kann aber sehr wohl neue Nachrichten verschicken und Kontakte übernehmen.

Empfohlene Vorgehensweise:

WhatsApp bietet eine „Verifizierung in zwei Schritten" mit einen persönlichen sechsstelligen Pin. Zusätzlich kann eine Mailadresse angegeben werden, mittels welcher man im entsprechenden Situationen kontaktiert wird. Ohne den PIN kann der Täter das Konto nicht übernehmen. Sollte es bereits übernommen worden sein, kann man versuchen es wiederherzustellen. Dabei meldet man sich mit der Handynummer und dem gesendeten Verifizierungscode neu an.
Aber Achtung! Wird dieser Code mehr als zwölf Mal angefordert, wird das Konto für zwölf Stunden gesperrt.

8. WhatsApp Gold

Dieser Scam erstand in 2016 und taucht seitdem immer wieder auf. Es handelt sich um Nachrichten, die angeblich von einem „offiziellen" WhatsApp-Account stammen und Nutzer dazu einladen, auf „WhatsApp Gold" umzusteigen. Dabei werden viele neue Funktionen versprochen. Stattdessen wird jedoch Malware auf das Handy geladen, was Hackern Zugriff auf den Account und Kontakte ermöglicht.

Empfohlene Vorgehensweise:

WhatsApp Gold existiert nicht. Sollte sich das irgendwann ändern, würde die Information nicht per WhatsApp-Nachricht übermittelt werden, so der Messenger-Dienst. Dementsprechend sollte die Nummer blockiert und gemeldet werden.
Offizielle Accounts haben zudem auch immer (!) einen blauen Hacken.

9. Tech-Support-Betrug

Da wird der Trick mit dem blauen Hacken auch schon wieder ausgenutzt. Hier geben sich die Betrüger als WhatsApp-Mitarbeiter (mit Haken) aus, und behaupten die „Sicherheit des Kontos" zu prüfen. Daraufhin wird man zur Bestätigung der eigenen Identität – also zur Angabe sensibler Informationen – aufgefordert. In manchen Fällen sogar derer der Kreditkarte.

Empfohlene Vorgehensweise:

Den WhatsApp Support kontaktieren. Diesen findet man ganz einfach unter den Einstellungen im Bereich „Hilfe". Wenn dieser die Nummer nicht bestätigt, heißt es auch hier wieder: Blockieren und Melden.

10. „Sexortion"

Ähnlich wie „Love Scamming" beginnt auch hier die Masche mit einer Freundschaftsanfrage auf Social Media oder einer aus dem Nichts kommenden Nachricht auf WhatsApp. Meistens von einer unglaublich attraktiven Person. Wieder ganz im Sinne von „zu schön, um wahr Erweist sich die Kennlernphase als erfolgreich, wird der nächste Schritt eingeleitet. Hier gibt es jetzt zwei verschiedene Wege, die genutzt werden:
Die Täter fordern die Opfer zum Videochat auf, oft unter einem schummrigen Licht um ihre wahre Identität zu verschleiern. Sie beginnen sich auszuziehen. So soll es auch das Opfer tun. Ohne dem Wissen des Betroffenen wird der Call aufgezeichnet.
Für diejenigen, die sich nicht zum Videochat überreden lassen, haben die Verbrecher einen Plan B: Sie verlangen, dass die Opfer aufreizende Fotos oder Videos von sich senden. Die expliziten Bilder werden im Nachhinein nicht für die Belustigung des Täters genutzt. Sondern für ihre eigene Erpressung. Um einer Veröffentlichung bzw. Verbreitung der Fotos zu entkommen, werden auch hier wieder extreme Summe verlangt, welche die Opfer überweisen müssen.

Empfohlene Vorgehensweise:

Prinzipiell ist das Versenden von Nacktfotos keine gute Idee. Egal ob Bekannter oder Unbekannter. Und – sofern man die Identität des Liebhaber nicht selbst verifiziert hat – sollte ein solcher Akt auf jeden Fall unterlassen werden. Im Nachhinein kann– im besten Fall – nur noch die Polizei zur Hilfe kommen.

Zusammenfassend lässt sich sagen: Prävention ist der Schlüssel. Misstrauen gegenüber unbekannten Nachrichten, Vorsicht bei Links und Anhängen, und die Überprüfung von verdächtigen Angeboten sind wichtige Maßnahmen, um sich zu schützen.
Die Welt der Cyberkriminalität schläft nie, und Betrüger sind ständig auf der Suche nach neuen Opfern. Nur wer immer auf dem neuesten Stand ist, ist auch in der digitalen Welt sicher.