



!!! Vorsicht ! Betrüger auch in unserer Region unterwegs ! Vorsicht !!!

Zitat aus der RP, 17.02.2022, 1. Seite der Krefelder Stadtpost:

„Seniorin um hohen Geldbetrag betrogen

(bk) Eine Seniorin ist am Dienstag Opfer von Betrügern geworden. Wie die Polizei gestern mitteilte, verlor die Frau ... eine hohe fünfstellige Summe und Wertgegenstände. ...“

Wenn man solche Berichte liest, denkt man ja zunächst: „Wie kann man nur auf solche altbekannten Tricks hereinfliegen?“ Aber offensichtlich haben die Täter nach wie vor Erfolg mit ihren Maschen. In den vergangenen Wochen fanden sich in der örtlichen Presse immer wieder Berichte über ähnliche Betrugsversuche, bei denen häufig gezielt Seniorinnen und Senioren als Opfer ausgewählt wurden. Neben den Betrugsmaschen, vor denen wir in den letzten beiden Ausgaben des SSP gewarnt haben, häufen sich wieder Betrugsversuche mittels E-Mail oder Telefon.

- Bei den **E-Mail-Betrügereien** versenden die Täter E-Mails mit einer falschen Absenderangabe. Als Absender werden häufig Banken oder Sparkassen angegeben. Die Betrüger wollen ihre Opfer unter einem Vorwand dazu bewegen, einen Link anzuklicken der angeblich auf die Internetseite der Bank verweist. Auf dieser FALSCHEN Seite werden dann Angaben zu Kontonummer und Passwort abgefragt; mit diesen Daten räumen die Gauner dann möglicherweise das Konto leer.

Andere beliebte Absenderangaben sind die von Telefongesellschaften (Telekom), Polizei oder Bundeskriminalamt (BKA); die Anhänge bzw. Links bewirken meistens, dass ein Schadprogramm auf dem eigenen Rechner installiert wird, mit dem die Gauner von außen einen Zugriff auf den Rechner bekommen. Sie können damit den Rechner fernsteuern oder Tastatureingaben abfangen; so gelangen sie an Zugangsdaten und Passwörter.

- Bei der Telefon-Masche gibt es zwei typische Fälle: „**Schock-Anrufe**“, wobei diese neuerdings auch mittels „**Whatsapp-Meldung**“ auftreten und „**Hotline-Anrufe**“ / „**Service-Anrufe**“. Die „Schockanrufe“ und „Whatsapp-Meldungen“, auch bekannt als „Enkel-Trick“ oder „Verwandten-Trick“, gaukeln den Angerufenen vor, dass ein naher Angehöriger in finanziellen Schwierigkeiten steckt oder auch plötzlich schwer erkrankt ist. Es geht **IMMER** darum, dass der Angerufene schnell Geld besorgen soll und dieses an einen Kurier (oft angeblich ein Kriminalpolizist oder ein enger Freund des Betroffenen) übergeben soll. Auffällig ist, dass die Betrüger dem Opfer keine Zeit zum Nachdenken geben und häufig verlangen, dass man dauerhaft in telefonischer Verbindung bleibt; so wollen die Täter verhindern, dass man sich bei der Polizei melden oder bei den Betroffenen nachfragen kann.

Die „Hotline-Anrufe“ kommen häufig von einer angeblichen „Microsoft-Service-Stelle“; die Anrufer geben sich aber auch als Mitarbeiter anderer Firmen aus wie z.B. von Telefongesellschaften, von Banken oder neuerdings in Kempen von den Stadtwerken.

Das Ziel der Anrufe kann man auf zwei Arten beschreiben:

Entweder soll der Angerufene den Computer einschalten, eine bestimmte Internetseite aufrufen und dem Anrufer über diesen Weg Zugriff auf den eigenen Rechner ermöglichen, damit dieser dann „dringend erforderliche Wartungsarbeiten oder Updates“ durchführt, die „nur von besonders geschultem Service-Personal“ durchgeführt werden können.

Oder der Anrufer versucht, mit Hilfe eines erfundenen Sachverhaltes sein Gegenüber dazu zu bewegen, Kundendaten und Zugangsdaten, vor allem auch Passwörter, herauszugeben. Mit diesen Daten werden dann entweder Konten „leergeräumt“, oder beispielsweise Bestellungen ausgeführt.

In allen diesen Fällen gilt: **!!! VORSICHT - BETRUG !!!**

Weder Banken noch Polizei nehmen in solchen Fällen Kontakt mit ihren Kunden über einfache E-Mails auf. Wenn sensible Daten ausgetauscht werden müssen, kommen alle Informationen per Post. Also: **E-MAIL SOFORT LÖSCHEN!**

Und bei Schock-Anrufen oder Anrufen von Microsoft: **EINFACH AUFLEGEN!**

Falls Ihr Telefon eine Rufnummernanzeige hat, gegebenenfalls noch die Nummer des Anrufers notieren und anschließend bei der Polizei Anzeige erstatten. wh