POLIZEI
KOMMUNALPOLIZEI
REGION PFÄFFIKON

Falscher Polizist

Bei der zurzeit im Kanton Zürich zunehmend angewendeten Betrugsvariante gibt sich der Täter als Polizist aus. Die Telefonanrufe erfolgen oft unter einer technisch manipulierten Rufnummer. So kann selbst **die Polizeirufnummer** auf dem Display erscheinen.

Tatablauf

1. **Das Opfer erhält den Telefonanruf eines vermeintlichen Polizisten.**
   Dieser erzählt eine bestechende Geschichte. Beispielsweise, dass er in einem Betrugsfall ermittle und man bei einer verhafteten Person sensitive Daten über die angerufene Person vorgefunden hätte. Somit sei u.a. deren e-Banking-Konto nicht sicher und müsse vor einem „Hacker-Angriff" geschützt werden. Vielfach wird auch vorgeschoben, dass bei in der Region tätigen und verhafteten Einbrecher eine Namensliste mit potentiellen Opfern vorgefunden worden sei.

2. **Das Opfer wird aufgefordert, bei der Aufklärung der Straftat mitzuwirken.**
   Es solle als Lockvogel der Polizei bei der Ergreifung der Straftäter helfen und dabei sein Geld und andere Vermögenswerte bei der „Polizei" in Sicherheit zu bringen, um es vor dem Zugriff von Kriminellen zu schützen.

3. **Hat das Opfer in die Mitwirkung eingewilligt, wird es aufgefordert, seine Vermögenswerte bei der Bank zu beziehen oder am besten gleich Zugang zu seinem Computer, insbesondere zu seinem e-Banking zu gewähren.**
   Aktuell versucht die Täterschaft, das Opfer dazu zu bringen, dem vermeintlichen Polizisten den Fernzugriff auf seinen Computer zu ermöglichen. Dies gelingt mit der Installierung einer Fernwartungssoftware (Remotesoftware). Erteilt das Opfer dann die Freigabe des Fernzugriffs, kann die Täterschaft den Computer übernehmen und direkt auf Bankkonten zugreifen.

4. **Das Opfer wird zur Übergabe des Geldes oder Deponierung an einem angewiesenen Ort aufgefordert, sofern es nicht gleich direkt via e-Banking – meist ins Ausland – transferiert werden kann.**
   Nach wie vor beliebt ist die Aufforderung, Bargeld bei der Bank zu beziehen oder Bargeld und Wertgegenstände aus der Wohnung einem Polizisten an einem angewiesenen Ort zu übergeben oder sicherheitshalber an einer bezeichneten Stelle zu deponieren.

Wie kann ich mich schützen?

Seien Sie misstrauisch wenn ein Polizist (generell eine fremde Person) Sie dazu bringen will:

- eine Fernwartungssoftware auf Ihren Computer zu laden und ihm den Zugriff darauf zu gewähren.

- Bargeld oder Wertgegenstände abzuheben, jemandem zu übergeben oder irgendwo zu deponieren.

Verschaffen Sie sich Sicherheit, indem Sie:

- bei einem verdächtigen Anruf die Identität des vermeintlichen Polizisten abklären.
- den Anruf des vermeintlichen Polizisten selber durch Drücken der roten Taste auf ihrem Apparat unterbrechen, einen Moment warten und danach selbständig die Ihnen bekannte Telefonnummer des Polizeipostens an ihrem Wohnort oder die 117 wählen.

Handeln Sie besonnen, indem Sie:

- sich niemals unter Druck setzen lassen.
- niemals fremden Personen den Zugriff auf Ihren Computer gewähren.
- niemals Bargeld/Wertsachen an eine Ihnen unbekannte Person – auch wenn Sie Ihnen vertrauenswürdig erscheint – übergeben.

Verschaffen Sie sich Gewissheit, wen Sie vor sich haben. Das ist nicht unhöflich, sondern korrekt!

- Echte Polizisten weisen sich immer mit ihrem Polizeiausweis aus! Echte Polizisten verlangen niemals Geld von Ihnen am Telefon!

Ändern Sie Ihren Telefonbucheintrag!

- Bei der Suche nach potenziellen Opfern orientieren sich Telefonbetrüger am öffentlichen Telefonbuch. Darin suchen sie gezielt nach Personen mit einem traditionellen Vornamen, da dieser einen Hinweis auf das Alter liefern könnte. Beugen Sie vor, indem Sie Ihren Vornamen im Telefonbuch auf den ersten Buchstaben reduzieren und somit anonymisieren.
- Das Formular "Anderung des Telefonbucheintrags" kann bei der Kommunalpolizei Region Pfäffikon angefordert warden.

Achtung – neue Entwicklungen beim Vorgehen der Täter!

Die Täter lassen sich immer neue Vorgehensweisen einfallen, um an das Geld ihrer Opfer zu kommen. So geben Sie sich – teilweise auch in CH-Dialekt - als Mitarbeiter einer Bank, einer Finanzaufsichts- oder Bankenaufsichtsbehörde aus. Mit Argumenten wie, es seien betrügerische Abbuchungen von Dritten erfolgt oder es bestehe die Gefahr, dass die Bankkonten gehackt werden könnten, wird versucht, die angeblich betroffene Person dazu zu bringen, Geld abzuheben, zu überweisen oder den Bankkarten-Code preis zu geben. Weder Banken noch die Polizei verlangen von Ihnen am Telefon, irgendwelche Finanztransaktionen zu tätigen! Lassen Sie sich niemals unter Druck setzen! Geben Sie keine Informationen wie Passwörter oder Pin-Codes weiter! Melden Sie solche Anrufe sofort der Polizei!

Quelle: Kantonspolizei Zürich, www.telefonbetrug.ch