POLIZEI
Nordrhein-Westfalen
Bonn

KK KP/O - Telefonbetrug

Polizei Bonn warnt vor neuen Maschen des Telefonbetrugs:

Die Bandansage - die falschen Mitarbeiter*innen von Europol oder Interpol - der Fernzugriff auf den eigenen Computer

Die Kreativität und Anpassungsfähigkeit der Täter*innen kennen keine Grenzen. Wir warnen Sie vor konkreten Phänomenen und schon passen die Betrüger*innen ihre Vorgehensweise an und wandeln Ihre Maschen ab. Im Bereich des Telefonbetruges sind neue Varianten zu den Ihnen vielleicht schon geläufigen hinzugekommen.

Im deutschsprachigen Raum, bundesweit und im Zuständigkeitsbereich des PP Bonn ebben Hinweise auf betrügerische Anrufe, die sich o.g. Stichworten zuordnen lassen, nicht ab.

Anruf kommt nicht selten anonym oder mit manipulierter Rufnummernanzeige!

Bei Anrufen von potenziellen Opfern manipulieren die Täter*innen nicht selten mittels des sogenannten „Call-ID-Spoofing“ die Rufnummernübermittlung beim Angerufenen so, dass auf dem Display z. B. die Rufnummer der örtlichen Polizei, Staatsanwaltschaft usw. oder sogar die Notrufnummer 110 (in der Regel in Verbindung mit der örtlichen Vorwahl vorweg (z. B. 0228 110) oder anderen Zahlenfolgen (111, 113, …) erscheinen.

Eines ist aber bei allen Vorgehensweisen der Telefonbetrüger*innen gleich: Die Kriminellen zielen zuallererst darauf ab, Betroffene zur Übergabe oder Überweisung von Geldbeträgen zu bewegen.

Die Bandansage

Die Täter*innen spielen zu Beginn des Telefonats eine Bandansage ab: Eine Computerstimme meldet dem Angerufenen z.B., dass aktuell in der Ortschaft/Nachbarschaft eingebrochen wird. Eventuell wird auch ein Passwort genannt und aufgefordert, es sich zu merken. Im weiteren Verlauf des Anrufs schaltet sich ein(e) falsche(r) Polizistin unter Passwortabfrage zu und versucht dem Betroffenen einzureden, dass seine Wertsachen gefährdet seien und die Polizei diese in Sicherheit bringen wolle. Oder Sie hören z.B. eine englischsprachige Bandansage: "*Your Identity Card has been misused.*" und werden dann aufgefordert, die Taste "1" an Ihrem Telefon zu drücken. Ein vermeintlicher "Police Officer" der deutschen Bundespolizei meldete sich in gebrochenem Englisch und forderte zum Beispiel Kreditkartennummern oder andere persönliche Daten. Zwei Beispiele von vielen möglichen.

Bedenken Sie: Gegebenenfalls kann auch ein anderes polizeiliches Szenario beschrieben werden.

Die falschen Mitarbeiter*innen von Europol oder Interpol

Bei anderen Anrufen - u.U. zunächst auch mit Bandansage - gaukeln angebliche Mitarbeitende internationaler Polizeibehörden Europol und Interpol unterschiedliche glaubwürdig anmutende, aber trotz allem erdichtete Vorfälle vor.

„This is a message from the Federal Police Department.“

Die Bandansage

Oh Schreck - ein Anruf der Polizei? Auf Englisch? Was kann da passiert sein?

Den Täter*innen erfragen persönliche Daten (z.B. Personalausweisnummer, Kontodaten…) und Auskünfte über finanzielle Verhältnisse der Betroffenen. Zum Beispiel, dass die Personalien des Angerufenen i.Z.m. einer Straftat genutzt worden seien.

Ein Abgleich der personenbezogenen Daten sei für die Aufklärungsarbeit der Polizeibehörden erforderlich, da es im Internet z.B. zu einem Identitätsdiebstahl oder Missbrauch von Bankdaten gekommen sei.

Durch die Behauptung, man mache sich selbst strafbar und es drohe eine hohe Haftstrafe, wenn man die erbetene Unterstützung ablehne und seine persönlichen Daten nicht zum Abgleich preisgebe, üben die Täter*innen massiv Druck auf die Angerufenen aus…In einigen Fällen stimmte sogar die Anrufnummer mit einer echten Rufnummer von Europol überein (s. Links zum Thema Manipulation).

Die erbetene Unterstützungsarbeit sieht letztlich so aus, dass Geldbeträge zu überweisen (auf ein ausländisches Konto, vielfach Thailand), Guthabenkarten zu kaufen (bis zur Erreichung des Tageslimits einer Bankkarte) und den Anrufer*innen die wertvollen Codes der Guthabenkarten durchzugeben sind. So könne das Geld der Betroffenen „in Sicherheit“ gebracht werden.

Der Fernzugriff auf Ihren Computer

In Einzelfällen kam es bei einigen Vorfällen auch zum Zugriff der Betrüger*innen auf Computer der Geschädigten.
Damit das möglich wird, müssen die Betroffenen dies aktiv erlauben. Wie geht das vor sich?
Die Angerufenen wurden in den Telefonaten aufgefordert einen Zugriff auf den eigenen Computer zu erlauben. Dazu wurden die Betroffenen telefonisch angeleitet, was am Computer zu tun ist. Die Täter*innen leiten sie an, selbst eine sog. Fernwartungssoftware (auch Remote Service oder Remote Administration - z.B. AnyDesk, TeamViewer, Chrome Remote) auf ihren Computern zu installieren. Nach erfolgreicher Installation müssen die Betroffenen nur noch per Mausklick den Zugriff „aus der Ferne“ erlauben und schon haben die Betrüger*innen freien Zugriff auf den Computer des Angerufenen.
Die Betroffenen sehen nun auf ihrem Bildschirm wie „ferngesteuert“ und wie von fremder Hand Aktionen auf dem Computer erfolgen. Was aber tatsächlich geschieht, hat der Betroffene nicht mehr unter Kontrolle: Es können nun private Daten kopiert, auf das Online-Banking zugegriffen und ggf. Konten manipuliert, Schadsoftware aufgespielt oder der Computer gesperrt werden. In diesem Augenblick oder später! Die Täter*innen können ab jetzt von Ihrem Computer aus Straftaten begehen und dafür Ihre Identität nutzen…

Verhaltenstipps:

- Erhalten Sie solche Anrufe, bewahren Sie bitte Ruhe. Lassen Sie sich nicht unter zeitlichen oder emotionalen Druck setzen und zu irgendeinem Handeln drängen!
- Geben Sie fremden Personen über Ihre Personaldaten oder Ihre Vermögens-verhältnisse keine Auskünfte.
- Legen Sie auf!
- Überweisen Sie niemals Geld.
- Weder Polizei, noch Europol bitten um Überweisungen oder den Kauf von Guthabenkarten. Europol hat keinerlei Befugnis, Bußgelder zu verhängen. Folgen Sie keinesfalls den Aufforderungen der Anrufer*innen!
- Bedenken Sie bei Anrufen: Auch (angebliche) Staatsanwälte, Richter oder Polizeibeamte (örtliche Polizei, LKA, BKA, Europol, Interpol), selbst wenn Ihnen diese noch so vertrauenswürdig erscheinen, sind für Sie grundsätzlich Fremde.
- Gewähren Sie niemals einer fremden Person Fernzugriff auf ihren Computer. Ohne Ihr eigeninitiatives Zutun bzw. Ihren Auftrag werden sich weder Polizei noch ein Computer-Support (Apple, Microsoft, Google,…) bei Ihnen melden und einen Zugriff verlangen!
- Bereiten Sie sich gedanklich schon heute auf solche Anrufe vor – spielen Sie sie für sich durch.
- Und zuletzt: Denken Sie bitte daran, dass auch immer Gemengelagen dargestellter oder Ihnen bereits bekannter Tatabläufe vorkommen können. Rechnen Sie bitte auch mit Varianten bisher bekannter Tatabläufe.

Wenn Sie bereits Opfer geworden sind:

- Erstatten Sie immer eine Strafanzeige. Nur so erhält die Polizei Kenntnis von der Straftat und kann die Täterinnen oder Täter verfolgen.
- Außerdem erhält sie dadurch Informationen zum Ausmaß dieses Deliktsfelds, kann Zusammenhänge herstellen und ggf. Tatserien erkennen. Eine Strafanzeige können Sie persönlich auf der nächst-gelegenen Polizeidienststelle oder online unter polizei.nrw/ erstatten.
- Leisten Sie auf keinen Fall weitere Geldzahlungen.
- Informieren Sie umgehend Ihr kontoführendes Geldinstitut, um eventuell ggf. getätigte Geldflüsse noch anzuhalten oder rückgängig zu machen.

Weiterführende Informationen:

polizei-beratung.de

Bei weiteren Fragen wenden Sie sich an unser Kriminalkommissariat Kriminalprä-vention und Opferschutz (KK KP/O)

bonn.polizei.nrw

Polizeipräsidium Bonn
Direktion K – KK KP/O
Königswinterer Straße 500, 53227 Bonn
Telefon +49 228-15-7617 oder -7676
KKKPO.Bonn@polizei.nrw.de