

Polizei warnt vor neuer Internet-Betrugsmasche - Stadt und Kreis Offenbach und Main-Kinzig-Kreis

(jmr) Vor einer neuen Betrugsmasche, mit der sich aktuell die Internetermittler im Polizeipräsidium Südothessen beschäftigen müssen, warnt derzeit die Polizei die Nutzer von sozialen Netzwerken wie Facebook und Co.

Bislang liegen allein der hiesigen Kripo mehr als ein Dutzend Anzeigen von betrogenen Nutzern der Internetplattform Facebook vor. Rainer Lechtenböher, Chef des Internetkommissariates ZK 50 beim Polizeipräsidium Südothessen, weiß aber, dass inzwischen bundesweit insbesondere Menschen türkischer Herkunft von der neuen Betrugsmasche betroffen sind.

Die Betrüger, so Lechtenböher, übernehmen die Identität von Facebook-Mitgliedern mit türkischen Namen und schreiben über den Facebook-Chat sämtliche "Freunde" mit türkischen Namen an. Sie bitten unter einem Vorwand um die Übermittlung der Mobilfunknummer. Gibt der "Freund" seine Nummer preis, erhält er - wie zuvor angekündigt - kurz darauf eine SMS von den Online-Bezahldiensten "ZONG" oder "BAKU" mit einem Zahlencode. Den so erhaltenen Code gibt der Geschädigte dann wieder über den Facebook-Chat an den vermeintlichen "Freund" weiter. Was der Geschädigte nicht ahnt: Dadurch wird ein Zahlungsvorgang bestätigt und über den Mobilfunkanbieter das Kundenkonto belastet. Meist handelt es sich um Geldbeträge zwischen 20 und 50 Euro, über die dann die Betrüger durch die Übermittlung des Codes für Internetgeschäfte verfügen können, weiß Lechtenböher. Die Zahlungen werden dem Empfänger - der in der Regel im Ausland sitzt - sofort gutgeschrieben. Eine spätere Rückbuchung des Betrages gestaltet sich oftmals schwierig bzw. ist nahezu unmöglich.

Nach bisherigen Erkenntnissen handelt es sich um ein bundesweit auftretendes Phänomen, wobei die Täter jeweils in der Landessprache des Opfers kommunizieren, um deren Glaubwürdigkeit zu erhöhen.

Polis yeni bir internet dolandırıcılığına/hilekarlığına karşı uyarıyor! - Stadt ve Kreis Offenbach ve Main-Kinzig-Kreis

(jmr) Güneydoğu Hessen Emniyet Müdürlüğü (Polizeipräsidium Südothessen) internet dedektiflerini aktüel „Facebook“ gibi Sosyal medya üzerinden yapılan yeni bir dolandırıcılık serisi meşgul ediyor.

Şu ana kadar internet veritabanı (platformu) „Facebook“ kullanıcısı ve dolandırıcılık mağduru bir düzine vatandaş teşkilatımız kriminal dairesine suç duyurusunda bulunmuştur.

Rainer Lechtenböher, Güneydoğu Hessen Emniyet Müdürlüğü Internetkomiserliği ZK 50 müdürü özellikle Türk kökenli vatandaşlarımızın tüm Almanya genelinde bu yeni dolandırıcılık sisteminin mağduru olduğunu belirtti.

Lechtenböher, dolandırıcıların türk/çe isimli Facebook-üyelerinin (identitelerini) kayıtlarını kopyalayarak türk/çe isimli Facebook-Chat „arkadaşlarıyla“ o şahıs adına yazıyorlar.

Onlara herhangi bir uydurma neden göstererek onlardan cep telefonu numaralarını vermeleri rica ediliyor. Numarasını veren „arkadaş“ - önceden kendisine belirtildiği gibi - Online Ödeme Servisi „ZONG“ yada „BAKU“ dan SMS-Mesajı ile bir ödeme kodu almakta. Mağdur şahıs kendisine gönderilen bu kodu Facebook-Chat üzerinden dolandırıcıya, yani sahte „arkadaş“ gönderiyor.

Mağdurun anlamadığı şey: bu kodla birlikte mağdurun cep telefonu üzerinden ödeme yapılmakta ve bu ödeme cep telefonu müşteri hesabından kesilmekte. Lechtenböher genellikle dolandırıcılar tarafından bu kodla 20 ve 50 Euro arasında ödeme yapılmakta olduğunu ve bu paranın internet üzerinden yapılan alışverişlerde kullanılmakta olduğunu belirtiyor. Bu ödemeler – genellikle yurt dışında yaşayan- alıcıların hesabına anında geçmektedir. Bu ödemelerin sonradan geri çekilmesi çok zor ve hatta imkansız hale gelmektedir. Tespitlere göre tüm Almanya’da ortaya çıkan bu fenomende dolandırıcılar kurbanlarıyla onların güvenini kazanmak için onlarla kendi ana dillerinde konuşmaktalar.

Markus Wortmann, Präventionsberater für Internet im Offenbacher Polizeiladen warnt davor, über Chats in sozialen Netzwerken persönliche Daten - insbesondere die eigene Mobilfunkrufnummer - weiterzugeben:

Wortmann rät:

- Behandeln Sie Ihre Daten stets vertraulich und geben Sie nicht mehr als notwendig von sich Preis.
- Streng vertraulich sollten Ihre Adresse, Bankverbindung oder Rufnummer von Ihnen und Ihren Familienangehörigen sein, auch wenn ein sogenannter "Freund" aus einem sozialen Netzwerk Sie danach fragt. Kommunizieren Sie in diesen Fällen lieber persönlich. Vergewissern Sie sich im Zweifel telefonisch, dass der Freund authentisch ist.
- Reagieren Sie mit Argwohn, wenn Sie ungewollt Nachrichten von unbekanntem Absender oder Firmen erhalten.
- Bestätigen Sie die erwähnten ZONG/BAKU-SMS nicht, es sei denn, Sie haben diese persönlich und wissentlich initiiert, um ein Geschäft abzuschließen oder einen Kauf zu tätigen.
- Sollten Sie eine SMS dieser Art erhalten haben, so nehmen Sie persönlich mit dem Facebook-Freund Kontakt auf und informieren Sie ihn darüber, dass sein Account möglicherweise manipuliert wurde.
- Wenn Sie selbst Opfer durch eine derartige Straftat geworden sind, sollten Sie Ihren Mobilfunk-Vertrag schnellstmöglich dahingehend ändern, dass derartige Abbuchungen nicht mehr möglich sind und wenden Sie sich umgehend an die Polizei.

Markus Wortmann, Emniet teşkilatı internet önleyici tedbirler danışmanı (Polizeiladen Offenbach – Kriminal Teknik Danışma Servisi) kullanıcılara sosyal medya bağlantılarında şahsi bilgilerini ve özellikle cep telefonu numaralarını vermemelerini tavsiye ediyor.

Wortmann'ın tavsiyeleri:

- Şahsi bilgilerinizi her zaman bilinçli ve dikkatli kullanınız. Şahsınızla ilgili gereğinden fazla bilgi vermeyiniz.
- Adresiniz, banka bağlantılarınız, sizin ve aile fertlerinizin telefon numaraları hususunda çok muhafazakar olunuz. Eğer sosyal medya üzerinden sizinle irtibat kuran „arkadaş“ olsa bile, kendisiyle internet üzerinden değil, şahsen irtibat kurunuz. Şüpheli durumlarda kendisiyle telefonla irtibata geçerek onun gerçekten arkadaşınız olduğu konusunda emin olunuz.
- Tanımadığınız şahıs ve firmalardan istenmeyen/beklenmeyen bir mesaj alırsanız, buna çok ihtiyatlı bakınız.
- Siz kendiniz bilinçli olarak şahsen ticari yada alışveriş amaçlı işlem yapmadysanız bahsedilen ZONG ve BAKU SMS-Mesajlarını onaylamayınız.
- Belirtilenlere benzer bir SMS-mesajı alırsanız Facebook-arkadaşınızla şahsen irtibata geçerek bilgilerinin (Account) manipule edilmiş/ oynanmış olabileceğini bildiriniz.
- Eğer benzeri bir hilenin kurbanı olduysanız, cep telefonu sözleşmenizi bu gibi ödemelerin olmaması için değiştiriniz ve polise başvurunuz.