PRÄVENTION VERBINDET.

SONDER-TRENDLETTER

– polizeiinterne Informationen –

Ausgabe 02-2011

Betrug im Internet

Liebe Kolleginnen,
liebe Kollegen,

das Internet gehört für viele Mitmenschen zum Alltag, ob im Beruf oder zu Hause. Einkaufen, Bankgeschäfte erledigen oder den Urlaub buchen – das Internet bietet dem Nutzer viele Möglichkeiten. Von den Vorteilen des Internets profitieren aber auch Kriminelle: Sie nutzen jede Schwachstelle für ihre Machenschaften.

Einige der Vorgehensweisen der Betrüger haben wir in diesem Trendletter zu Ihrer Information und insbesondere zur Weitergabe an Bürgerinnen und Bürger zusammengestellt. Der aktuelle Anlass dazu ist der Beginn des ***Online-Ticketverkaufs für die Olympischen Sommerspiele in London 2012.*** *Trotz Warnungen werden viele sportbegeisterte Opfer von Betrügern, die ihnen im Internet Karten für das Sportereignis anpreisen – stattdessen aber nur das Geld aus der Tasche ziehen. In diesem Sonder-Trendletter haben wir in Zusammenarbeit mit dem BKA Informationen für Sie zusammengestellt, die Sie bei Ihrer täglichen Arbeit unterstützen können.*

Ihr
Andreas Mayer

Ihr
Harald Schmidt

PRÄVENTION VERBINDET.

SONDER-TRENDLETTER

– polizeiinterne Informationen –

Ausgabe 02-2011

Betrug im Internet

1. Betrug beim Online-Kauf von Eintrittskarten

Seit einigen Wochen läuft der **Ticketverkauf für die 30. Olympischen Sommerspiele 2012 in London:** 6,6 Millionen der insgesamt 8,8 Millionen Tickets können von Sportbegeisterten aus aller Welt erstanden werden. Mit dem Beginn des Ticketverkaufs sind auch Betrugshandlungen in diesem Zusammenhang zu erwarten. Die britischen Behörden haben hierzu auf den Missbrauch von Personendaten hingewiesen. In Anbetracht des möglichen Schwarzmarktes werden alle Interessenten darauf hingewiesen, dass Tickets nur dann einen Platz in den Sportstätten garantieren, wenn sie über **offizielle Stellen** erworben werden. Nachfolgend einige Empfehlungen für den Ticketkauf und die Buchung von Pauschalreisen zur Weitergabe an Interessierte.

Hinweis: Der Verkauf für die Olympischen Sommerspiele endet am 26. April 2011. Die Karten für die Paralympischen Spiele werden ab dem 09. September veräußert.

1.1 Informationen zum Kauf von Eintrittskarten

Eintrittskarten zu den Olympischen Spielen (und auch zu anderen größeren Sportveranstaltungen) sollten **immer bei offiziellen Internetseiten** bestellt werden. Nur dort erhalten Interessierte auch garantiert die gewünschte Eintrittskarte – und werden nicht Opfer von Betrügereien. Wer Tickets bei nicht offiziellen Stellen (Internetseiten, Geschäften oder Personen) bezieht, kann schnell Opfer einer Straftat werden. Betrüger handeln oft mit Karten, die schlicht gar nicht existieren oder spähen die Kreditkartendaten der Käufer aus. Die Opfer haben dann nicht nur den finanziellen Schaden, sondern erhalten auch keinen Zutritt zu den Olympischen Spielen.

■ Für die **Olympischen Sommerspiele in London** können Tickets offiziell erworben werden unter: **www.tickets.london2012.com**

■ Eine weitere sichere Quelle für Tickets ist die Internetseite des **Deutschen Olympischen Sportbundes** unter: **www.dosb.de/de/olympia/olympische-spiele/**

■ Die autorisierte Verkaufsagentur für Deutschland ist der **Reiseveranstalter Dertour**. Auf dessen Internetseite können Tickets für die Olympischen Spiele 2012 in London gebucht werden: **www.dertour.de/portal/dertour/app/content/resourceId/olympia-2012-london.html**

Hinweis: Nicht benötigte Tickets können durch die autorisierten Verkaufsagenturen rückerstattet und über **www.tickets.london2012.com** weiterverkauft werden. Auf keiner dieser Seiten ist bei der Bezahlung die zusätzliche Eingabe von persönlichen PIN- und TAN-Nummern des für die Bezahlung verwendeten Bankkontos erforderlich. Sollten Sie auf einer dieser Seiten dazu aufgefordert werden, brechen Sie den Vorgang ab und versuchen Sie sich erneut über die offizielle Internetseite einzulocken.

Linktipp: http://www.met.police.uk/olympic_and_paralympic_games_policing/op_podium.htm

1.2 Informationen über Pauschalreiseangebote

Nicht im Vereinigten Königreich und bestimmten europäischen Ländern wohnhafte Personen können Pauschalreisen zu den Olympischen Spielen auch bei den jeweiligen **Nationalen Olympischen Komitees und autorisierten Ticket-Resellern** beziehen.

Pauschalreiseangebote (Games Breaks und Hospitality Packages) können bei den folgenden drei offiziellen Anbietern gebucht werden:

- **Thomas Cook:**
  www.thomascooklondon2012.com
- **Prestige Travel:**
  www.prestigeticketing.london2012.com
- **Jet Set Travel:**
  www.jetsetsports.com

Die autorisierte **Verkaufsagentur für Deutschland** ist **www.dertour.de/portal/dertour/app/content/resourceId/olympia-2012-london.html**

Hinweis: Vor der Buchung sollte sich jeder Interessierte mit den allgemeinen Geschäftsbedingungen vertraut machen.

2. Vorauszahlungsbetrug

Die Machenschaften der Betrüger sind vielfältig. Im Folgenden stellen wir Ihnen einige Beispiele vor, die Sie auch in ausführlicher Form auf unserer Internetseite **www.polizei-beratung.de** finden können.

2.1 Romance-Scamming: Betrug mit vorgetäuschter Liebe

Besonders perfide und für die Opfer mit hohem emotionalem Stress verbunden ist das **Love- oder Romance-Scamming.** In Online-Partnerbörsen oder auch in sozialen Netzwerken sind die Scammer auf der Suche nach potenziellen Opfern. Ist ein Kontakt erst einmal hergestellt, werden diese mit Liebesbekundungen und Aufmerksamkeit überhäuft - allein mit dem Ziel, ihnen das Geld aus der Tasche zu ziehen. Die virtuellen Partner geben z. B. vor, bei einer Geschäftsreise nach Westafrika in Geldnot geraten zu sein. Oder sie benötigen Geld für eine wichtige Operation ihres Kindes oder eines Angehörigen. Auch gestohlene Koffer und Pässe, unbezahlter Lohn oder eine unbezahlte Hotelrechnung sollen das ahnungslose Opfer dazu bringen, Geld zu überweisen. Und viele tun es auch, schließlich sind sie zu diesem Zeitpunkt schon von ihrem Internet-Partner/ihrer Internet-Partnerin emotional abhängig.

Informationen:
http://www.polizei-beratung.de/themen-und-tipps/betrug/scamming/romance-scamming.html

PRÄVENTION VERBINDET.

SONDER-TRENDLETTER

– polizeiinterne Informationen –

Ausgabe 02-2011 | Betrug im Internet

2.2 Betrug mit falschen Geld- oder Gewinnversprechen

Zu einem der ältesten Tricks der Nigeria Connection gehören **E-Mails (vormals Briefe oder Faxe), die dem Empfänger eine Menge Geld versprechen – aus einer Erbschaft oder einem Familienschatz beispielsweise.** Um an das gewünschte Geld zu kommen, werden allerdings zunächst viele Tausend Euro für Gebühren, Notarkosten oder Steuern fällig. Wenn das Opfer zahlt, brechen die Betrüger den Kontakt ab – das gezahlte Geld ist unwiederbringlich verloren. Eine weitere Betrugsmasche sind Gewinnbenachrichtigungen und überraschende Lotteriegewinne. Dabei werden Personen hohe Gewinnversprechen (beim Besuch einer Internetseite oder über schriftliche Anschreiben) in Aussicht gestellt. Um an den Gewinn zu kommen, muss der vermeintlich glückliche Gewinner zunächst noch Gebühren, Anzahlungen u. Ä. zumeist in Höhe von einigen Hundert bis Tausend Euro entrichten. Dieses Geld verschwindet in dunklen Kanälen – einen Gewinn sieht das Opfer nie.

2.3 Betrug mit Wohnungsangeboten

Eine tolle **Wohnung zu einem Schnäppchenpreis** ist ein Angebot, das zu gut ist, um wahr zu sein. Gerade bei Immobilienbörsen im Internet können Wohnungssuchende auf Betrüger hereinfallen. Die Masche läuft fast immer gleich ab: Die Betrüger geben sich als Engländer oder Amerikaner aus, die die zu vermietende Wohnung geerbt hätten. Oder sie erzählen, sie hätten mal in Deutschland gearbeitet und wollten die alte Bleibe nach einem beruflich bedingten Wechsel ins Ausland vermieten. Nach einer Vorauszahlung der ersten Miete und der Kaution per Bargeldtransfer beispielsweise mit Western Union sollten dem neuen Mieter die Schlüssel über einen Paketdienst oder eine Agentur geschickt werden. Bei Nichtgefallen könne das Geld ja später wieder erstattet werden. Doch das Geld sehen die Opfer nie wieder, und auch die Wohnung existiert oft gar nicht oder gehört einem anderen Eigentümer, der vom Betrug selbst nichts mitbekommt.

2.4 Betrug mit dem Traumjob

Auch unter den **Stellenanzeigen in Tageszeitungen** suchen Betrüger nach möglichen Opfern. Es ist der Traumjob bei hervorragender Bezahlung, der viele zum Telefonhörer greifen lässt – eine Telefonnummer ist meistens die einzige angegebene Kontaktmöglichkeit. Nach dem ersten Anruf sollen die Opfer Bewerbung und Lebenslauf faxen. Und nach einem telefonischen Vorstellungsgespräch hat man den vermeintlichen Job schon in der Tasche. Es müssen nur noch einige Hundert Euro für Uniform oder Arbeitsschuhe oder Begleichung der Gebühren für angeblich behördlich geforderte Zulassungen an den neuen Arbeitgeber überwiesen werden. Kaum ist das Geld transferiert, löst sich der Arbeitgeber in Luft auf.

Zu beachten ist auch, dass seriöse Arbeitgeber niemals eine Kontaktaufnahme über mit überhöhten Gesprächsgebühren belegte Telefonnummern voraussetzen.

2.5 Betrug mit gefälschten Schecks

In Anzeigen in Zeitungen und im Internet suchen die Betrüger Menschen, denen sie ihre **gefälschten Schecks** auf scheinbar legalem Wege andrehen können: Sie tätigen damit beispielsweise einen Kauf bei Privatpersonen. Meistens sind die Schecks auf einen höheren Betrag ausgestellt, als zum Beispiel das privat angebotene Auto tatsächlich gekostet hat. Es wird vereinbart, dass das Opfer den Differenzbetrag gleichzeitig vom eigenen Konto per Bargeldtransfer an den Betrüger überweist. Problem ist, dass selbst Bankangestellte einen gefälschten Scheck nur selten erkennen. Das Opfer hat in zweifacher Hinsicht das Nachsehen. Dass der Scheck gefälscht war, stellt sich erst in einigen Tagen heraus, dann ist das überwiesene Geld bereits in undurchsichtigen Kanälen verschwunden. Außerdem kann die Bank wegen Betrug strafrechtliche Schritte gegen das Opfer einleiten.
Link: http://www.sicherer-autokauf.de/

Informationen zu Scamming: http://www.polizei-beratung.de/themen-und-tipps/betrug/scamming.html

3. Phishing

Das sogenannte **Phishing tritt insbesondere im Bereich des Online-Bankings** in Erscheinung.
Der Trick: In betrügerischer Absicht werden Bankkunden mit täuschend echt aufgemachten E-Mails dazu veranlasst, über einen Link vermeintliche Internet-Seiten von Banken aufzurufen. Dort sollen dann persönliche Daten wie Zugangsdaten, Passwörter oder ähnliches eingeben werden – angeblich aus Sicherheitsgründen, zur Bestätigung oder um, wie es oft heißt, Datenabgleiche auszuführen. Tatsächlich landen die Kunden aber keinesfalls auf echten Bank-, sondern vielmehr auf gefälschten Internet-Seiten. Manchmal wird als Variante dieser betrügerischen Tour vor der eigentlichen Internet-Seite der Bank ein Pop-Up geöffnet, das zur Eingabe der Daten auffordert. Mit diesen persönlichen Daten können Betrüger Missbrauch betreiben („Identity Theft" = Übernahme einer fremden Identität) und mit der vorgegaukelten Identität im Namen des Geschädigten online nahezu alle Geschäfte abwickeln (Geld überweisen, Dispokredit ausschöpfen, Online-Einkäufe tätigen etc.).

Informationen: http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing.html

4. Gratisdienste

Was früher Dialer waren, sind heute vermeintliche Gratisdienste: **Internetdienste, die sich als gratis tarnen und dann als kostenpflichtig darstellen.** Diese Dienste werden inzwischen für nahezu alle Kategorien angeboten.
Die Offerten reichen von vermeintlich kostenfreien Bildern über SMS-Dienste bis hin zu Gedichte- und Witzedownloads. Die Angebote sollten vor dem Herunterladen oder einer Registrierung genau angeschaut werden. Besonders achten sollte man auf die AGBs (Allgemeine Geschäftsbedingungen).
Wer dennoch auf ein unseriöses Angebot hereingefallen ist, kann gegen eine unberechtigte Forderung Widerspruch einlegen. Entsprechende Musterschreiben finden sich über die Suchmaschine im Internet. Mahnungen oder Drohungen durch ein Inkassobüro sollten niemanden aus der Ruhe bringen. Gegebenenfalls sollte man sich an einen Rechtsbeistand wenden.

PRÄVENTION VERBINDET.

SONDER-TRENDLETTER

– polizeiinterne Informationen –

Ausgabe 02-2011

Betrug im Internet

5. Finanzagenten und Warenagenten

Immer mehr Bürgerinnen und Bürger fallen auf dubiose Stellenangebote herein, ohne sich der Folgen dieser scheinbar harmlosen Betätigung bewusst zu sein. Im Jahr 2009 wurden bundes weit 2.394 Verdachtsanzeigen wegen Geldwäsche registriert, weil sich Kontoinhaber als **„Finanzagenten“** für Kriminelle betätigt haben. 2008 wurden noch 971 Fälle gemeldet. In Jobbörsen und auf anderen Internetseiten oder auch in E-Mails geben sich Betrüger beispielsweise als Vertreter seriöser „Finanzmanagementunternehmen“ aus, die im Auftrag ihrer Firma nach „Finanzagenten“, „Finanzmanagern“ oder „Regional Managern für Zahlungsbearbeitung“ suchen. Ihr Ziel sind ahnungslose Kontoinhaber, die das eigene Girokonto für Überweisungen zur Verfügung stellen sollen. Der geworbene „Finanzagent“ soll die zunächst auf sein Konto überwiesenen Beträge umgehend per Bargeldversand (z. B. als Western Union-Geldtransfer) an eine Person im Ausland weiterleiten. Alternativ werden die Überweisungen auch direkt von einem Betrüger selbst durchgeführt, der das Konto des „Finanzagenten“ „angemietet“ hat und dem PIN und TAN zur Verfügung gestellt wurden. Als Belohnung darf eine Provision zwischen fünf und 20 Prozent des Überweisungsbetrags einbehalten werden. Später wird die Buchung auf das Konto des „Finanzagenten“ storniert und dieser bleibt auf dem Fehlbetrag und damit dem Schaden sitzen.

Viele „Finanzagenten“ sind sich nicht bewusst, dass sie im Auftrag von Kriminellen arbeiten. Denn die zunächst auf das Konto des „Finanzagenten“ überwiesenen Gelder stammen nahezu ausnahmslos von Personen, die selbst Opfer von sogenannten Phishing-Aktionen oder von betrügerischen Internet-Auktionen geworden sind. Leitet der „Finanzagent“ diese Geldbeträge weiter, drohen ihm statt eines lukrativen Nebenverdienstes eine Anzeige wegen leichtfertiger Geldwäsche und somit strafrechtliche Konsequenzen wie Geld- oder Freiheitsstrafe. Da „Finanzagenten“ für ihre Tätigkeit eine Provision erhalten, betreiben sie oft unbewusst gewerbsmäßig ein Finanztransfergeschäft. Dieses bedarf jedoch einer Erlaubnis durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Liegt eine solche nicht vor, kann die BaFin ein Verwaltungsverfahren einleiten.

Mit der gleichen Masche werden zwischenzeitlich auch Jobs als **„Warenagent“** angeboten. Hierbei ist angeblich lediglich die Übernahme von Paket- und Warensendungen an der eigenen (Privat-)Adresse notwendig. Diese Waren müssen dann in neue Pakete umgepackt oder nur mit neuen Adressaufklebern versehen werden, um sie an ausländische Adressen weiterzuversenden. Tatsächlich handelt es sich bei diesen Warensendungen regelmäßig um auf betrügerische Weise erlangte, meist hochwertige Produkte. Die „Warenagenten“ werden in diesen Fällen regelmäßig als Mittäter einer Straftat zur Verantwortung gezogen.

Informationen:
http://www.polizei-beratung.de/themen-und-tipps/betrug/finanzagenten.html

Informationen und Kampagnen der Polizei

Medien:

- **Infoblatt „Gewinnbenachrichtigung“**
  (Bezugsquelle: Medienportal des ProPK)

- **Infoblatt „Offertenschwindel“**
  (Bezugsquelle: Medienportal des ProPK)
- **Infoblatt „Vorauszahlungsbetrug / Nigeria-Briefe“**
- **Faltblatt „Vorsicht! Karten-Tricks!“**
  (Bezugsquelle: Medienportal des ProPK)

Hinweis: Alle Medien sind auch als Download verfügbar unter **http://www.polizei-beratung.de/medienangebot.html**

Links:

- **www.kaufenmitverstand.de**
- **Aktion „Sicher mit Karte unterwegs“ unter: http://www.polizei-beratung.de/themen-und-tipps/betrug/ec-und-kreditkartenbetrug/sicher-mit-karte-unterwegs.html**
- **www.sicherer-autokauf.de**

Hinweise zum Trendletter

Der Trendletter ist ein polizeiinternes Medium, herausgegeben von der Polizeilichen Kriminalprävention der Länder und des Bundes. Der Trendletter sollte in vollständigem Umfang an nachgeordnete Bereiche gesteuert werden. Dies kann in Form einer E-Mail oder eines Ausdrucks geschehen. Die darin enthaltenen Informationen richten sich ausschließlich an Polizeibeschäftigte. Der Trendletter ist nicht für eine externe Verbreitung vorgesehen.