

das Bundeskriminalamt (BKA) warnt: Betrüger nutzen Sie als "Warenagenten" aus

Mit einem verlockenden Angebot per E-Mail versuchen Betrüger Sie als Komplizen zu gewinnen. Allerdings ist das für Sie natürlich nicht ersichtlich. Das Bundeskriminalamt (BKA) warnt deshalb nun auf seiner Internetseite vor einem lukrativen Jobangebot. Sie sollen dabei Pakete für die Kriminellen entgegennehmen und an diese weiterleiten, damit sie anonym bleiben.

Sie machen sich dadurch allerdings zum Mittäter, da Sie die Betrüger dabei unterstützen, ihre kriminellen Geschäfte zu tarnen. Antworten Sie daher nicht auf E-Mails, die Ihnen für eine solche Leistung als Nebenverdienst Geld anbieten. Die Jobbezeichnung in den aktuellen E-Mails lautet "Warenagent". Es ist allerdings davon auszugehen, dass die E-Mails nach der öffentlichen Warnung von den Betrügern verändert werden.

<http://www.bundeskriminalamt.de/pressemitteilungen/2008/pm081124.html>

die Meldung vom 24.11.2008

Im Bereich der Internetkriminalität setzen die Täter nicht nur immer professionellere Schadsoftware ein, sondern entwickeln auch ständig neue Methoden. Das Bundeskriminalamt (BKA) warnt vor einer neuen Tatbegehungsweise: Dabei versuchen die Täter mit Hilfe von ungezielt gestreuten Spam-Mails so genannte „Warenagenten“ anzuwerben. Sie versenden dazu Job-Angebote mit folgendem oder ähnlichem Inhalt:

*Betreff: 7858 pro Monat ist vorstellbar
Anlieferer gesucht!!!
Auch fuer Fruehrentner geeignet! Ein Fahrzeug
kann gestellt werden.
Bewerbung bitte an xxx“*

Die so angeworbenen „Warenagenten“ haben dann die Aufgabe, Pakete entgegenzunehmen und diese gemäß den Vorgaben der Täter weiter zu leiten. Der Verdienst wird auf Provisionsbasis in Aussicht gestellt – angeblich 30 Euro pro weiter geleitetem Paket. Darüber hinaus sollen Versand- und Benzinkosten erstattet werden. Um das Arbeitsangebot seriös erscheinen zu lassen, übersenden die Täter nach Kontaktaufnahme echt wirkende Arbeitsverträge, z. B. aus dem Bereich der Kurier- oder Paketdienstleistungsbranche.

Die Täter gehen bei diesem „Geschäftsmodell“ neue Wege, um anonym zu bleiben und illegal Kundenkon-

ten von Online-Auktionshäusern zu übernehmen mit dem Ziel, über diese Accounts hochpreisige Waren zu ersteigern. Diese werden nach Änderung der Empfängeradresse im Konto des Online-Auktionshauses vom ahnungslosen Verkäufer an die zuvor angeworbenen „Warenagenten“ verschickt. Die Bezahlung der Ware erfolgt durch die Täter. Die Gelder wurden zuvor illegal von Online-Bankkonten abgephisht. Die „Warenagenten“ haben in der Folge die Aufgabe, die widerrechtlich erlangten Waren an vorgegebene Adressen weiterzuleiten oder an Packstationen eines deutschen Postdienstleisters zu versenden.

Durch den Einsatz der angeworbenen „Warenagenten“ gelangen die Täter anonym an die rechtswidrig erlangte Ware. Personen die sich auf die falschen Job-Angebote einlassen und die widerrechtlich erlangten Waren weiterleiten, können sich strafbar machen und müssen darüber hinaus mit zivilrechtlichen Ansprüchen bei der Regulierung entstandener Schäden rechnen.

Das Bundeskriminalamt rät daher:

- Antworten Sie nicht auf E-Mails, die in der oben angegebenen Form an sie versandt werden.
- Lassen Sie sich nicht durch dubiose Jobangebote als „Warenagent“ anwerben.

die Meldung vom 20.10.2006
Die Pressestelle des Bundeskriminalamtes teilt mit:

Bundeskriminalamt warnt vor neuen Phishing-Tricks: Internetverkäufer, Firmen und Vermieter von Wohnungen werden zu Mittätern wider Willen

Das Bundeskriminalamt warnt vor neuen Tricks, mit denen im Internet agierende Betrüger unbescholtene Bürger ohne deren Wissen zu Mittätern machen. Im Rahmen vorgetäuschter legaler Geschäftsaktivitäten wird die Gutgläubigkeit der Betroffenen ausgenutzt, um Gelder, die von ausgespähten Onlinekonten abgezweigt wurden, ins Ausland zu verschieben.

In der Vergangenheit hatten interessierte Bürger auf per E-Mail übersandte Arbeitsangebote von Firmen mit schillernden Namen reagiert und sich um eine Anstellung als Finanzagent beworben. Die Aufgabe der Finanzagenten war, bestimmte Überweisungen unmittelbar nach Zahlungseingang in bar abzuheben. Die Gelder wurden anschließend über sogenannte "Minutendienstleister" wie zum Beispiel "Western Union" oder "Moneygram" ins Ausland weitergeleitet. Die Finanzagenten setzten sich damit der Gefahr aus, wegen Geldwäsche belangt zu werden und blieben vielfach auf dem entstandenen Schaden sitzen.

Aktuelle Entwicklungen belegen nun, dass die Täter mittlerweile zu alternativen Methoden greifen, um auch Personen - ohne ihr Wissen - als Finanzagenten zu missbrauchen.

Vorsicht bei privaten Kfz-Verkäufen:

Über Gebrauchtwagen-Internetportale wird aus dem Ausland per E-Mail Kontakt zu in der Regel privaten Verkäufern von Gebrauchtfahrzeugen aufgenommen. Nachdem man sich über den Kaufpreis geeinigt hat, wird eine kurzfristige Überweisung des Betrages vom Konto eines Freundes angekündigt. Tatsächlich erfolgt die Überweisung jedoch von einem zuvor mittels Phishing ausgespähtem Onlinekonto.

Nach Zahlungseingang beim Verkäufer treten die Täter per E-Mail unter einem Vorwand vom Kauf zurück. Der bereits überwiesene Kaufpreis wird, unter Abzug eines geringen Teilbetrages für die entstandenen Unannehmlichkeiten, zurückgefordert. Das Geld soll dabei jedoch ins Ausland transferiert werden. Der wenig später erfolgende Rückruf der Phishing-Überweisung trifft dann den nichts ahnenden Kfz-Verkäufer.

Firmen mit Internetvertriebsportalen betroffen:

Die Täter bestellen bei Firmen bzw. Gewerbetreibenden Waren im Wert von mehreren tausend Euro. Da es sich um die erste Geschäftsbeziehung handelt, wird der Rechnungsbetrag vorab überwiesen. Auch hier erfolgt die Überweisung von einem zuvor mittels Phishing ausgespähtem Onlinekonto. Unmittelbar nach Eingang der Überweisung beim Verkäufer wird

die Bestellung storniert bzw. auf einen Minimalbetrag reduziert. Unter einem Vorwand wird darum gebeten, das verbliebene Guthaben ins Ausland zu transferieren. Auf diese Weise leistet die Firma unbemerkt einen wesentlichen Tatbeitrag.

Vorsicht bei der Vermietung von Ferienwohnungen:

Auch Vermieter von Ferienwohnungen sollten auf der Hut sein. Aus dem Ausland wird per E-Mail Kontakt zu ihnen aufgenommen und die inserierte Wohnung unter Hinweis auf in Deutschland erfolgende Schulungen für einen längeren Zeitraum gebucht. Es wird vereinbart, den entsprechenden Betrag vorab zu überweisen. Auch hier erfolgt die Zahlung jedoch tatsächlich von einem zuvor mittels Phishing kompromittierten Onlinekonto. Wenig später wird die Buchung der Ferienwohnung unter Hinweis auf die kurzfristige Verlegung des Veranstaltungsortes ins Ausland storniert. Wiederum wird gebeten, das be-

reits überwiesene Geld an den neuen Veranstaltungsort zu überweisen. Der Vermieter darf dabei einen Teilbetrag zur Begleichung seiner entstandenen Kosten und Mietausfälle einbehalten.

Nach Einschätzung des BKA haben die Phishing-Täter mittlerweile Schwierigkeiten, eine angemessene Anzahl von Finanzagenten zu rekrutieren. Dies ist unter anderem auf die Berichterstattung in den Medien, die Warnhinweise von Polizei und Banken sowie der mittlerweile erfolgten Verurteilungen von Finanzagenten zurückzuführen.

Das BKA empfiehlt:

- ⇒ Prüfen Sie Angebote kritisch, bei denen Sie Ihr Konto zur Abwicklung von Zahlungen für Firmen oder Personen, insbesondere im Ausland, zur Verfügung stellen sollen.
- ⇒ Seien Sie argwöhnisch, wenn unerwartete Gutschriften auf Ihr Konto erfolgen und Sie kurze Zeit später um Rücküberweisung dieser Gelder gebeten werden. Nehmen Sie im Zweifelsfall Kontakt zu Ihrer örtlichen Polizei oder Bank auf.
- ⇒ Seien Sie vorsichtig, wenn über das Internet oder per Telefon vereinbarte Zahlungen vom Konto einer dritten Person oder Firma erfolgen. Nehmen Sie im Zweifelsfall Kontakt zu Ihrer Bank auf, um zu klären, ob die Überweisung mit dem Wissen des Kontoinhabers erfolgt ist.
- ⇒ Führen Sie etwaige Rückbuchungen nicht ohne Weiteres direkt ins Ausland, sondern nur auf das jeweilige Ursprungskonto der Buchung aus.

Phishing ist die illegale Erlangung von Kundendaten, um damit Gelder von den Kundenkonten abzuzweigen. Es ist durch die ständige Zunahme des Online-Verkehrs mit Banken eine lukrative Einnahmequelle für Straftäter geworden.

Weitere Informationen zum Thema Phishing finden Sie auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de) unter Abzocker und Spione / Passwort-Fischer, unter www.polizei-beratung.de sowie unter www.sparkasse.de und auf den Internetseiten der örtlichen Sparkassen.