



W H I T E P A P E R

# Betrugsversuche über Spam-E-Mails



Unter dem Begriff „Spam“ versteht man oft nur elektronische Briefe mit Reklamecharakter, doch das ist nicht ganz richtig. Einige Arten von Spam verfolgen ein anderes Ziel als nur für gefälschte Uhren und blaue Pillen zu werben. Zu den gefährlichsten Spielarten dieser Sorte von E-Mails gehören insbesondere betrügerische Briefe.

Mit Spam-Technologien lassen sich Nachrichten von falschen Absenderadressen und infizierten Computern völlig ahnungsloser Nutzer massenhaft versenden. Es verwundert daher nicht, dass dies Cyberkriminelle unterschiedlichen Kalibers anzieht. Mit den Spam-Verfahren können sie nicht nur Anwender betrügen, sondern auch die Spuren ihrer kriminellen Tätigkeit verwischen. Spam mit betrügerischem Inhalt wird auch deswegen so häufig verschickt, weil deren Absender aufgrund der anonym gesendeten E-Mails nicht leicht zu finden sind. Daher können die Cyberkriminellen auf Straffreiheit zählen. Verkäufer nachgemachter oder gefälschter Produkte nutzen die Dienste der Spammer ebenso wie Anbieter krimineller Dienste und Virenschreiber.

Cyberkriminelle verschicken diese Spam-Variante mit der Absicht, den Empfänger um Geld zu erleichtern oder an dessen vertrauliche Daten zu gelangen, um damit wiederum Geld zu verdienen.

### Phishing

Phishing zählt zu den gefährlichsten Varianten von betrügerischem Spam. Mithilfe von Phishing-E-Mails (engl. phishing von fishing = angeln) versuchen die Spammer, persönliche User-Daten zu stehlen und sie für ihren Profit zu verwenden. In Frage kommen beispielsweise Logins und Passwörter für Online-Zahlungssysteme oder Nummern und PIN-Codes von Kreditkarten. Nutzer von Internet-Banking und Web-Zahlungssystemen sind am häufigsten Opfer von Phishing-Attacken.

Phishing-E-Mails ahmen offizielle Mitteilungen seriöser Organisationen wie Banken, Finanzunternehmen oder Zahlungssystem-Anbieter nach. Derartige E-Mails enthalten in der Regel einen Link auf eine gefälschte Webseite. Dort soll der Nutzer unter einem bestimmten Vorwand seine persönlichen Daten eintragen, die so in die Hände der Betrüger gelangen. Damit das Opfer den Betrug nicht bemerkt, ist die Webseite der offiziellen Unternehmensseite täuschend echt nachempfunden. Auch die Absenderadresse ist gefälscht.

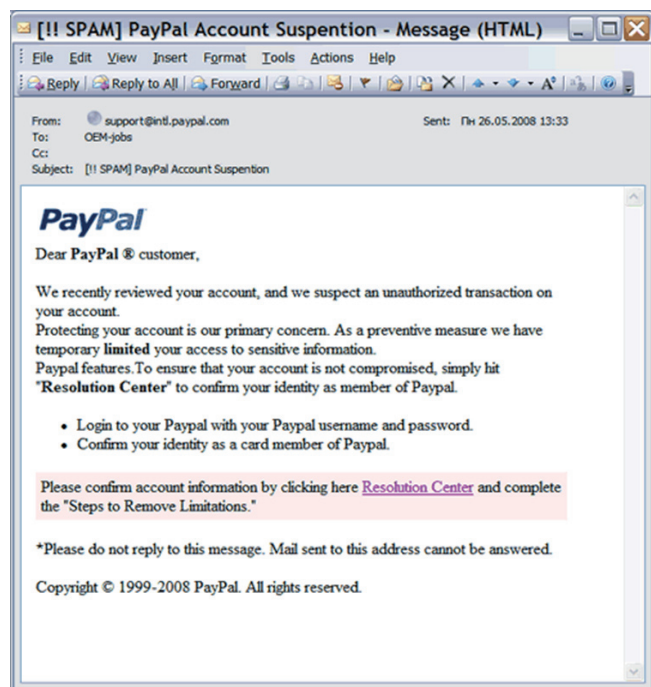
In einigen Fällen wird der Browser des Nutzers nach Eingabe und Absenden der Daten sogar auf die offizielle Webseite umgelenkt. Damit hat das Opfer praktisch keine Chance, Verdacht zu schöpfen.

Manchmal geraten Anwender nicht auf eine gefälschte Webseite, sondern auf eine mit Exploits infizierte Seite. Dabei wird eine Software-Schwachstelle ausgenutzt, um einen Trojaner auf dem Rechner des Anwenders zu

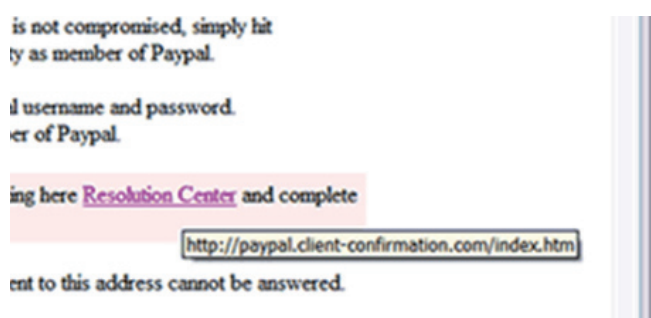
installieren. Dort sammelt der Schädling unterschiedlichste Informationen wie zum Beispiel Zugangscodes zu Konten und schickt diese an den Cyberkriminellen. Auf diese Art und Weise infizierte Rechner lassen sich zudem leicht einem Zombie-Netz hinzufügen, das für Cyberattacken oder zum Spam-Versand genutzt wird.

Um auch diejenigen Anwender zu täuschen, die sowohl den Webseiten-Aufbau als auch die Adresse genau überprüfen, tarnen Phisher die verwendeten URLs und versuchen, deren Bezeichnung so nahe wie möglich am Original zu halten. Die Phisher begannen anfangs damit, Domain-Namen auf kostenlosen Webhosts zu registrieren, die der Webseite einer anzugreifenden Organisation ähnelte. Mit der Zeit setzten sie jedoch immer ausgeklügeltere Methoden ein.

Als Beispiel für eine als offizielle Mitteilung getarnte Phishing-Mail dient folgende an Kunden von PayPal gerichtete Nachricht:



Nur wenn ein aufmerksamer Leser den Mauszeiger auf den in der E-Mail angegebenen Link bewegt, kann er erkennen, dass der Weblink in Wirklichkeit auf eine Phishing-Seite führt. Der Weblink ähnelt der Adresse der offiziellen Paypal-Webseite sehr stark. Doch die Domäne, an die der Nutzer gerät, ist eine völlig andere: client-confirmation.com.



Der Screenshot zeigt die in der E-Mail auftauchende falsche Adresse. Nur ein fortgeschrittener und extrem aufmerksamer Anwender ist hier in der Lage, die Fälschung anhand des Weblinks zu erkennen.

Natürlich existieren auch primitivere Betrugsversuche. Anwender erhalten beispielsweise im Namen einer Bank oder eines Zahlungsdienst-Anbieters Mitteilungen, in denen sie aufgefordert werden, ihre Zugangsdaten an eine in der E-Mail angegebene Adresse zu senden. In der Regel geschieht das mit der Androhung, der Account würde ansonsten geschlossen.

Im russischen Runet gelangen Phisher mit dieser Methode vor allem an Zugangsdaten von E-Mail-Accounts. Sobald sie die Post des Nutzers lesen können, erhalten die Betrüger oftmals auch seine Kennwörter für weitere Internetdienste.



Deutsche Übersetzung:

*Guten Tag!*  
*Im Zusammenhang mit dem Update der Datenbanken bitten wir Sie darum, sich erneut auf unserem E-Mail-Server anzumelden, um den Verlust Ihres E-Mail-Accounts zu vermeiden. Wir bitten für diese Unannehmlichkeiten um Entschuldigung!*

*Authorisierung*  
*Im Feld „Antwort“ tragen Sie bitte Ihr Kennwort ein und klicken Sie auf „antworten“.*

*Das Kennwort muss genau so eingetragen werden wie bei der Registrierung – unter Berücksichtigung der Groß- und Kleinschreibung und unbedingt in dem gleichen Feld wie bei der Registrierung (wenn bei der Registrierung Ihre Tastatur zufällig in der russischen Belegung geschaltet war oder CapsLock gedrückt wurde, können Sie Ihr Kennwort eingeben, indem Sie die Tastatur in den gleichen Modus schalten oder verschiedene mögliche Kombinationen probieren: [Rus], [CapsLock], [CapsLock + Rus] sowie verschiedene Codierungen der russischen Sprache).*

*Wenn Sie Besitzer weiterer Accounts unseres E-Mail-Dienstes E-Mail.ru sind, empfehlen wir, auch die Daten dieser Accounts anzugeben, um sie unserem neuen System der „Spam-Blockierung“ hinzuzufügen.*

*1999-2008, E-Mail.Ru*  
*Регистрация   Сообщество пользователей*

Eine andere verbreitete Methode zum Sammeln von E-Mail-Passwörtern ist der Versand von Nachrichten, die für eine „Schwachstelle bei der Kennwortwiederherstellung“ werben. Darüber kann man angeblich das Passwort eines anderen Nutzers erfahren. Um den Zugang zu einem fremden Account zu erhalten, muss der Empfänger der Spam-Mitteilung das Login des Opfers sowie sein eigenes Kennwort in an eine Webadresse senden. Wer dieses zweifelhafte Angebot annimmt, wird selbstverständlich selbst zum Opfer der Übeltäter. Mit der Zeit erkannten immer mehr Anwender, dass seriöse Unternehmen ihre Kunden niemals darum bitten, Kennwörter in E-Mails zu versenden. Damit wurden derartige Betrügereien zunehmend weniger effektiv. Da Spammer gefälschte E-Mails heutzutage immer sorgfältiger tarnen, fällt es den Anwendern immer schwerer, sie von legitimen Mitteilungen zu unterscheiden.

In westlichen Ländern verbreitete Internet-Zahlungssysteme und Online-Banking-Portale mit einer großen Anzahl von Kunden werden gewöhnlich zur Zielscheibe von Phishing-Angriffen. Da sich Online-Banking auch im russischen Internet immer stärker etabliert, führen die Phisher auch dort immer öfter Angriffe durch.

Ein Beispiel sind die nach klassischem Schema durchgeführten Phishing-Attacken auf Kunden der Alfa-Bank. Kunden erhielten vordergründig von der Bank-Administration verschickte E-Mails, die einen Link auf eine präparierte Webseite enthielten – äußerlich eine genaue Kopie der Alfa-Bank-Homepage. Die Nutzer wurden in der E-Mail aufgefordert, ihre Online-Banking-Zugangsdaten auf der Phishing-Webseite einzugeben. Unaufmerksame Nutzer verloren nicht nur ihre Kennwörter, sondern infizierten ihren Rechner über den Weblink obendrein auch mit einem Schadprogramm. Auf ähnliche Weise wurden Angriffe auf die Kunden der Systeme WebMoney und Yandex.Money durchgeführt. Einige Male war auch die Citibank im Visier der Phisher.

Die Übeltäter versuchen, durch Phishing-E-Mails auch oftmals an Zugangsdaten für E-Mail-Accounts heranzukommen, indem sie Anwender wie oben beschrieben nach ihren Logins und Passwörtern fragen.

## Ergaunern von Geld per Spam

Neben Phishing nutzen Internet-Betrüger viele andere Spam-Varianten, um gutgläubige Anwender um ihr Geld zu erleichtern. Die Spammer rechnen dabei vor allem mit der Naivität und Habgier ihrer potenziellen Opfer – übrigens ein charakteristisches Merkmal aller Schwindler. Um ihr Ziel zu erreichen, verwenden die Betrüger unterschiedliche Methoden. Die am weitesten verbreiteten werden im Folgenden detailliert betrachtet.

### Nigeria Connection

Dieses populäre Betrugsschema stammt ursprünglich von Cyberkriminellen aus Nigeria und wird deswegen oft auch als „Nigeria Connection“ bezeichnet. Heutzutage praktizieren jedoch Gauner aus der ganzen Welt die „nigerianische“ Betrügerei.

Bei der „nigerianischen“ Variante schicken Spammer E-Mails, deren Dramaturgie immer gleich aufgebaut ist. Der Absender handelt anscheinend im Auftrag einer angesehenen afrikanischen Familie, die aufgrund von Bürgerkrieg, einem Staatsstreich, einer Wirtschaftskrise oder politischer Verfolgung in der Heimat in Ungnade gefallen ist. Im „nigerianischen“ Brief wird der Empfänger in gebrochenem Englisch deshalb gebeten, zum Transfer des Familienvermögens sein eigenes Konto zur Verfügung zu stellen. Als Belohnung versprechen die Betrüger eine stattliche Prämie, in der Regel einige Prozent der überwiesenen Summe. Im Verlauf der Hilfsoperation stellt sich aber heraus, dass der Helfer nun selbst Geld zahlen soll, um die Überweisung in Gang zu bringen. Es verwundert daher wenig, dass nach Überweisung des Geldes plötzlich jeder Kontakt mit dem Familienvertreter abbricht. Doch manchmal wird das Opfer unter dem Vorwand außerplanmäßiger Komplikationen noch einige Male darum gebeten, in die Tasche zu greifen.

In einer Variante der Nigeria Connection gibt sich der Absender als hochgestellter Beamter aus. Dieser hat durch Bestechung und Betrügereien ein ziemlich großes Vermögen angehäuft, steht jetzt aber unter Beobachtung und kann das Geld nicht ins Ausland transferieren. Empfänger dieser E-Mail sollen dem Betrüger zur Überweisung des Geldes Zugang zu ihrem Bankkonto gewähren und werden wiederum mit einem bestimmten Prozentsatz der Gesamtsumme geködert. Natürlich lassen die Cyberkriminellen keinen Cent auf dem Konto des gutgläubigen Nutzers zurück, sobald sie die Zugangsdaten erhalten haben.

Kaum zu glauben, was für dramatische Geschichten in den „nigerianischen“ Briefen erzählt werden. Für ihre Fantasie wurde den unbekanntem Autoren im Jahre 2005 sogar der Anti-Nobelpreis für Literatur verliehen. Auch die russischen Ausgaben waren erfinderisch. Im Jahr 2005 wurden typische „nigerianische“ Briefe in

englischer Sprache verschickt, deren Absender angeblich zum näheren Umfeld des geächteten Oligarchen Mikhail Khordokovsky gehören. Abgesehen vom russischen Bezug gibt es ansonsten keinerlei Unterschiede zum klassischen „nigerianischen“ Betrugsschema.

*Dear Friend,*

*I am Lagutin Yuriy and I represent Mr. Mikhail Khordokovsky the former C.E.O of Yukos Oil Company in Russia. I have a very sensitive and confidential brief from this top (Oligarch) to ask for your partnership in re-profiling funds over US\$450 million. I will give the details, but in summary, the funds are coming via Bank Menatep. This is a legitimate transaction. You will be paid 4% for your „Management Fees“.*

*If you are interested, please write back by eMail and provide me with your confidential telephone number, fax number and eMail address and I will provide further details and instructions. Please keep this confidential; we can't afford more political problems. Finally, please note that this must be concluded within two weeks. Please write back promptly.*

*Write me back. I look forward to it.*

*Regards,*

*Lagutin Yuriy*

Es existiert auch eine romantische Variante dieses Betrugs-Schemas, nämlich die Briefe „nigerianischer“ Bräute. Hier stammen die Mitteilungen scheinbar von Mädchen aus exotischen Ländern und enthalten das Foto einer dunkelhäutigen Schönheit. Solche E-Mails erhalten vor allem Nutzer, die bei Online-Bekanntschaffungsvermittlungen registriert sind. Wenn sich das potenzielle Opfer auf einen elektronischen Briefwechsel einlässt, erzählt man ihm eine Geschichte im Stil einer Seifenoper: Die Verwandten wurden ermordet, das Mädchen kann nicht aus dem Land heraus und ist eine reiche Erbin. Bereits im dritten Brief schwört das Mädchen dem Empfänger ewige Liebe und bittet ihn, sie gemeinsam mit den Millionen außer Landes zu bringen. Alles, was der Retter tun muss, ist beim Transfer der Geldsumme zu helfen, wofür er eine stattliche Prämie erhalten soll. Natürlich werden vom Helfer vorläufige Ausgaben verlangt, die sich auf einige tausend, manchmal auch zehntausende von US-Dollar belaufen können. Um noch überzeugender zu wirken, bringen die Cyberkriminellen zum Beispiel einen fiktiver Pfarrer ins Spiel und bringen schließlich sogar gefälschte Dokumente in Umlauf.

### Falschmeldungen über Lottogewinne

Diese Art von betrügerischem Spam ähnelt den nigerianischen Briefen sehr. Nutzer erhalten fingierte Mitteilungen über Lotteriegewinne, die angeblich unter zufällig ausgewählten E-Mail-Adressen oder Telefonnummern ermittelt wurden. Die E-Mail kann dabei alle möglichen falschen Informationen wie Losnummer, Registrierungsnachweis, Fotos vom Preis oder die Lizenzdaten des Betreibers enthalten. Wie im Nigeria-Fall muss der Empfänger eine gewisse Summe vorab auf das Konto der Betrüger überweisen, um an seinen Gewinn zu kommen.



Empfänger derartiger Nachrichten sollten unbedingt beachten, dass die Teilnahme an einer beliebigen Lotterie immer ihre vorherige Zustimmung voraussetzt. Wenn Anwender keine Erlaubnis erteilt haben und ihnen die Lotterie unbekannt ist, liegt ein typischer Spam-Betrugsversuch vor. Cyberkriminelle wollen dem Nutzer höchstens Geld aus der Tasche ziehen, ihn aber keinesfalls mit einem Gewinn beglücken.

### **Fehlerhafte Zahlungssysteme, Wunderbörsen, Code-Generatoren**

Spam-Nachrichten dieser Art informieren Empfänger über eine angebliche Schwachstelle eines Zahlungssystems, über die man sich schnell bereichern könne. Des Weiteren wird eine Nebenverdienst-Möglichkeit empfohlen, die normalerweise darin besteht, eine Geldsumme an eine „Wunderbörse“ zu schicken. Die Betrüger versprechen, dass sie dem Nutzer innerhalb einer bestimmten Zeit nach Überweisung die doppelte oder dreifache Summe seines Geldes zurückerstatten. Es versteht sich von selbst, dass diese „Wunderbörse“ den Betrügern gehört und die überwiesenen Gelder unwiederbringlich verloren sind. Darüber hinaus kann der Geschädigte seinen Verlust bei der illegalen Börse auch nirgends geltend machen.

Bei einer weiteren Betrugsvariante wird dem Opfer ein Programm angeboten, das angeblich Kreditkartennummern generieren kann, oder mit dem man Geld von fremden Konten abheben kann. Die ersten Einsätze der Software sind kostenlos, allerdings müssen Nutzer dafür ihre eigenen Kontodaten samt Kennwort angeben. Beim Versuch, ein fremdes Konto zu knacken, landen die eingegebenen Daten prompt bei den Übeltätern, die natürlich das Konto des Nutzers plündern.

Dieses Betrugsschema gibt es nicht nur für Bankkonten, sondern existiert auch für Mobilfunkdienste oder Internetanschlüsse. Bei diesen Programmen sollen Anwender zuerst die Nummer einer noch nicht aktivierten

Karte eingeben, die als Vorlage für alle anschließend erzeugten Codes dienen soll. Ebenso wie bei den Kreditkarten-Tools gelangen die eingegebenen Daten in die Hände der Betrüger. Während das Programm vor-täuscht, neue Nummern zu berechnen, bezahlen die Betrüger mit dem „Beispielcode“ bereits ihr Lehrgeld.

### **Löchrige Casinos**

Eine weitere Betrugsart zielt auf Kunden von Online-Casinos ab. In darauf zugeschnittenen E-Mails wird Anwendern suggeriert, sie könnten ihre Spielhallen-Gewinnchancen mit einer jüngst entdeckten Sicherheitslücke drastisch erhöhen. Anschließend beschreibt die Nachricht die Gewinnstrategie und verweist per Link auf die Webseite des Casinos. Natürlich existiert keine Sicherheitslücke. Den im Auftrag der Casinoseite tätigen Cyberkriminellen geht es nur darum, möglichst viele Anwender in die virtuelle Spielhölle zu locken. In anderen E-Mail-Varianten wird dem Anwender vorgeschlagen, ein bestimmtes Programm herunterzuladen, das angeblich die Schwachstelle ausnutzt. Allerdings erweist sich das Tool dann als Spionageprogramm.

### **Schnelle Verdienstmöglichkeiten**

E-Mails, die mit schnellen Verdienstmöglichkeiten werben, beginnen charakteristischerweise wie folgt: „Diese Nachricht ist KEIN Spam, sondern ein ernst gemeintes Angebot zum Geldverdienen. Sie erhalten diese Mitteilung nur ein einziges Mal. Verpassen Sie nicht die Gelegenheit, schnell und einfach Geld einzunehmen.“ Früher oder später kommt dann das Schneeballsystem zur Sprache: Der Empfänger soll dem Absender eine gewisse Summe zahlen und anschließend die E-Mail selbst an mehrere Empfänger weitersenden, um von diesen wiederum jeweils den gleichen Betrag einzufordern. Ein solches System verspricht jedem Beteiligten märchenhafte Gewinne, doch wer diesem Schwindel aufsitzt, hat sein Geld für immer verloren.

Gerissener gehen diejenigen Spammer vor, die Nutzern über E-Mails fingierte Jobangebote unterbreiten. Dabei versprechen sie ihnen einen hohen Lohn für eine nicht besonders schwierige Tätigkeit. Kommt ein Kontakt zustande, bitten die Cyberkriminellen um Überweisung eines Geldbetrages für detaillierte Job-Informationen oder für Postausgaben. Nutzer werden dabei gedrängt, möglichst schnell Geld zu zahlen, weil die vakante Stelle sonst anderweitig besetzt werde.

Manchmal schicken die Betrüger ihre Angebote direkt an Nutzer, die ihre Kontaktdaten in Online-Jobbörsen eingetragen haben. Ihnen wird die Teilnahme an einem internationalen Projekt vorgeschlagen, bei dem es zum Beispiel um Gold- oder Diamantenförderung, dem Abschluss von Serviceverträgen oder der Herstellung medizinischer Geräte, Impfstoffe oder Chemikalien geht. In der Regel bezieht sich das Jobangebot auf den Tätigkeitsbereich des Bewerbers oder auf seine

Geschäftskontakte. Irgendwann kommen die Betrüger unweigerlich auf „administrative Kosten“ zu sprechen und bereichern sich am Geld des Opfers.

*Subject: Prospective Employee  
Attn: Prospective Employee,  
Spiralnergy Exploration, UK is an oil and gas exploration and production company based in United Kingdom.  
The Company's producing properties and Exploration activities are focused on the UK Central North Sea.  
The goal of Spiralnergy Exploration in the near term is to achieve oil production from its interests in the North Sea while carrying out an active exploration /development program on both its own properties and in various joint venture opportunities currently being considered by the Company.  
Spiralnergy Exploration, UK hereby inform that, you have been shortlisted as one of the personnel/expatriate for our upcoming project schedule to commence March, 2008.  
The project involves the construction of a new LPG(Liquefied Petroleum Gas ) Plant and Oil Wells at UK Central North Sea, UK.  
You are hereby require to send your detailed resume and application via fax or eMail attachment to us in not later than 5(five) days of receiving this eE-Mail.  
All resumes/application should be in MS Word format.  
Thanks for your interest.  
William Peters  
{Address}, UK*

*This eMail and any attachments to it contain information that is confidential and may be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s) please note that any form of distribution, copying or use of this communication or the information contained in it is strictly prohibited and may be unlawful. If you have received this eMail in error, please return it to the sender (Spiralnergy Exploration) and delete the eMail from your records.*

## Erpressung

Um an das Geld ihrer Opfer heranzukommen, greifen Spammer mitunter nicht nur zum Zuckerbrot, sondern auch zur Peitsche: Beispielsweise fordern Cyberkriminelle vom Anwender Geld und drohen ihm bei Nichtzahlung mit einer Spam-Lawine. Doch es gibt auch weitaus ernstzunehmendere Angriffe. In manchen E-Mails werden die Empfänger von einem angeblichen Killer mit dem Tod bedroht und sollen sich mit Geld freikaufen.

*Subject: BE WARN!!!  
HELLO  
I am very sorry for you Xxxxxx, is a pity that this is how your life is going to end as soon as you don't comply. As you can see there is no need of introducing myself to you because I don't have any business with you, my duty as I am E-Mailing you now is just to KILL you and I have to do it as I have already been paid for that.  
Someone you call a friend wants you Dead by all means, and the person have spent a lot of money on this, the person also came to us and told me that he wanted you dead and he provided us with your name ,picture and other necessary information's we needed about you. So I sent my boys to track you down and they have carried out the necessary investigation needed for the operation on you, and they have done that but I told them not to kill you that I will like to contact you and see if your life is Important to you or not since their*

*findings shows that you are innocent.  
I called my client back and ask him of your eMail address which I didn't tell him what I wanted to do with it and he gave it to me and I am using it to contact you now. As I am writing to you now my men are monitoring you and they are telling me everything about you.  
Now do you want to LIVE OR DIE? As someone has paid us to kill you. Get back to me now if you are ready to pay some fees to spare your life, \$4,000 is all you need to spend You will first of all pay \$2,000 then I will send a tape to you which i recorded every discusion in made with the person who wanted you dead and as soon as you get the tape, you will pay the remaining \$2,000. If you are not ready for my help, then I will carry on with my job straight-up.  
WARNING: DO NOT THINK OF CONTACTING THE POLICE OR EVEN TELLING ANYONE  
BECAUSE I WILL KNOW.REMEMBER, SOMEONE WHO KNOWS YOU VERY WELL WANT YOU DEAD!  
I WILL EXTEND IT TO YOUR FAMILY, INCASE I NOTICE SOMETHING FUNNY.  
DO NOT COME OUT ONCE IT IS 7:PM UNTILL I MAKE OUT TIME TO SEE YOU AND GIVE YOU THE TAPE OF MY DISCUSSION WITH THE PERSON WHO WANT YOU DEADTHEN YOU CAN USE IT TO TAKE ANY LEGAL ACTION. GOOD LUCK AS I AWAIT YOUR REPLY EE-MAIL:donwilliam1@gE-Mail.com*

## Abzocke per SMS

Neben bekannten Internet-Betrugsschemata, die vor allem auf ein westliches Publikum abzielen, setzen Cyberkriminelle im Runet neue Methoden ein. Sie mieten Handynummern bei Mobilfunkbetreibern und versenden darüber Spam. Empfänger sollen dazu verleitet werden, eine SMS an die gepachtete Nummer zu schicken. Die Betrüger erhalten einen Teil der dabei fälligen Gebühren. Um ihr Ziel zu erreichen, wenden die Betrüger verschiedene Tricks an: Sie locken Nutzer mit kostenfreien Internetzugängen und Gewinnversprechen oder drohen damit, ihre E-Mail-Box zu blockieren, sollten sie keine SMS absenden.

*Sehr geehrter Nutzer von E-Mail.ru!  
Wir möchten Sie darüber informieren, dass heute, am 06. April 2008, von Ihrem elektronischen Postfach Spam aus verschickt wurde.  
Um den Vorfall untersuchen zu können, haben wie Ihre E-Mail-Konto für 24 Stunden blockiert. Sollten Sie keinen Spam verschickt haben und wünschen keine Blockierung Ihres Postfachs, so senden Sie eine SMS an die Nummer 1171 mit dem Code = vips 1. Danach erhalten Sie in einer Antwort-SMS weitere Instruktionen. Sollten Sie keine SMS senden, wird Ihr Account vom Antispam-System blockiert.  
Wir empfehlen Ihnen, künftig ein sicheres Kennwort zu verwenden.  
Achtung, die SMS ist kostenpflichtig! Der Preis für die SMS beträgt inklusive Mehrwertsteuer 2.9 Rubel.*

*Bitte antworten Sie nicht auf diese E-Mail, sie wurde maschinell erstellt!*

*Mit freundlichen Grüßen  
Servicecenter E-Mail.ru*

In einer Spam-E-Mail wurde den Empfängern sogar angeboten, sich vor Spam schützen zu lassen. Der Absender bezog sich auf das in Russland am 1. Juli 2007 in Kraft getretene Gesetz „Über die Werbung“ und warb mit einem direkten Zugang zu einer Spammer-Datenbank. Dazu sollte der Empfänger eine kostenlose SMS abschicken, würde anschließend einen Weblink zur Datenbank erhalten und könnte seine dort gespeicherte E-Mail-Adresse löschen.

Manchmal kann in einer Spam-Mail auch nur ein Link auf eine von den Spammern speziell geschaffene Webseite enthalten sein. Auf der Seite wird dem Anwender (zum Beispiel einem, der schon einen angeblichen „Gewinn“ angefordert hat) vorgeschlagen, eine SMS-Mitteilung an eine Kurzwahl zu senden. Eine solche Ausdehnung und Verkomplizierung des Schemas, das zu dem von den Spammern gewünschten Absenden der SMS führt, ist dazu bestimmt, die Aufmerksamkeit auch der wachsamsten Nutzer abzustumpfen.

### Zusammenfassung

Kaspersky Lab ordnet betrügerische Spam-E-Mails der Rubrik „Computerbetrug“ zu. Ihr Anteil am gesamten Spam-Aufkommen lag im Jahr 2007 bei ungefähr 7 Prozent. Im ersten Quartal 2008 verringerte sich dieser Wert um mehr als die Hälfte und kam nur noch auf 2,5 Prozent.

Betrügerische Spam-E-Mails kursieren zwar in geringeren Mengen als noch 2007, werden aber immer ausgereifter und damit gefährlicher. Cyberkriminelle führen auch immer öfter gezielte Angriffe durch. Selbst gesunder Menschenverstand reicht dann unter Umständen nicht mehr aus, um die raffinierten Betrugsversuche zu durchschauen. Gegen Phishing-Versuche helfen ohnehin nur die passenden Schutzprogramme wie Phishing-Schutz und Anti-Spam-Software.

Kaspersky Lab kann allen Anwendern deshalb nur raten, den Angeboten der Spammer keinen Glauben zu schenken und ausschließlich Software zu verwenden, die zuverlässig vor Spam, Phishing-E-Mails und Malware schützt. Obwohl diese Empfehlungen trivial erscheinen, schützt man damit nicht nur die Daten seines Computers, sondern auch sein Geld.

**Natalya Zablotskaya**  
Senior Spam Analyst, Kaspersky Lab

### Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

### Kontakt

Kaspersky Labs GmbH  
Steinheilstr. 13  
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0  
Telefax: +49 (0)841 981 89 100

info@kaspersky.de  
www.kaspersky.de