G Data

Whitepaper 6/2011

Gefährliche E-Mails

Sabrina Berkenkopf & Ralf Benzmüller
G Data SecurityLabs

Inhalt

1 Einleitung 2

1.1 E-Mail, ein kurzer Überblick 2
1.2 Wer steckt hinter dem Spamversand? 3
1.3 Psychologische Grundlagen von Spam 4

2 Die verschiedenen Maschen 5

2.1 Die Neu-Anmelden-Masche (Datendiebstahl, Malware) 5
2.2 Die Unregelmäßigkeiten-Masche (Phishing) 6
2.3 Die Grußkarten-Masche (Malware) 7
2.4 Die Paketversand-Masche (Malware und Phishing) 8
2.5 Die „Schau mal hier"-Masche (Malware und Werbung) 9
2.6 Die Rabatt-Masche (Malware) 10
2.7 Akademische Grade und Titel-Masche (Phishing und Abzocke) 11
2.8 Online Casino-Masche (Phishing und Abzocke) 12
2.9 419er-Masche / Nigeria-Spam (Abzocke) 13
2.10 Job-Masche (Malware und Abzocke) 14
2.11 Russian Bride-Masche (Abzocke) 15
2.12 Lotterie-Masche (Abzocke) 16

3 Tipps und Tricks 17

3.1 Nützliche Verhaltensregeln 17
3.2 Technische Maßnahmen 17

4 Glossar 18

1 Einleitung

1.1 E-Mail, ein kurzer Überblick

Das Kommunikationsmedium E-Mail ist in der heutigen Zeit aus dem Berufsalltag und auch aus dem Privatbereich nicht mehr wegzudenken. Der Versand von E-Mails ist extrem kostengünstig und schnell und das bei einer weltweiten Reichweite.

Anwender benutzen zum Arbeiten mit E-Mails installierte Programme auf ihrem Rechner (E-Mail Clients) oder rufen die E-Mails per Browser ab. Eine derart beliebte Funktion lockt natürlich auch Betrüger an, die technische Unzulänglichkeiten ausnutzen.

Die Abwicklung des Versands und Empfangs von Mails wird dabei im Hintergrund vorgenommen und der Anwender bekommt davon im Idealfall nichts mit. Das Protokoll zum Versand nennt sich SMTP, Simple Mail Transfer Protocol. Empfangen werden E-Mails über POP3 (Post Office Protocol, Version 3) oder IMAP (Internet Message Access Protocol).

Der Aufbau von elektronischer Post ist, ähnlich wie bei einer Postkarte, aufgeteilt. Auf der einen Seite, im Informationsteil (Header), werden Absenderdaten, Empfängerdaten, Datum, Betreff etc. untergebracht. Der zweite Bestandteil ist der Textteil (Body), der den eigentlichen Inhalt transportiert.

Da beim Versand einer Mail im SMTP keine Authentifizierung des Klartextes stattfindet, kann an dieser Stelle geschummelt werden: Es ist zum Beispiel möglich, die Absenderadresse im Header zu ändern und so dem Empfänger eine falsche Identität vorzugaukeln. Auch Inhalte können ohne großen Aufwand manipuliert werden.

Bei all den schon erwähnten positiven Eigenschaften von E-Mails gibt es allerdings auch die andere Seite der Medaille: Das E-Mail Postfach quillt schon wieder über, der Großteil der empfangenen Mails ist unerwünschte Post mit zwielichtigen Werbeversprechen, Traumjobangeboten, Flirteinladungen und ähnliches. Was die Computeranwender dieser Welt täglich nervt ist ☞Spam[1]. Diese unaufgefordert und massenhaft empfangenen Mails sind nicht nur wegen ihrer hohen Anzahl störend, sondern können auch gefährlich sein.

Betrügerische und gefährliche E-Mails kommen in vielen verschiedenen Varianten. Als unerwünschte Werbemail, Phishing, Malware mit Dateianhang oder einem Link auf präparierte Webseiten. Bevor im folgenden Kapitel die einzelnen Vorgehensweisen und Maschen der E-Mail-Betrüger genau beschrieben werden, wollen wir noch einige Hintergründe beleuchten.

[1] Die Erklärungen für Fachbegriffe die mit ☞ gekennzeichnet sind, stehen im Glossar

1.2 Wer steckt hinter dem Spamversand?

Cyberkriminelle nutzen das Medium E-Mail nach wie vor ausgiebig für ihre betrügerischen Machenschaften. Der massenhafte Versand von unerwünschten E-Mails, kurz Spam, ist eine der bekanntesten Geschäftszweige der Schattenwirtschaft von Cyberkriminellen. Im vierten Quartal 2010 waren durchschnittlich 83 % des globalen E-Mail-Verkehrs Spam, was einem Mittelwert von 142 Milliarden Spam-Mails pro Tag entspricht.[2]

Die Beliebtheit lässt sich unter anderem durch die gute Kosten-Nutzen-Rechnung erklären: Der Versand von 1.000.000 Spam-E-Mails kostet aktuell bei verschiedenen Anbietern zwischen 399 und 800 US-Dollar. Auch im Angebot: 2.000.000 Mails zum Preis von 1.000.000.

General Email Marketing Campaign Prices			
# of Emails Delivered	Price	Cost p/ Thousand	
100,000	$99	$1.00	Order Now!
250,000	$199	$.80	Order Now!
400,000	$249	$.62	Order Now!
1,000,000 (Get a 2 million campaign	$399* for the price of 1 million)	$.19	Order Now!
3,000,000	$549	$.18	Order Now!
10,000,000	$1499	$.15	Order Now!
25,000,000	$1999	$.08	Order Now!
50,000,000	$2499	$.05	Order Now!

Screenshot 1: *Die Preisliste eines Bulk-E-Mail Versandservices im Internet. Diese Preise sind für generellen Spamversand, ohne feste Zielgruppe*

Die Adressenlisten mit Zielpersonen werden ebenfalls im Untergrund angeboten oder direkt bei den Bulk-E-Mail Servicedienstleistern verkauft und, wenn nötig, auch auf den jeweiligen Kunden zugeschnitten. So ist es möglich, Adressen sortiert nach Zielgruppen zu kaufen – z.B. spezielle Listen mit Online-Gamern oder Personen aus bestimmten Regionen und viele andere Kategorien.

Georgraphic Email List Options	Price	
1 Country or 1 State or 1 City or 1 US Zip Code	$298	Order Now!
2 Countries or 2 States or 2 Cities or 3 US Zip Codes	$398	Order Now!
3 Countries or 4 States or 4 Cities or 6 US Zip Codes	$498	Order Now!
6 Countries or 8 States or 8 Cities or 15 US Zip Codes	$798	Order Now!
12 Countries or 14 States or 14 Cities or 25 US Zip Codes	$1198	Order Now!
Larger List Packages	Inquire	Order Now!

Screenshot 2: *Aufpreise für gezielten Mailversand – In diesem Fall geht es um lokale Zielgruppen*

Versendet werden die Spam-Mails überwiegend per ☞Botnetz. Mit einem eher kleinen Botnetz von rund 20.000 ☞Zombie-Rechnern benötigt ein Botnetz-Betreiber für die Ausführung eines Auftrags mit 1.000.000-Mails bei beispielsweise 2 Mails pro Sekunde und aktivem ☞Bot gerade mal 25 Sekunden. Rein rechnerisch kann ein Betreiber eines relativ kleinen Botnetzes für den Versand also bis zu 115.200 US-Dollar pro Stunde verdienen.

[2] Commtouch, Q4 2010 Internet Threats Trend Report. Zahlen basieren auf ungefiltertem Datenstrom, ohne firmeninternen Traffic

1.3 Psychologische Grundlagen von Spam

Egal in welcher Form die E-Mail in das digitale Postfach flattert, häufig basieren die Tricks der E-Mail-Betrüger auf ☞Social Engineering. Dabei werden gezielt Emotionen, Meinungen, Einstellungen und Verhaltensweisen ausgenutzt, um die Mail-Empfänger in die Falle zu locken. Dieser Versuch, durch soziale Manipulation an vertrauenswürdige Daten zu gelangen, nutzt quasi die „Sicherheitslücke Mensch".

Um wirkungsvoll Social Engineering zu betreiben, bedienen sich die Betrüger des (gefälschten) Absenders, der Betreffzeile und des Inhalts der Mail. Aber auch der Dateiname des Dateianhangs, doppelte Dateiendungen, populäre Icons oder der Domainname des Links können zur Verschleierung eines solchen Betrugsversuchs genutzt werden. In einer Studie von 2005 nennen Jordan und Goudey[3] die folgenden 12 psychologischen Faktoren, auf denen die erfolgreichsten Würmer zwischen 2001 und 2004 beruhten:

- Unerfahrenheit (inexperience)
- Neugier (curiosity)
- Gier (greed)
- Zaghaftigkeit/Schüchternheit (diffidence)
- Höflichkeit (courtesy)
- Eigenliebe (self-love)
- Leichtgläubigkeit (credulity)
- Wunschdenken (desire)
- Lust und Liebe (lust)
- Drohung (dread)
- Gegenseitigkeit (reciprocity)
- Freundlichkeit (friendliness)

Ein Jahr später ergänzte M. Braverman[4]:

- Allgemeine Konversation (generic conversation): Kurze Aussagen, wie "Cool" etc.
- Virenwarnungen und Software-Patches
- Malware-Fund auf dem PC
- Virenprüfberichte am Ende der Mail
- Informationen oder Meldungen zu Accounts: z.B. der Telekom-Trojaner, der sich als überhöhte Telefonrechnung ausgibt
- Fehlermeldungen der Mailzustellung
- Körperliche Anziehung (Physical attraction)
- Anklagen (Accusatory): z.B. der BKA-Trojaner, der angeblich illegale Dateien gefunden haben will
- Aktuelle Ereignisse
- Free stuff: Manche Menschen lassen alle Vorsicht fahren, sobald es etwas umsonst gibt

[3] vgl. Jordan, M., Goudey, H. (2005) "The Signs, Signifiers and Semiotics of the Successful Semantic Attack". In: Proceedings of the EICAR 2005 Conference, S. 344 - 364.
[4] vgl. Braverman (2006) "Behavioural Modelling of Social Engineering-based Malicious Software". In: Proceedings of Virus Bulletin Conference 2006, S. 15-22.

2 Die verschiedenen Maschen

2.1 Die Neu-Anmelden-Masche (Datendiebstahl, Malware)

Die E-Mail suggeriert, dass ein Onlinesystem oder ein Programm aktualisiert wurde und nun eine sofortige (!) Aktualisierung der Kundendaten geschehen muss, damit die Funktionen des Services weiterhin einwandfrei benutzt werden können. Der Link zur angeblichen Aktualisierungs-Webseite ist in der Mail direkt angegeben und häufig ist es nur durch einen genauen Blick auf die verlinkte Adresse erkennbar, dass es sich nicht um die originale Adresse handelt. Die verlinkte Webseite selbst ist häufig eine 1:1-Kopie des Originals und rein optisch fast nicht als Fälschung zu enttarnen.

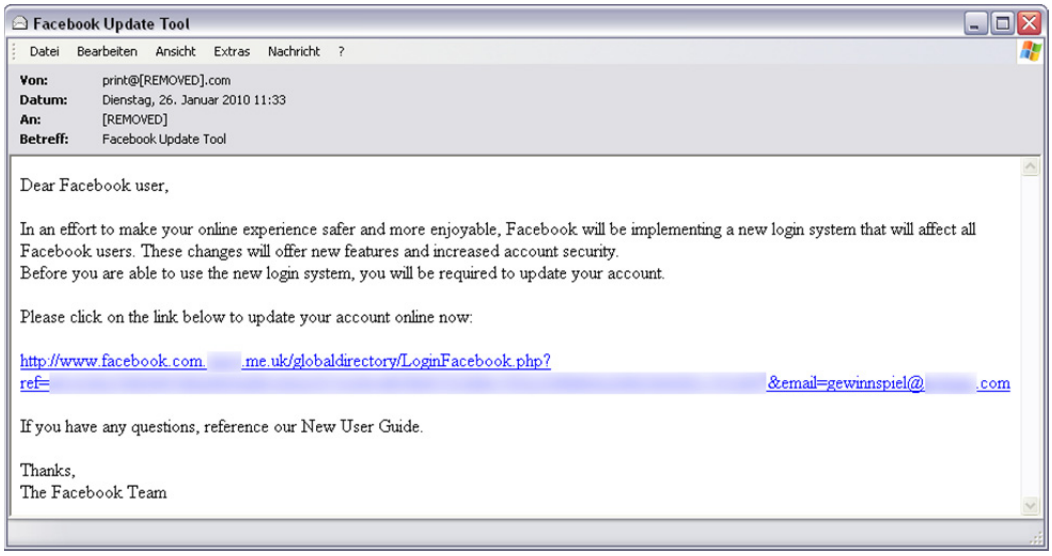
Die Zielgruppe: Jeder Internetnutzer, jedoch besonders Kunden verschiedenster Banken und Bezahldienste, sowie Benutzer populärer Software, Sozialer Netzwerke, Online-Spiele, kostenlosen E-Mail-Diensten und Webapplikationen

Psychologische Ansatzpunkte: Unerfahrenheit, Leichtgläubigkeit, Sicherheitsbewusstsein

Die Gefahr: Gibt der gutgläubige Besucher auf der verlinkten, gefälschten Webseite die angefragten Daten ein, erhalten die Betrüger damit wertvolle Informationen über die Person. Diese können, je nach Art und Aufmachung der Webseite, von Namen und Adresse bis hin zu Kreditkartennummern und PIN-Codes reichen. Der Missbrauch dieser Daten ist vorprogrammiert!

Bei dieser Masche spielt Autorität eine wichtige Rolle, denn unerfahrene Nutzer lassen sich durch einen gefälschten Absender und die Vorgabe einer bekannten Instanz leicht zu Klicks und anderen Aktionen verleiten.

Betreff-Beispiele: Facebook Password Reset Confirmation. Customer Message.
Yahoo Warning!!! (Verify Your Account Now To Avoid Service Suspension..)
Urgent Notice: Paypal Limited
Your account has open issues !!!
Facebook Update Tool
World of Warcraft Account - Subscription Change Notice



Screenshot 3: *E-Mail mit Update-Aufruf per Link. Dieser Link leitet nicht etwa auf facebook.com, sondern auf eine Seite mit der Second Level Domain .me.uk*

2.2 Die Unregelmäßigkeiten-Masche (Phishing)

Diese Masche gaukelt dem potenziellen Opfer vor, es hätte ein Problem in seinem Account gegeben und dieser würde daher umgehend gesperrt werden müssen. Um die Sperrung abzuwenden, soll der User sofort (!) seine Account-Daten auf einer verlinkten Webseite angeben.

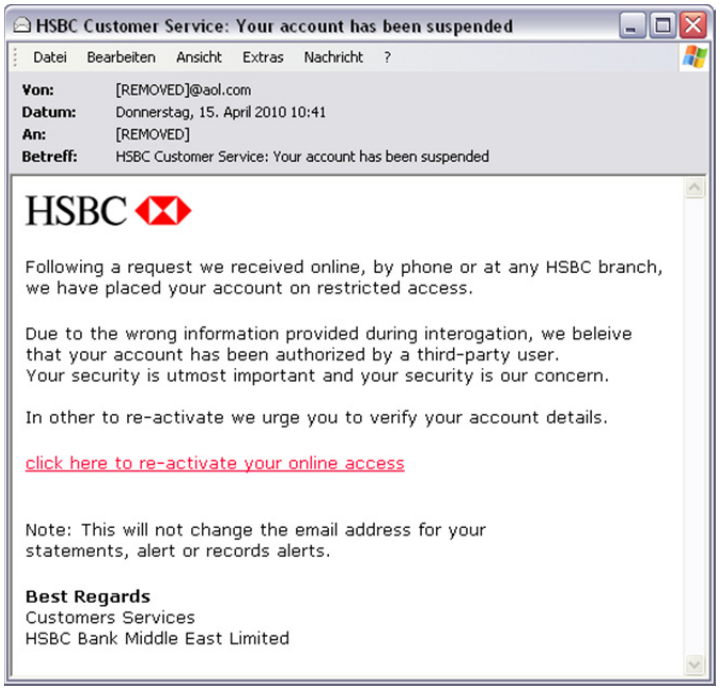
Die Zielgruppe: Jeder Internetnutzer, jedoch besonders Kunden verschiedenster Banken und Bezahldienste, E-Mail Services, etc.

Nutzer von Diensten, deren einzige Zugangskontrolle in einem Login-Namen und einem Passwort besteht, sind besonders lohnende Ziele – insbesondere wenn über die Dienste Geld transferiert werden kann oder wenn sie in der Untergrund-Ökonomie einen Wert besitzen (Geldwäsche, Spamversand, Versand von Hehlerware etc.)

Psychologische Ansatzpunkte: Unerfahrenheit, Schüchternheit und Drohung

Die Gefahr: Wie bei der Neu-Anmelden-Masche wird auch hier ganz gezielt nach gehaltvollen persönlichen Daten gefischt und ein besonderes Augenmerk liegt hier auf Bankdaten jeglicher Art. Auch in diesem Fall, wie bei der Aktualisierungs-Masche, ist die Akzeptanz von vorgetäuschten Autoritäten ein Kriterium für den Erfolg der Attacke.

Betreff-Beispiele: Attention! Your PayPal account has been violated!
Your Pay PalAccount May Be Compromised
Multiple Logon Errors on your Account.
Notification of Limited Account Access RXI034
Santander Merger Important Urgent Message
<<< IMPORTANT MESSAGE FROM SECURITY CENTER >>>
Attn. All Webmail Users



Screenshot 4: *Eine Phishing E-Mail, die offizielle Korrespondenz einer Bank nachahmt*

2.3 Die Grußkarten-Masche (Malware)

Gefälschte Grußkarten werden das ganze Jahr über verbreitet, jedoch erhalten sie gerade zu Fest- und Feiertagen immer wieder spezielle Aufmerksamkeit von Betrügern und Betrogenen. Die Versuchung ist groß, sich den vermeintlichen Gruß „eines Freundes“ anzusehen, doch genau da schnappt die Falle zu.

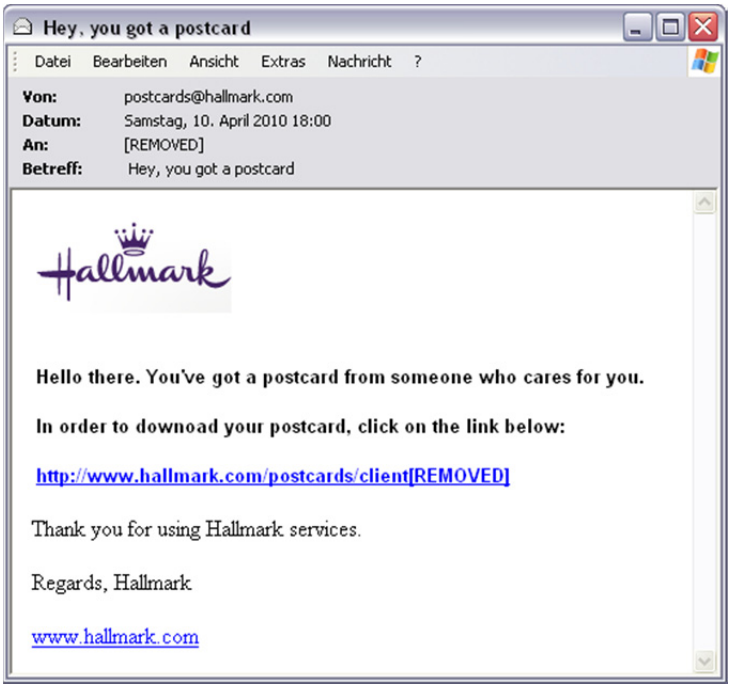
Es gibt mehrere Arten von Mails: Einerseits gibt es Mails mit als eCard getarnten Anhängen, die ihre Attacke ausführen, sobald sie geöffnet werden. Dann gibt es die Mails, die den Nutzer auf einer Webseite auffordern, einen vermeintlichen Codec oder Multimediaplayer zu installieren, damit die vermeintliche eCard angezeigt wird. Und zu guter Letzt noch die Mails, die beim Besuch einer angeblichen Grußkarten-Webseite eine unbemerkte Drive-By-Infektion auslösen.

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Neugier, Freundlichkeit

Die Gefahr: Ebenso wie bei der so bezeichneten „Schau mal hier“-Masche ist der User dem schädlichen Code ausgesetzt sobald er eine Seite besucht, den Anhang öffnet oder das tarnende Abspielprogramm installiert. Daraus ergeben sich dann die Möglichkeiten für die Schadprogramme, persönliche Daten zu stehlen und/oder weiteren Schaden anzurichten.

Betreff-Beispiele: Kiss You My Love! Happy Valentine's Day!
You have received a Christmas Greeting Card!
Despina sended you a giftcard!
You Have a dGreetings card from a friend .
You have received a greeting from somebody who cares you !!!
Hey, you have a new Greeting !!!



Screenshot 5: *Die legitim wirkende Mail enthält einen gefährlichen Link – dieser zeigt auf eine ausführbare EXE-Datei und nicht auf die Homepage des Grußkartenanbieters*

2.4 Die Paketversand-Masche (Malware und Phishing)

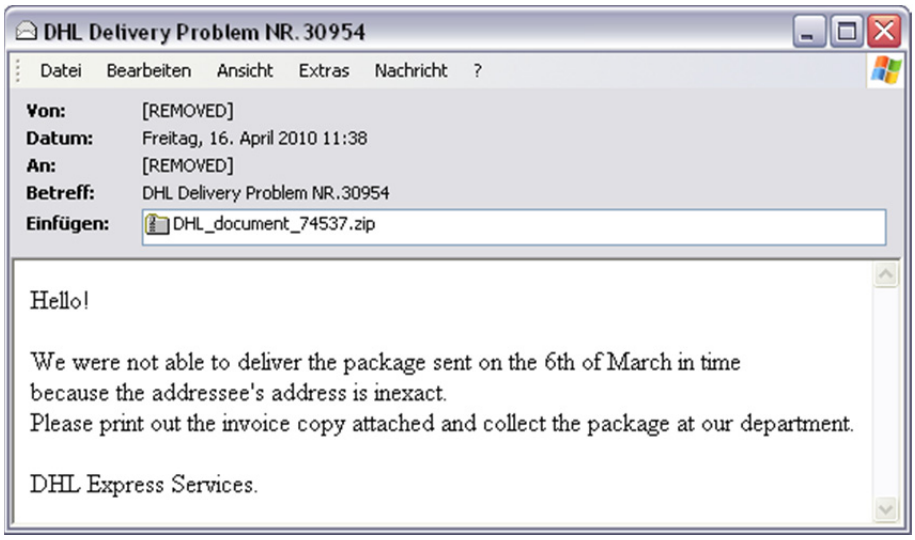
Der Empfänger erhält eine Mail mit einer Nachricht über einen angeblich fehlgeschlagenen Versandvorgang. Zur Lösung des Problems, oder um weitere Informationen zu erlangen, soll der Empfänger entweder eine angehängte Datei öffnen oder einen angegebenen Link besuchen. Hierbei haben es die Kriminellen häufig auf Kunden von Versanddienstleistern abgesehen, bei denen Pakete und Päckchen zeitlich ungebunden mit Nutzung einer PIN an einer Sammelstelle abgeholt werden können. International renommierte Versanddienstleister werden häufig zum Instrument für diese Phishing Kampagnen.

Die Zielgruppe: Jeder Internetnutzer, jedoch besonders Kunden populärer Versanddienstleister.

Psychologische Ansatzpunkte: Neugier, Gier, Wachsamkeit

Die Gefahr: Startet der User eine angehängte Datei aus der Mail, die häufig als Lieferschein getarnt wird, installiert er ungewollt Schadcode auf seinem Rechner, der zum Beispiel als Passwortstehler, Keylogger, etc. persönliche Daten ergaunern und weiterleiten kann. Nutzer geraten in die Phishingfalle, wenn sie z.B. ihre persönlichen Daten und Details der Paketempfangsstation auf einer gefälschten aber täuschend echt aussehenden Seite der Versanddienstleister eingeben. So gelangen Cyberkriminelle an die Zugangsdaten, können dort die an den Terminals angelieferten Pakete stehlen und außerdem den Ort als Anlieferungspunkt für Sendungen krimineller Machenschaften benutzen. Accounts dieser Stationen werden im Untergrund zum Versand von Waren genutzt, die mit gestohlenen Bankdaten oder Kreditkarten bezahlt wurden. Sie dienen letztlich der Geldwäsche und sind daher begehrt. Wer also seine Daten durch die Eingabe auf einer gefälschten Anmeldeseite preisgibt, muss mit weitreichenderem Schaden rechnen.

Betreff-Beispiele: DHL Services. Please get your parcel NR.0841
DHL Office. Get your parcel NR.1572
DHL Express. Get your parcel NR.3029
UPS Delivery Problem NR 68522.
Thank you for setting the order No.538532



Screenshot 6: *Eine E-Mail mit infiziertem Anhang, der sich als offizielles Dokument tarnt*

2.5 Die „Schau mal hier“-Masche (Malware und Werbung)

Bei dieser Variante vertrauen die Bösewichte vor allem auf die Kunst des Social Engineering und machen den Mail-Empfänger neugierig auf die angeblich brandaktuellen Neuigkeiten aus dem Netz, scheinbar peinliche Bilder und Videos der eigenen Person oder andere interessante Themen.

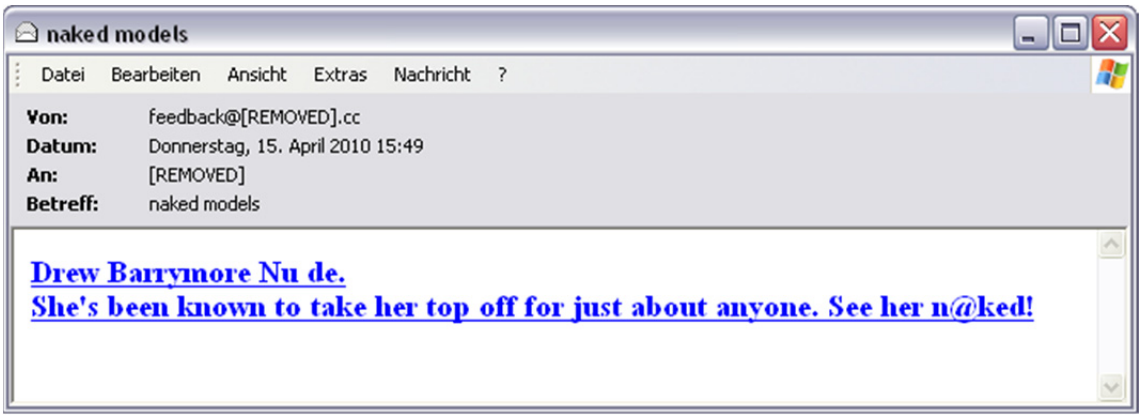
Der Schadcode lauert hier entweder direkt im infizierten Anhang der Mail oder auf der Webseite, auf die aus der Mail verlinkt wird. Hinter dem Link verbirgt sich zumeist die Aufforderung zur Installation eines Codecs oder eines neuen Abspielprogramms, welche dann bei der Ausführung Schadcode auf den Rechner bringen.

Die Zielgruppe: Jeder Internetnutzer, aber besonders Nutzer sozialer Netzwerke

Psychologische Ansatzpunkte: Neugier, Lust

Die Gefahr: Bei dieser Variante wird das Opfer durch Schadcode attackiert und kann so seinen Rechner mit verschiedenen bösartigen Programmen infizieren. Diese Programme können dann Passwörter auslesen, Kreditkartendaten stehlen, den PC in ein Botnetz einbinden und vieles mehr.

Betreff-Beispiele: Skandal Britney Spears tot
Iceland volcano disrupts flights accumulable
200,000 flood Shanghai Expo preview acetabular
NEW SCANDAL VIDEO
are you a teacherin the picture?
Why You?
Fwd: Photo
Windows Live User has shared photos with you



Screenshot 7: *Eine E-Mail, die versucht, neugierige Menschen auf infizierte Webseiten zu locken. Ein sehr berühmtes Beispiel einer solchen Mail war 2001 die Ankündigung der entblößten Anna Kurnikova.*

2.6 Die Rabatt-Masche (Malware)

Die Spam-Filter haben mit den unerwünschten Werbungen für billige blaue Pillen, unschlagbar billige Software, Schmuck-Rabatten und Diät-Versprechen einiges zu tun. In diesem Fall gilt die Regel: Finger weg von Angeboten, die zu schön klingen, um wahr zu sein.

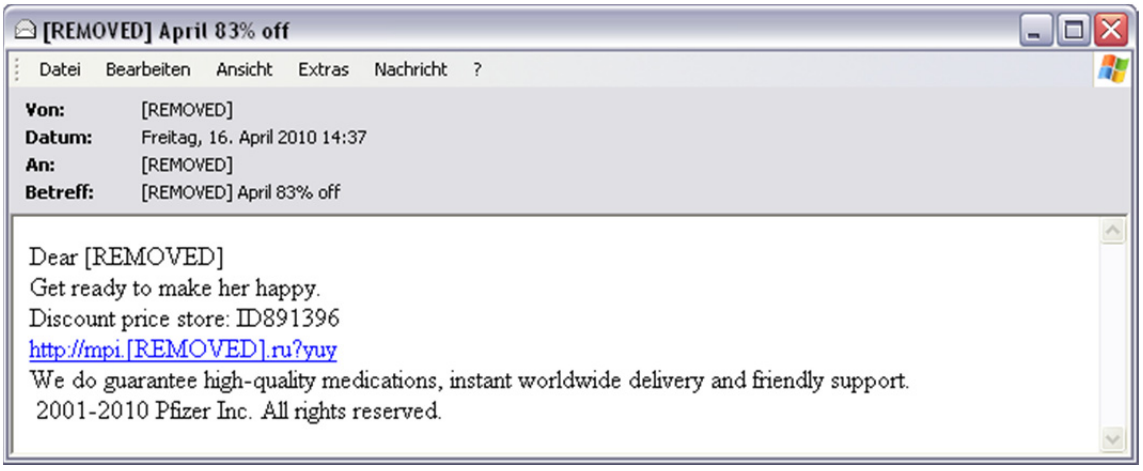
Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Gier

Die Gefahr: Der Klick auf den Link führt den Benutzer zu dubiosen Online-Shops. Hier warten die Cyberkriminellen nur darauf, dass der User seine wertvollen persönlichen Daten, Bankdaten oder Kreditkartendaten in ein Formular einträgt. Mit großer Wahrscheinlichkeit kann es auch zu einer Infektion des Rechners per Drive-by-Download kommen, wenn die verlinkten Seiten besucht werden – Die Folge davon sind unerwünschte Computerschädlinge, die allerlei Schaden auf dem Rechner des Opfers anrichten.

Betreff-Beispiele:

- Rabatte:
  - Bestellen Und 40% Sparen, Nur im Maerz
  - Angebote an Software Die Sie Freuen!
  - Dear […], 15-22 March 2010 +4833 78% 0FF.
  - Save thousands of dollars on original D&G accessories.
  - Bvlgari jewelry would look great on your girlfriend.
  - So Billig Wie Noch Nie - Teure Uhren
- Pharma:
  - Worlds only herball pill that corrects erectile dysfunction, strengthens erections and enhances libido
- Diät:
  - You can be another on the long lish of Quick Slim Success stories.
  - So hat Mado#nn^a abg&enommen
  - Sport ist echt Mord
  - Zu dick? Abspecken!



Screenshot 8: *Diese E-Mail lockt mit hohen Rabatten*

2.7 Akademische Grade und Titel-Masche (Phishing und Abzocke)

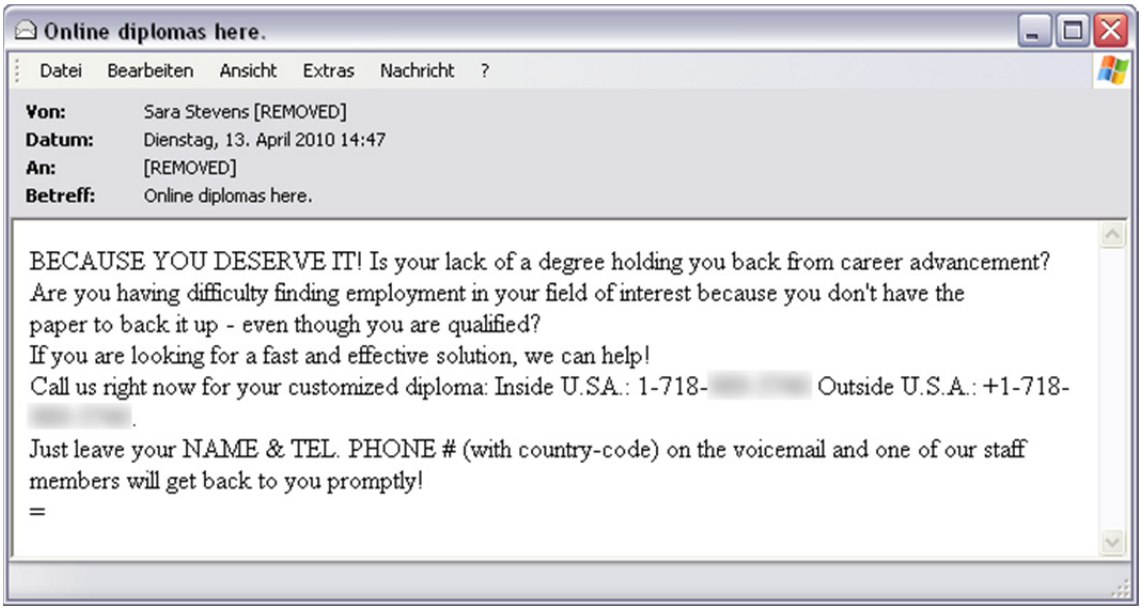
Die Werbetexte locken mit dem Versprechen, schnell und unkompliziert an einen akademischen Grad oder akademischen Titel zu gelangen – ganz ohne Studium und oft auch ohne Abschlussarbeit.

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Wunschdenken, Leichtgläubigkeit

Die Gefahr: Wer sich bei den angegebenen Telefonnummern oder E-Mailadressen meldet, muss zunächst einmal viele persönliche Daten angeben und gibt daher kostbare Information preis. Wer dann sogar einen Titel bei diesem Anbieter erwirbt, verliert er mit großer Wahrscheinlichkeit das bezahlte Geld. Wer sich auf diese dubiosen Universitäts-Urkunden beruft und den erkauften Titel nutzt, macht sich in Deutschland nach § 132a des Strafgesetzbuches strafbar.

Betreff-Beispiele: Doctorate degree can be yours.
Online diplomas here.
Re: MBA- qualification & award
Get a diploma for a better job.



Screenshot 9: *Mit dieser E-Mail werden Universitätsabschlüsse zum Kauf angeboten, um Karrierechancen zu verbessern*

2.8 Online Casino-Masche (Phishing und Abzocke)

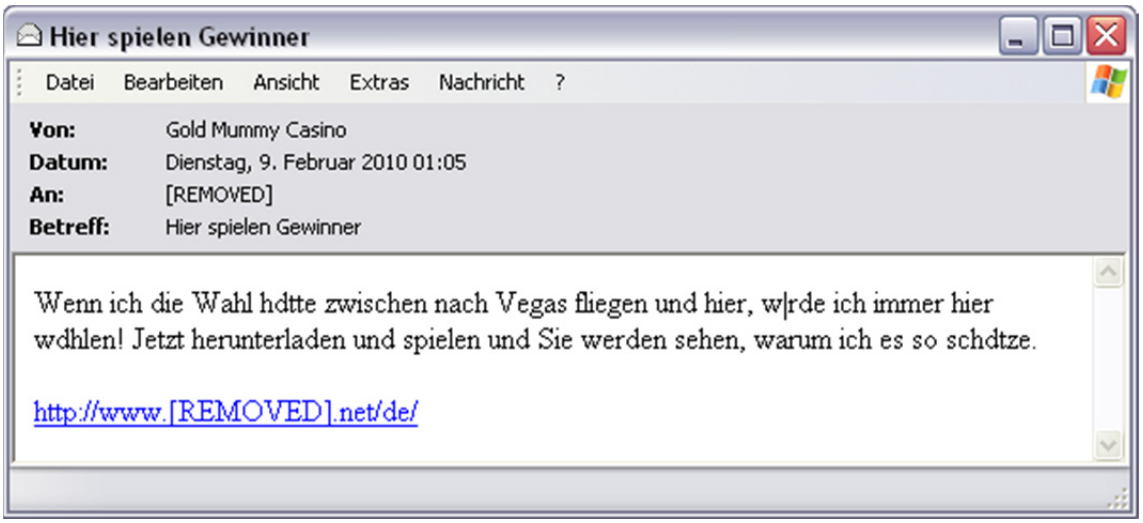
Online-Glücksspiel in jeglicher Form wird immer beliebter. Besonders hoch im Kurs steht seit längerem das Online-Pokern. Die Spam-Mails suggerieren, dass man mit wenig Einsatz viel Geld gewinnen kann – Als Starthilfe werden Boni für die erste Einzahlung versprochen oder schon vorhandenes Guthaben präsentiert.

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Wunschdenken, Gier, Neugier, Spieltrieb

Die Gefahr: Die Online-Casinos, die aus rechtlichen Gründen nicht in Deutschland beheimatet sind, verlangen eine erste Zahlung von den potentiellen Spielern – Dabei geben User oft unbedacht ihre wertvollen Bankdaten oder gar Kreditkartendaten in dubiosen Online-Spielstätten preis. Ein weiterer Gefahrenaspekt sind die Auszahlungen von Geld im Fall eines Gewinns, denn die Auszahlungen werden oft aus den verschiedensten Gründen verweigert und sowohl das eingezahlte Geld als auch das gewonnene Geld sind weg. Eine rechtliche Handhabe hat man dann nicht, da sowohl das Anbieten, als auch das Teilnehmen an Online-Glücksspielen in Deutschland seit Januar 2009 verboten ist.

Betreff-Beispiele: Behalten Sie die Gewinne nachdem Sie dieses fantastische Angebot erlebt haben
Genießen Sie unsere Spiele mit unserem tollen Startbonus
Großzügiger Willkommens-Bonus
Letzt Mahnung



Screenshot 10: *Eine Mail mit Casino-Lockrufen*

2.9 419er-Masche / Nigeria-Spam (Abzocke)

Unter diesem Begriff versteht man Vorschussbetrug-Mails. Dem Empfänger der Mail wird weißgemacht, dass er aus den unterschiedlichsten Gründen eine größere Summe Geld erhalten soll – Beispielsweise als Erbe, als Dank für die Verwaltung von Angelegenheiten oder auch als Gewinner eines angeblichen Gewinnspiels. Andere Szenarien setzen darauf, dass der Empfänger eine wohltätige Funktion einnimmt und einem Wohnungssuchenden oder einem herrenlosen Tier oder ähnlich hilft – natürlich auch finanziell. Einzig notwendige Handlung zum Erhalt des Geldes/zur Mithilfe sei die Kontaktaufnahme mit der in der Mail genannten Person.

Die Bezeichnung „419-Scam" für diese Art von Spam entstand durch den Bezug zum nigerianischen Strafrecht, das unter Artikel 419, in Kapitel 38[5], die Sachverhalte und Strafen für Betrügereien und Schwindeleien erläutert.

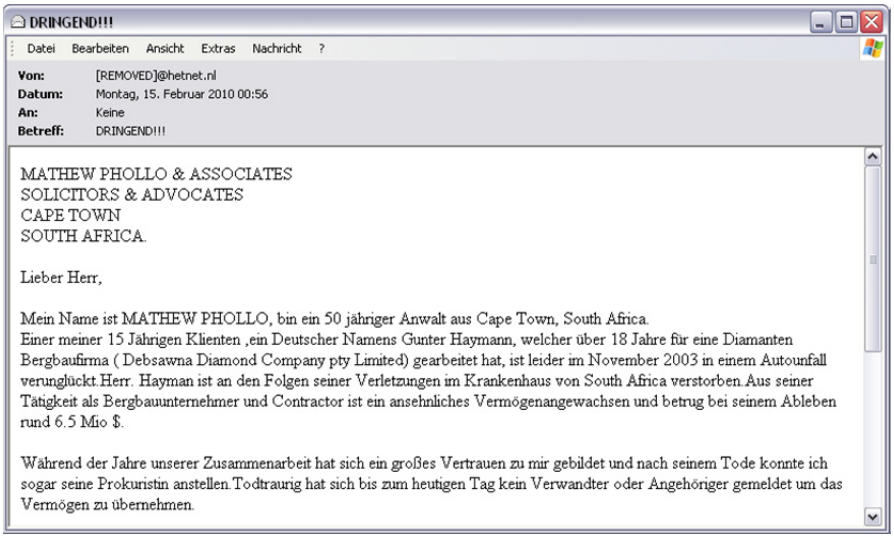
In Deutschland liegen die Schäden bei mindestens 522 Millionen US-Dollar und in den USA bei 2.110 Millionen US-Dollar als Verlust durch 419er-Spam und seine Folgen im Jahr 2009.[6]

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Gier, Leichtgläubigkeit

Die Gefahr: Wenn der Erstkontakt zu Stande gekommen ist, wird dem Opfer die große Summe Geld weiter schmackhaft gemacht. Jedoch würde zur Anweisung des Geldes auf das Konto des Opfers zunächst ein Betrag X benötigt, der vom Opfer z.B. auf ein Western Union Konto ins Ausland überwiesen werden muss. Dann kommen fingierte Zusatzkosten für Anwälte, Behördengänge, Urkunden, etc. dazu. Das Geld, das vom Opfer (in mehreren Schritten) überwiesen wird, ist unwiederbringlich weg und die eigentlich versprochene Geldsumme wird nie ausgezahlt.

Betreff-Beispiele: DRINGEND!
Reliable Partnership needed
NEED COMFIRMATION OF ACCEPTANCE
Your Notification Letter !!!


DRINGEND!!!

Datei Bearbeiten Ansicht Extras Nachricht ?

Von: [REMOVED]@hetnet.nl
Datum: Montag, 15. Februar 2010 00:56
An: Keine
Betreff: DRINGEND!!!

MATHEW PHOLLO & ASSOCIATES
SOLICITORS & ADVOCATES
CAPE TOWN
SOUTH AFRICA.

Lieber Herr,

Mein Name ist MATHEW PHOLLO, bin ein 50 jähriger Anwalt aus Cape Town, South Africa.
Einer meiner 15 Jährigen Klienten ,ein Deutscher Namens Gunter Haymann, welcher über 18 Jahre für eine Diamanten Bergbaufirma (Debsawna Diamond Company pty Limited) gearbeitet hat, ist leider im November 2003 in einem Autounfall verunglückt.Herr. Hayman ist an den Folgen seiner Verletzungen im Krankenhaus von South Africa verstorben.Aus seiner Tätigkeit als Bergbauunternehmer und Contractor ist ein ansehnliches Vermögenangewachsen und betrug bei seinem Ableben rund 6.5 Mio $.

Während der Jahre unserer Zusammenarbeit hat sich ein großes Vertrauen zu mir gebildet und nach seinem Tode konnte ich sogar seine Prokuristin anstellen.Todtraurig hat sich bis zum heutigen Tag kein Verwandter oder Angehöriger gemeldet um das Vermögen zu übernehmen.

Screenshot 11: *Großartige Versprechen, ohne erkennbaren Bezug zur eigenen Person, dafür aber mit sprachlichen Nachlässigkeiten*

[5] http://www.nigeria-law.org/
[6] Ultrascan Advanced Global Investigations (2010), „419 Advance Fee Fraud Statistics 2009" S. 29

2.10 Job-Masche (Malware und Abzocke)

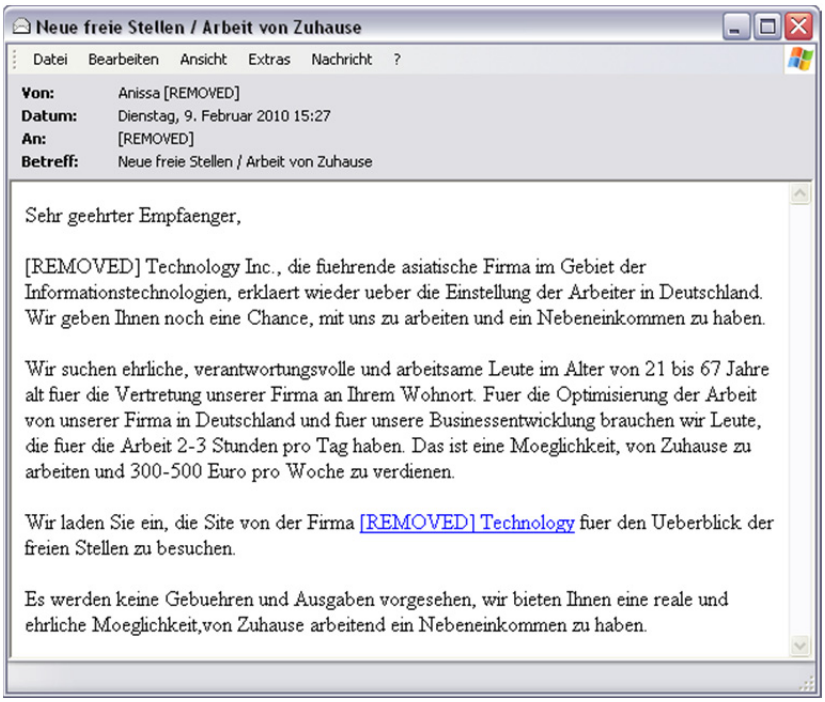
Die Versprechungen der Job-Mails preisen gutbezahlte Stellen (in namhaften Firmen) an, für die man wenig arbeiten muss. Die Gehälter seien hoch, die Arbeitszeit niedrig und der Arbeitsplatz sei oft sogar das heimische Wohnzimmer. Diese Aussichten sind gerade in der aktuell wirtschaftlich schwierigen Zeit ein effektives Lockmittel. Diese Masche kann unter anderem Teil einer 419-Scam Attacke sein.

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Wunschdenken, Selbstliebe

Die Gefahr: Manchmal werden diese Mails mit Anhängen verschickt, die den Rechner nach dem Öffnen mit Würmern infizieren und so für eine Weiterverbreitung der Job-Spam-Mails sorgen. Neben der technischen Gefahr lauert jedoch noch eine andere: Die angebotenen Jobs dienen oft der Geldwäsche oder der Weitergabe von illegal erworbenen Waren: Häufig ist die Benutzung eines Privatkontos eines der Hauptkriterien in der Jobbeschreibung und nicht selten macht sich ein leichtgläubiger Jobsuchender bei den Praktiken der Betrüger mit seinem Privatkonto der Geldwäsche bzw. der Hehlerei schuldig. Auch Identitätsdiebstahl ist nicht ausgeschlossen, wenn man den Betrügern z.B. zum Zwecke eines angeblichen Vertragsschlusses alle möglichen persönlichen Daten übermittelt.

Betreff-Beispiele: Stellenangebot. Vertrag. Teilzeit / Vollzeit. 8 Jahre in Business
Verbraucherservice/Stellenangebot/UPS/MBE
Nebenjob
Arbeiten Sie mit uns
Sie koennen eingestellt werden
Organisation sucht Kollegen
Management such Arbeitskollegen



Screenshot 12: *Eine Job-Scam E-Mail, die versucht, ahnungslose User in die Falle zu locken*

2.11 Russian Bride-Masche (Abzocke)

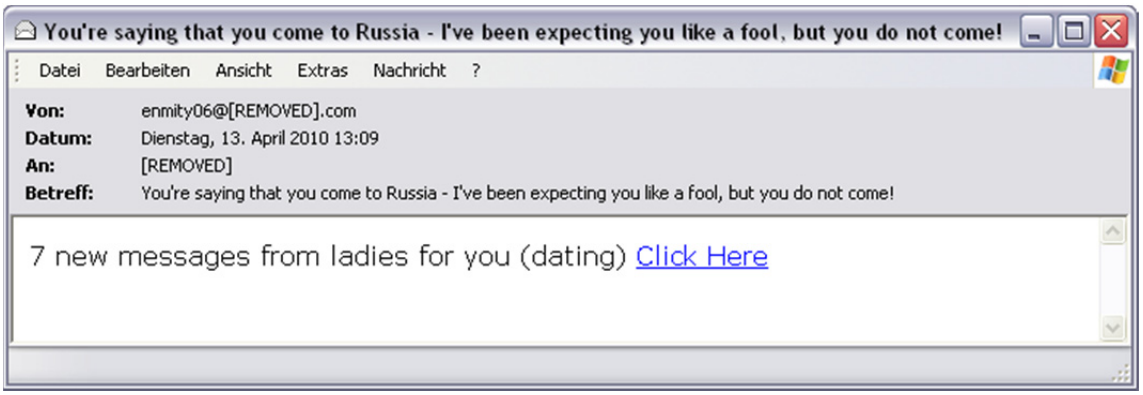
Diese Mails versprechen die große Liebe oder auch nur ein schnelles Liebes-Abenteuer mit, klischeebehaftet, meist jungen und blonden Frauen aus Russland. Die Damen würden schon lange auf die Rückantwort warten und würden den Angebeteten doch endlich treffen und/oder heiraten wollen. Solche Dates werden auch zur Geldwäsche genutzt. Der Verliebte wird dazu gebracht Waren weiterzuleiten und fremdes Geld über sein Konto zur Geliebten zu überweisen, damit sie ihn besuchen kann. Nicht selten benutzten 419-Scammer diese Masche.

Die Zielgruppe: Jeder Internetnutzer, jedoch hauptsächlich westeuropäische Single-Männer

Psychologische Ansatzpunkte: Lust und Liebe, Gegenseitigkeit

Die Gefahr: Antwortet man(n) auf diese Mail und stellt erst einmal der Kontakt zu den angeblichen Single-Frauen her, dreht sich das Thema relativ schnell um Geld, Visa und Heirat. Die Geliebte braucht Geld, um auszureisen, Taschengeld, Schmiergeld und noch mehr Geld – transferiert auf ein anonymes Bargeld-Konto. Überweist der gutgläubige Herr das Geld, wird er es nicht wiedersehen und auch seine Angebetete wird er sehr wahrscheinlich nie real zu Gesicht bekommen.

Betreff-Beispiele: You have new mail from Olga 26 y.o. Russia, dating
Meet Russian women here.
Still single?look at my profile, Olga from Russia
Want to know what the real Russian girls love and warmth?
Russian beauties are waiting.



Screenshot 13: *Eine von vielen Lock E-Mails mit Dating-Charakter*

2.12 Lotterie-Masche (Abzocke)

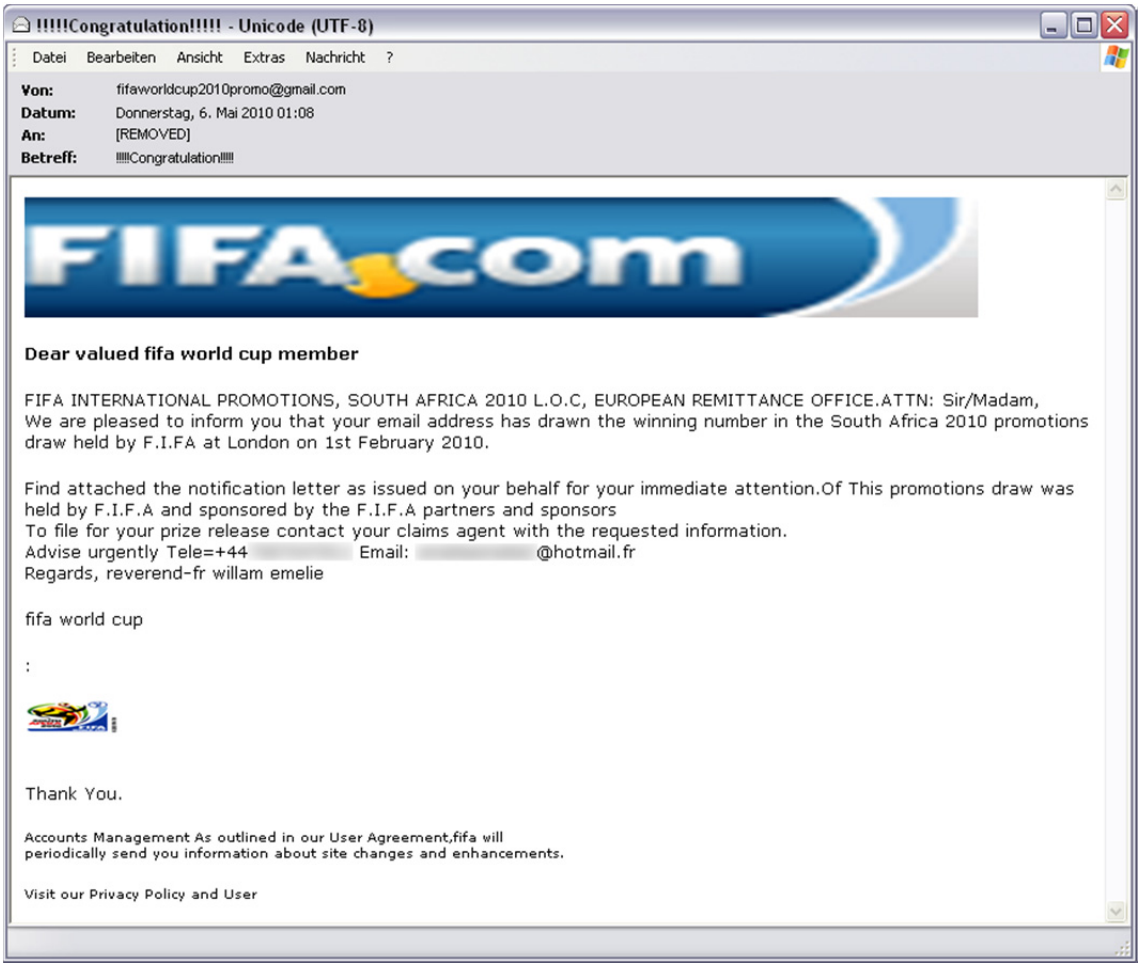
Dem Empfänger dieser Mails wird suggeriert, dass er einen hohen Geldbetrag in Euro, Dollar oder einen anderen Währung gewonnen hätte. Man müsse sich lediglich unter Angabe einiger persönlicher Daten bei Person XY melden. Die Lotterien werden angeblich von namhaften Firmen durchgeführt und auch die beteiligten Banken sind weltweit bekannt. Auch diese Masche kann Teil einer Attacke nach dem Nigeria-Spam Prinzip sein.

Die Zielgruppe: Jeder Internetnutzer

Psychologische Ansatzpunkte: Gier, Wunschdenken

Die Gefahr: Um diesen Betrag überwiesen zu bekommen, muss der vermeintliche Gewinner zunächst Gebühren an die Betrüger übersenden – Meist an ausländische und/oder anonyme Bankkonten. Auf eine Gebühr folgt die nächste, das Opfer zahlt und zahlt und wird weder den Gewinn noch die gezahlten Gebühren je (wieder) zu Gesicht bekommen.

Betreff-Beispiele: REF NR. GOOGLE-0293856-2009
Your E-mail Address Won
NOTICE OF GRANT AWARD (Congratulations you are a winner)



Screenshot 14: *Eine angebliche Gewinnbenachrichtigung*

3 Tipps und Tricks

Um nicht Opfer einer der beschriebenen Maschen zu werden, sollten folgende Punkte beachtet werden:

3.1 Nützliche Verhaltensregeln

- E-Mails von unbekannten Absendern sollten besonders misstrauisch behandelt werden. Erscheint eine Mail sehr eigenartig, dann gilt: Ignorieren, löschen, aber auf keinen Fall Anhänge öffnen oder URLs anklicken.
- Spam E-Mails sollten auch niemals beantwortet werden. Eine Antwort zeigt den Betrügern lediglich, dass die angeschriebene Adresse tatsächlich gültig ist.
- Es sollten keine persönlichen Informationen und/oder Bankdaten preis gegeben werden – Weder per E-Mail, noch auf dubiosen Webseiten.
- Es sollte keinesfalls Geld an Unbekannte überwiesen werden.
- Die eigene primäre E-Mail Adresse sollte nicht unbedacht online in z.B. Foren und Gästebüchern publiziert werden, da sie dort für Betrüger abgreifbar ist. Es hilft, sich für diesen Zweck eine Nebenadresse anzulegen.

3.2 Technische Maßnahmen

- Eine Sicherheitslösung für den Computer mit integrierter Anti-Spam Funktion schützt den PC schon vor Eintreffen der Mails durch Filter.
- Das Öffnen von Dateianhängen, vor allem von unbekannten Absendern, birgt Risiken. Anhänge sollten zunächst mit einem AntiViren Programm gescannt werden und ggf. ungeöffnet im Papierkorb landen.
- Links in E-Mails sollten keinesfalls unbedacht angeklickt werden. Man sollte die URL prüfen. Viele E-Mail-Programme erlauben es, das eigentliche Ziel der Verlinkung zu sehen, wenn man die Maus über den sichtbaren Link bewegt, ohne ihn jedoch anzuklicken – die sogenannte Mouseover Funktion.

4 Glossar

Bot: Bots sind kleine Programme, die meist unbemerkt im Hintergrund auf den Rechnern der Opfer laufen und dort je nach Funktionsumfang diverse Dinge erledigen – von DDoS-Attacken über E-Mail-Spam bis zum Mitlesen von Tastatureingaben und vielem mehr. Der Funktionsumfang ist primär eine Frage, wie viel Geld man für einen Bot anlegen möchte. Bots mit einem sehr großen Umfang sind naturgemäß teurer als eher einfache Bots, die nur wenig können. Verkauft werden sie unter anderem in Untergrundforen.

Botnetz: Ein Botnetz ist ein Verbund aus so genannten Zombie-PCs. Zur Verwaltung des Botnetzes werden Command-and-Control-Server (C&C Server) genutzt. Botnetze werden unter anderem dafür benutzt, gezielte Überlastangriffe auf Webserver zu starten (DoS- und DDoS-Attacken) und um Spam zu versenden.

Social Engineering: Als Social Engineering werden Überredungstaktiken bezeichnet, mit denen ein Hacker einen Anwender dazu veranlasst Informationen preiszugeben, die er dazu nutzen kann, dem Anwender oder seiner Organisation Schaden zuzufügen. Oft wird dazu Autorität vorgespiegelt, um Zugangsdaten oder Passwörter zu erlangen.

Spam: Mitte der 90er Jahre bezeichnet Spam die übermäßige Verbreitung der gleichen Nachricht in Usenet-Foren. Der Begriff selbst geht auf einen Sketch von Monty Python zurück. Mittlerweile verwendet man Spam in mehreren Bedeutungen. Als Oberbegriff steht Spam für massenhaft unaufgefordert zugesandte E-Mails. In einem engeren Sinn beschränkt sich der Begriff Spam auf Werbemails; das heißt: Würmer, Hoaxes, Phishing-Mails und AutoResponder werden nicht dazugezählt.

Zombie-PC: Als Zombie bezeichnet man einen PC, der sich über eine Backdoor von einem Außenstehenden fernsteuern lässt. Analog zum filmischen Vorbild gehorcht der Zombie-PC nur noch dem verborgenen Meister und führt dessen oftmals verbrecherische Befehle aus. Viele Zombies werden zu so genannten Botnetzen zusammengefasst.