G Data
White paper 1/2011

Dangerous e-mail

Sabrina Berkenkopf & Ralf Benzmüller
G Data SecurityLabs

Whitepaper_1-2011

Go safe. Go safer. **G Data.**

Contents

1 Introduction

1.1 E-mail - a quick overview

Nowadays, e-mail is an everyday medium of communication in the workplace and at home that we can no longer imagine doing without. Sending e-mails is extremely cheap and fast, all this with a global reach.

To work with e-mail, users use programs installed on their computers (e-mail clients) or retrieve them in a browser. Of course, popular functions such as this attract fraudsters, who can exploit technical vulnerabilities.

The send-and-receive processes for e-mails take place in the background and ideally the user is not involved in the process. The protocol for sending e-mails is called SMTP, Simple Mail Transfer Protocol. E-mails are received via POP3 (Post Office Protocol, version 3) or IMAP (Internet Message Access Protocol).

The composition of electronic mail is subdivided in a way that is similar to postcards. On the one hand, the information part (header) displays sender and recipient data, the date and subject, etc. The second component is the body text that conveys the actual message.

As there is no authentication of the plain text when sending an e-mail via SMTP, it is at this stage that fraud can take place. For example, it is possible to change the sender address in the header and thus deceive the recipient by using a false identity. Content can also be easily manipulated.

However, all the positive aspects of e-mail that have already been mentioned have another side to them. E-mail inboxes are still overflowing, with the majority of e-mail received being unsolicited mail containing dubious advertising offers, dream job offers, flirtatious invitations and the like. The thing that annoys the computer users around the world on a daily basis is ☞spam[1]. These unsolicited mass e-mails are not just irritating because of their large numbers - they can also be dangerous.

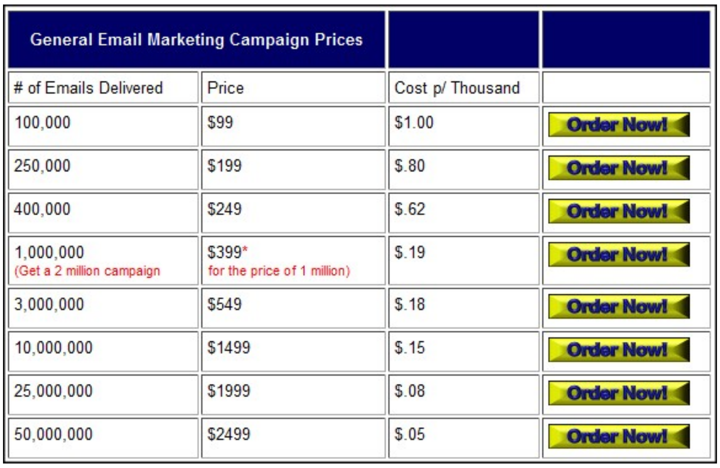
Fraudulent and dangerous e-mail comes in all sorts of different forms - unwanted advertising, phishing, malware with file attachments, or links to primed websites. Before describing in detail the specific processes and scams used by scammers in the following section, we would like to shed a little more light on the background to them.

[1] Explanations for specialist terms marked with ☞ are contained in the glossary

1.2 Who is behind the spam?

Cyber criminals continue to to make extensive use of the the medium of mass e-mail for fraudulent activities. The mass distribution of unsolicited e-mail, or spam for short, is one of the best known branches of the cyber criminals' black economy. In the fourth quarter of 2010, an average of 83% of all the e-mail traffic in the world was spam, which is the equivalent of an average of 142 billion spam e-mails per day.[2]

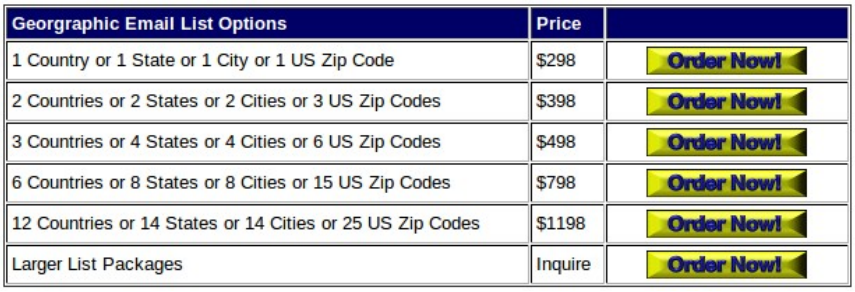
Much of its popularity can be explained by the attractive cost-benefit ratio. At present, it costs somewhere between 399 and 800 US dollars to send 1,000,000 spam e-mails, with various service providers. Offers also include 2,000,000 e-mails for the price of 1,000,000.



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: *Price list for a bulk e-mail distribution service on the Internet. These prices are for sending spam e-mail generally, without specifying target groups.*

Address lists with target groups are also available on the Internet or can be purchased directly from bulk e-mail distribution services. If necessary, they can be specifically customised. Therefore, it is possible to purchase addresses sorted by target group - e.g. specific lists of online gamers, or people form a specific region, and many other categories.



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: *Surcharges for targeted e-mail distribution - in this case for localised target groups*

The spam e-mail is primarily sent via ☞botnets. For example, it takes a botnet operator with a rather small botnet of some 20,000 ☞zombie computers operating at 2 e-mails per second per active ☞bot, just 25 seconds to execute a job involving 1,000,000 e-mails. Therefore, based on these figures alone, the operator of a relatively small botnet can earn up to US$ 115,200 per hour.

[2] Commtouch, Q4 2010 Internet Threats Trend Report. Figures based on unfiltered data flow, excluding internal company traffic

1.3 Psychological basis of spam

Regardless of the format that the e-mail streaming into your digital inbox takes, the majority of e-mail fraudsters' tricks are based on ☞social engineering. This involves exploiting emotions, opinions, attitudes and behaviour patterns in a targeted manner, in order to lure e-mail recipients into traps. Such attempts to use social manipulation to access confidential data exploit a kind of "human security hole".

To operate social engineering effectively, fraudsters use (bogus) sender names, subject lines and e-mail content. However, attachment file names, duplicate file endings and popular icons or domain names with links can also be used to disguise an attempt at a scam. In a report in 2005, Jordan and Goudey[3] named the following 12 psychological factors as those that the most successful worms between 2001 and 2004 were based on:

- Inexperience
- Curiosity
- Greed
- Diffidence
- Courtesy
- Self-love
- Credulity
- Desire
- Lust
- Dread
- Reciprocity
- Friendliness

A year later M. Braverman[4] expanded on this:

- Generic conversation: Short statements, such as "cool", etc.
- Virus warnings and software patches
- Malware discovered on the PC
- Virus check reports at the end of the mail
- Information or messages about accounts: e.g. the telecom Trojan, which identifies itself as an exaggerated telephone bill
- e-mail delivery error messages
- Physical attraction
- Accusatory: e.g. the BKA Trojan which purports to have found illegal files
- Current events
- Free stuff: some people throw caution to the wind as soon as there is any mention of getting something for free

[3] see Jordan, M., Goudey, H. (2005) "The Signs, Signifiers and Semiotics of the Successful Semantic Attack". In: Proceedings of the EICAR 2005 Conference, pp.344 - 364.

[4] see Braverman (2006) "Behavioural Modelling of Social Engineering-based Malicious Software". In: Proceedings of Virus Bulletin Conference 2006, pp.15-22.

2 Miscellaneous scams

2.1 The re-register scam (data theft, malware)

The e-mail suggests that an online system or program has been updated and the customer data must now be immediately(!) updated so the service features can continue to be used without a problem. The link to the supposed updating website is provided directly in the e-mail. It often takes a careful look at the address being linked to to see that it is not the original address. In fact, the website to which the link connects is often a replica of the original and, based on its appearance, it is hard to identify as being a fake.

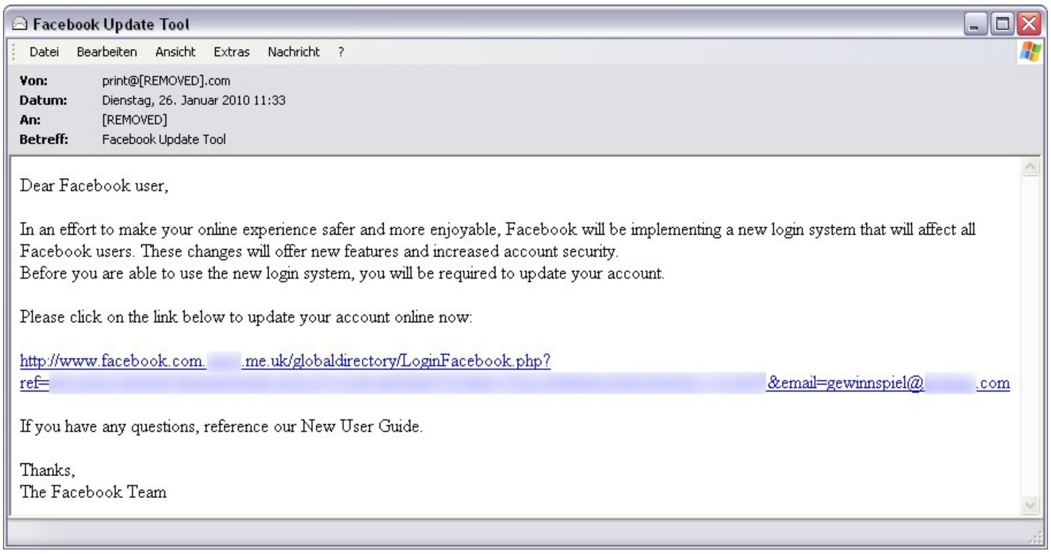
The target group: Any Internet user, but especially customers of a wide range of banks and paid-for services, plus users of popular software, social networks, online games, free e-mail services and web applications.-

Psychological starting points: Inexperience, credulity, security awareness

The risk: Fraudsters acquire valuable information about individuals, if trusting people visiting the bogus website via the link enter the requested data. Depending on the type and presentation of the website, this can range from their name and address to their credit card number and PIN code. Abuse of this data is planned from the start!

Authority plays an important role in this scam, as inexperienced users will easily let themselves be lured into clicking and carrying out other actions by bogus senders and orders from a known agency.

Subject line examples: 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



Von: print@[REMOVED].com
Datum: Dienstag, 26. Januar 2010 11:33
An: [REMOVED]
Betreff: Facebook Update Tool

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.

Please click on the link below to update your account online now:

http://www.facebook.com.[redacted].me.uk/globaldirectory/LoginFacebook.php?ref=[redacted]&email=gewinnspiel@[redacted].com

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

***Screenshot 3:** E-mail with a request to update via a link. This link does not connect to Facebook but rather to a site with the second level domain .me.uk*

2.2 The irregular practices scam (phishing)

This scam leads potential victims to believe that there has been a problem with their account and it will now have to be immediately blocked. To stop it from being blocked, the user must immediately(!) enter his account data on a website being linked to.

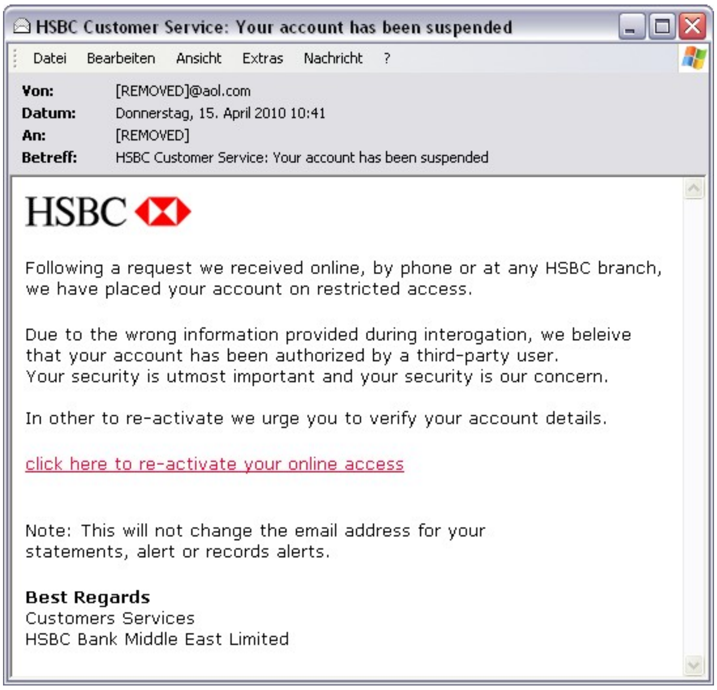
The target group: Any Internet user, but especially users of a wide range of banks and paid-for services, e-mail services etc.

Users of services whose only access control consists of a login name and password are particularly lucrative targets - especially if money can be transferred via the services or if they are of value to the underground economy (money-laundering, sending spam, sending stolen goods, etc).

Psychological starting points: Inexperience, diffidence and dread

The risk: As with the re-registration scam, phishing attacks specifically target personal data that is rich in content, with a specific focus on banking data of any kind. In this case, as with the update scam, acceptance of bogus authority is a criterion for the success of the attack.

Subject line examples: 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



Von: [REMOVED]@aol.com
Datum: Donnerstag, 15. April 2010 10:41
An: [REMOVED]
Betreff: HSBC Customer Service: Your account has been suspended

HSBC

Following a request we received online, by phone or at any HSBC branch, we have placed your account on restricted access.

Due to the wrong information provided during interogation, we beleive that your account has been authorized by a third-party user.
Your security is utmost important and your security is our concern.

In other to re-activate we urge you to verify your account details.

click here to re-activate your online access

Note: This will not change the email address for your statements, alert or records alerts.

Best Regards
Customers Services
HSBC Bank Middle East Limited

Screenshot 4: *A phishing e-mail imitating the official correspondence of a bank*

2.3 The greetings card scam (malware)

Fake greetings cards are distributed throughout the year; however they receive special attention from fraudsters and victims on celebratory days and holidays. There is a great temptation to look at the supposed greeting from "a friend", and this is precisely what the trap is relying on.

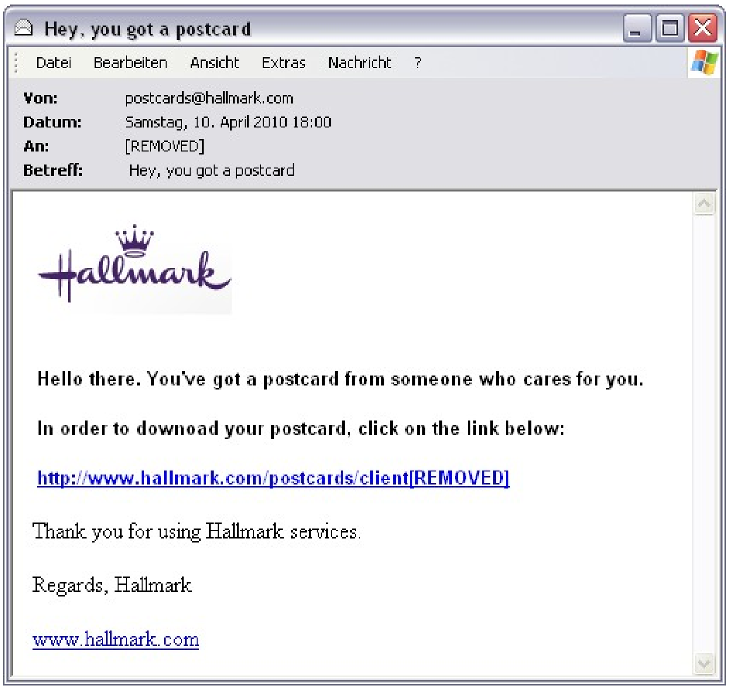
There are numerous types of e-mail: on the one hand, there are e-mails with attachments disguised as eCards that launch their attack as soon as they are opened. Then there are the e-mails that invite the user to visit a website to install a supposed codec or multi-media player, in order to display the supposed eCard. And finally there are the e-mails that launch an unnoticed drive-by infection when visiting a supposed greetings card website.

The target group: Any Internet user

Psychological starting points: Curiosity, friendliness

The risk: Like the so-called "Look at this" scam, the user is exposed to malicious code as soon as he visits a site, opens an attachment or installs the disguised executable program. This provides opportunities for the malware to steal personal data and/or wreak further chaos.

Subject line examples: 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 !!!



Von: postcards@hallmark.com
Datum: Samstag, 10. April 2010 18:00
An: [REMOVED]
Betreff: Hey, you got a postcard

Hello there. You've got a postcard from someone who cares for you.

In order to downoad your postcard, click on the link below:

http://www.hallmark.com/postcards/client[REMOVED]

Thank you for using Hallmark services.

Regards, Hallmark

www.hallmark.com

***Screenshot 5:** The legitimate-looking e-mail contains a dangerous link - leading to an executable EXE file rather than the greetings card company's homepage*

2.4 The package-sending scam (malware and phishing)

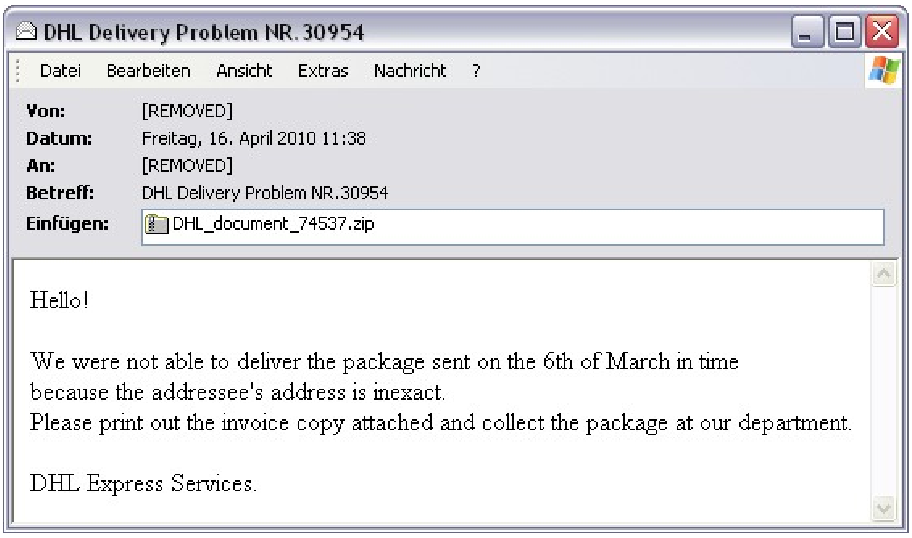
The recipient receives an e-mail with a message concerning an apparently failed attempt to send a package. To resolve the problem or acquire more information, the recipient is supposed to either open an attached file or click on a given link. Criminals frequently target customers of despatch companies where packages and parcels can be retrieved from a collection point at any time using a PIN. Internationally renowned despatch services are often used as an instrument for such phishing campaigns.

The target group: Any Internet user, but especially customers of popular despatch services.

Psychological starting points: Curiosity, greed, vigilance

The risk: If the user launches a file attachment in the e-mail, which is frequently disguised as a delivery note, he unintentionally installs malware on his computer such as password stealers, keyloggers, etc. that can dig out and forward personal data. Users fall into the phishing trap if they enter e.g. personal data and details regarding the package collection point on a bogus, albeit disguised and genuine-looking website for a despatch company. In this way cyber-criminals can acquire access data, steal packages delivered to the collection points and use the delivery point for sending criminally-acquired goods as well. Accounts for these collection points are used in the underground to send goods purchased using stolen bank data or credit cards. Finally, they can also be used for money-laundering, which is why they are sought after. Therefore, anyone who discloses his or her data by entering it on a fake login page can expect widespread damage.

Subject line examples: 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



Von: [REMOVED]
Datum: Freitag, 16. April 2010 11:38
An: [REMOVED]
Betreff: DHL Delivery Problem NR.30954
Einfügen: DHL_document_74537.zip

Hello!

We were not able to deliver the package sent on the 6th of March in time
because the addressee's address is inexact.
Please print out the invoice copy attached and collect the package at our department.

DHL Express Services.

Screenshot 6: *An e-mail with an infected attachment, disguised as an official document*

2.5 The "Look at this" scam (malware and advertising)

In this variant, the villains primarily rely on the trick of social engineering and make e-mail recipients curious about supposedly brand new offers on the Internet, apparently embarrassing images and videos of themselves or other subjects of interest.

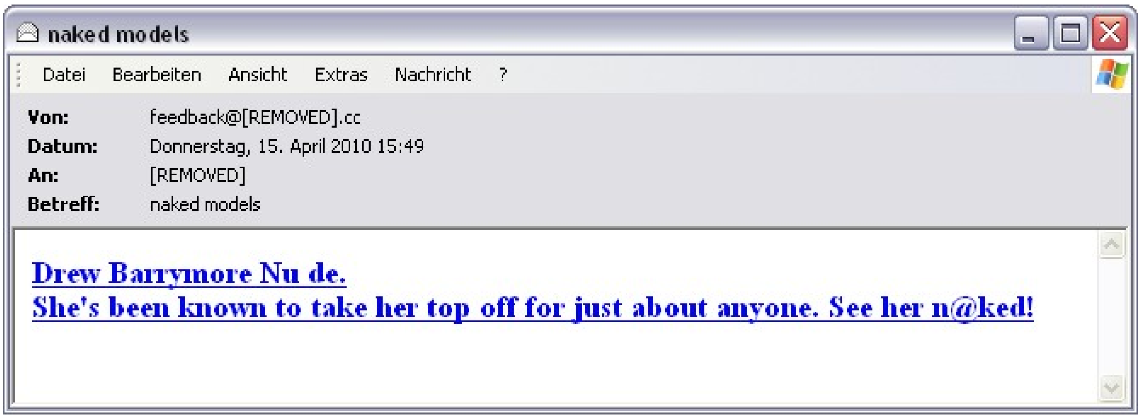
In this case, the malware is either lurking directly in the e-mail's infected attachment or on the website that the e-mail links to. The link mostly leads to a request to install a codec or a new executable program that will install malware on the computer when run.

The target group: Any Internet user, but especially social network users

Psychological starting points: Curiosity, lust

The risk: In this variant the victim is attacked with malware and can find his computer infected with various malicious programs. These programs can then read passwords, steal credit card data, attach the PC to a botnet and much more.

Subject line examples: Scandal Britney Spears dead
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



Von: feedback@[REMOVED].cc
Datum: Donnerstag, 15. April 2010 15:49
An: [REMOVED]
Betreff: naked models

Drew Barrymore Nu de.
She's been known to take her top off for just about anyone. See her n@ked!

***Screenshot 7:** An e-mail attempting to lure curious people to infected websites. A very famous example of such an e-mail was the announcement about nude pictures of Anna Kournikova in 2001.*

2.6 The discount scam (malware)

Spam filters have their work cut out with unsolicited adverts for little blue pills, unbeatably cheap software, fantastic reductions and dieting promises. With all of these the rule is: if it looks too good to be true, it probably is.

The target group: Any Internet user

Psychological starting points: Greed

The risk: Clicking on the link will take the user to dubious online shops. Cyber-criminals are waiting here in the hope that the user will enter valuable personal data, bank data or credit card data into a form. In all probability the computer will become infected by a drive-by download as well when the site linked to is visited. The consequences of this are undesirable computer malware that will wreak all kinds of havoc on the victim's computer.

Subject line examples: Order And Save 40%, For March Only
Software Offers You Will Love!
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.
Cheaper Than Ever - Expensive Watches

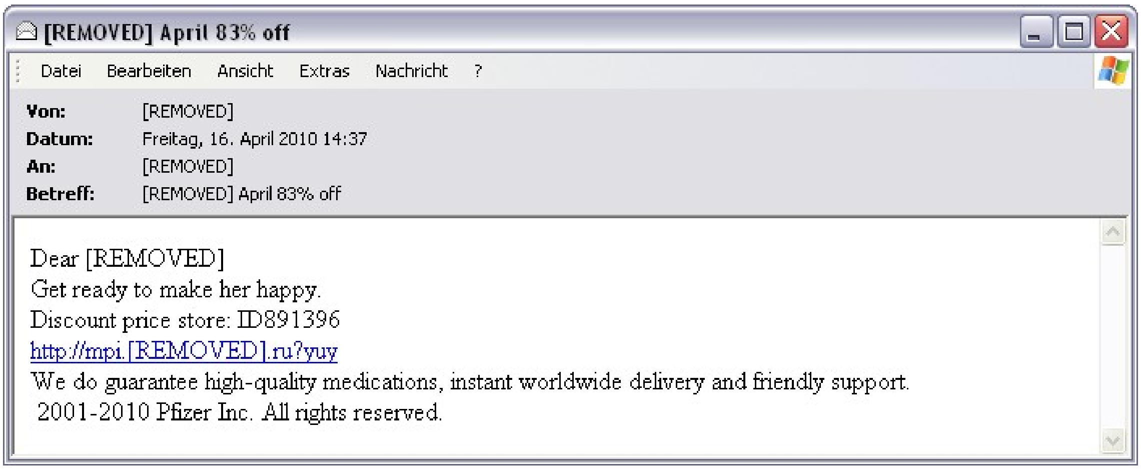
Reducti

Worlds only herball pill that corrects erectile dysfunction,
strengthens erections and enhances libido

Pharma

You can be another on the long lish of Quick Slim Success stories.
This Is How Mado#nn^a Lost Weight
Sport is Murder
Too Fat? Lose Weight!

Diet



Von: [REMOVED]
Datum: Freitag, 16. April 2010 14:37
An: [REMOVED]
Betreff: [REMOVED] April 83% off

Dear [REMOVED]
Get ready to make her happy.
Discount price store: ID891396
http://mpi.[REMOVED].ru?yuy
We do guarantee high-quality medications, instant worldwide delivery and friendly support.
2001-2010 Pfizer Inc. All rights reserved.

Screenshot 8: *This e-mail is using massive reductions to lure people in*

2.7 Academic degrees and titles scam (phishing and ripping off)

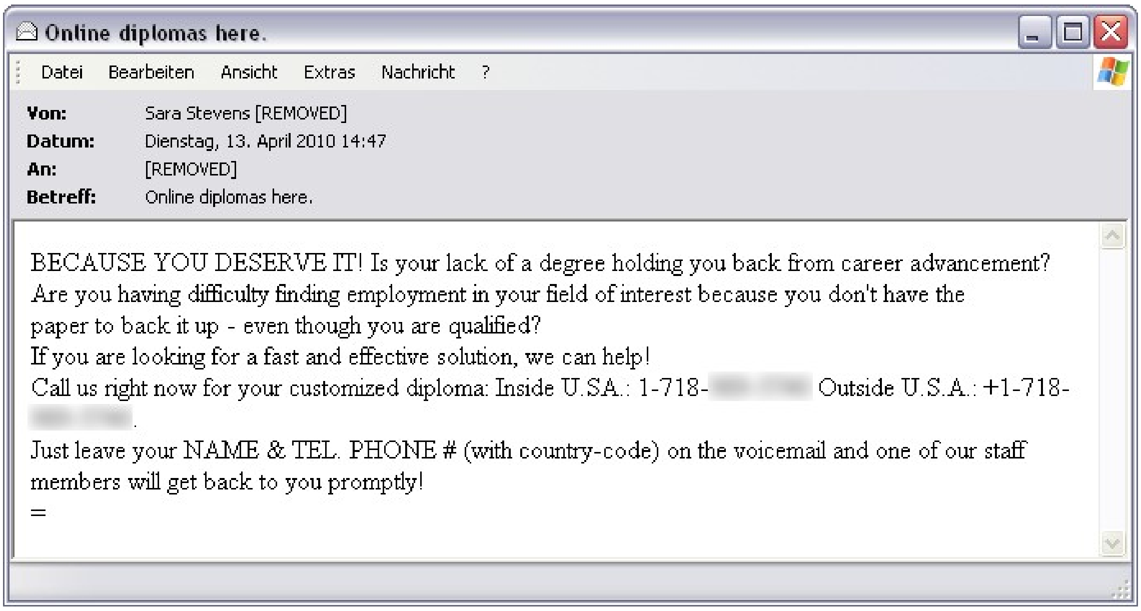
The advertising text lures people in with the promise of quickly and easily obtaining an academic degree or title - without any studying and usually without any final examination.

The target group: Any Internet user

Psychological starting points: Desire, credulity

The risk: Anyone who contacts the telephone numbers or e-mail addresses given must first enter a wealth of personal data, thereby disclosing valuable information. Anyone who then purchases even a title from such an outlet will more than likely lose the money they have paid out. Anyone who makes reference to dubious University qualifications like this and uses a purchased title is liable to prosecution in Germany under § 132a of the Penal Code.

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



Von: Sara Stevens [REMOVED]
Datum: Dienstag, 13. April 2010 14:47
An: [REMOVED]
Betreff: Online diplomas here.

BECAUSE YOU DESERVE IT! Is your lack of a degree holding you back from career advancement?
Are you having difficulty finding employment in your field of interest because you don't have the
paper to back it up - even though you are qualified?
If you are looking for a fast and effective solution, we can help!
Call us right now for your customized diploma: Inside U.S.A.: 1-718-[redacted] Outside U.S.A.: +1-718-
[redacted].
Just leave your NAME & TEL. PHONE # (with country-code) on the voicemail and one of our staff
members will get back to you promptly!
=

***Screenshot 9:** This e-mail offers University degrees for sale to improve career prospects*

2.8 Online casino scam (phishing and ripping off)

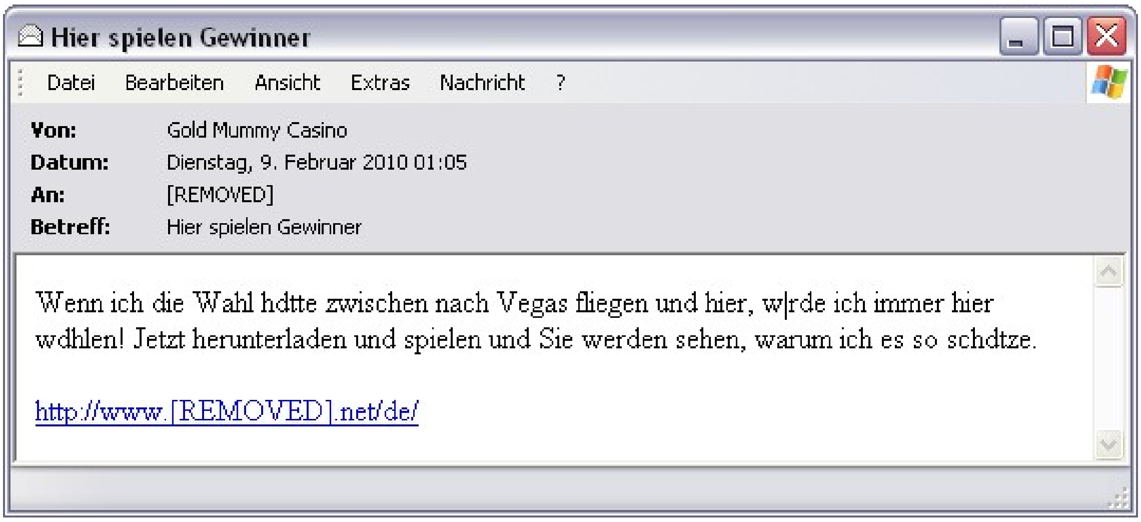
Online gambling of every kind is becoming more and more popular. Online poker has been especially highly rated for a long time. The spam e-mail suggests that a lot of money can be won for a small outlay. As an incentive, bonuses are promised with the first payment or credits already available are offered.

The target group: Any Internet user

Psychological starting points: Desire, greed, curiosity, play instinct

The risk: The online casinos, which for legal reasons cannot be based in Germany, demand an initial payment from potential players. In doing so, users often unintentionally disclose valuable bank data or even credit card data in dubious online gaming sites. A further danger is paying out money in the event of a win, because the payments are often denied for various reasons so both the money paid out and the winnings are lost. There is no legal recourse here, as both the provision of and participation in online gambling have been banned in Germany since January 2009.

Subject line examples: Take your winnings after experiencing this fantastic offer
Enjoy playing our games with our fantastic start bonus
Generous welcome bonus
Final reminder



Von: Gold Mummy Casino
Datum: Dienstag, 9. Februar 2010 01:05
An: [REMOVED]
Betreff: Hier spielen Gewinner

Wenn ich die Wahl hdtte zwischen nach Vegas fliegen und hier, w|rde ich immer hier wdhlen! Jetzt herunterladen und spielen und Sie werden sehen, warum ich es so schdtze.

http://www.[REMOVED].net/de/

***Screenshot 10:** An e-mail luring people to a casino*

2.9 419 scam / Nigerian spam (ripping off)

This term refers to advance payment scam e-mails. The e-mail recipient is led to believe that he is entitled to receive a huge sum of money for some reason, for example inheritance, a thank you for handling various transactions or winnings from a supposed competition. Other scenarios are based on the recipient undertaking a benevolent function and helping a homeless person or an abandoned animal, etc. - for money, of course. The only action necessary to receive the money/provide aid is to contact the person named in the e-mail.

The name "419 scam" for this type of spam came from the reference to Nigerian penal law where article 419 in section 38[5] explains the circumstances and penalties for fraud and swindling.

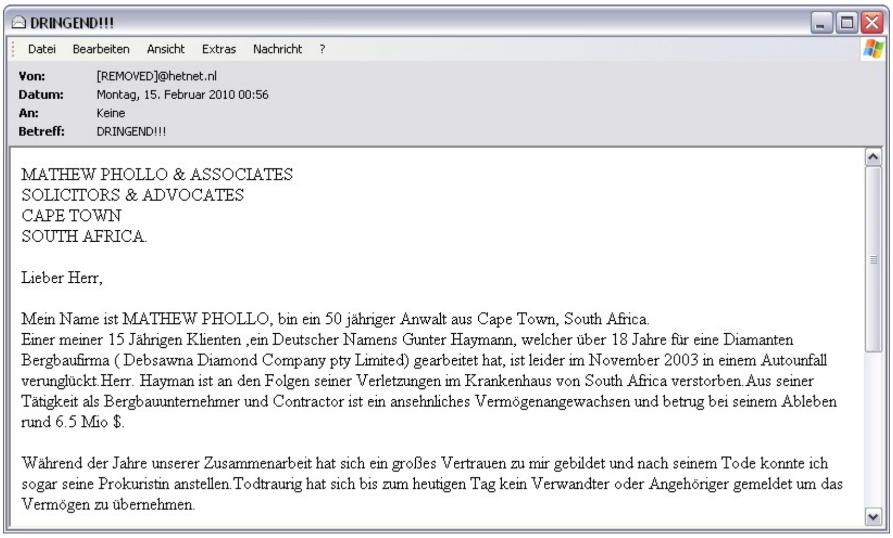
The damage caused by 419 spam and its consequences in 2009 amounts to losses of at least US$ 522 million in Germany and US$ 2,110 million in the USA.[6]

The target group: Any Internet user

Psychological starting points: Greed, credulity

The risk: Once initial contact has been made, the large sum of money is made even more appealing to the victim. However, in order to transfer the money to the victim's account, an amount of X is first required that must be transferred by the victim to a Western Union account abroad. Fictitious extra costs then follow, for lawyers, visits to the authorities, certificates etc. The money sent by the victim (in multiple stages) is irretrievably lost and the actual sum of money promised is never paid out.

Subject line examples: URGENT!
Reliable Partnership needed
NEED COMFIRMATION OF ACCEPTANCE
Your Notification Letter !!!



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:** Grandiose promises with no recognisable reference to an actual person, but using poor language skills*

[5] http://www.nigeria-law.org/

[6] Ultrascan Advanced Global Investigations (2010), „419 Advance Fee Fraud Statistics 2009" S. 29

2.10 Job scam (malware and ripping off)

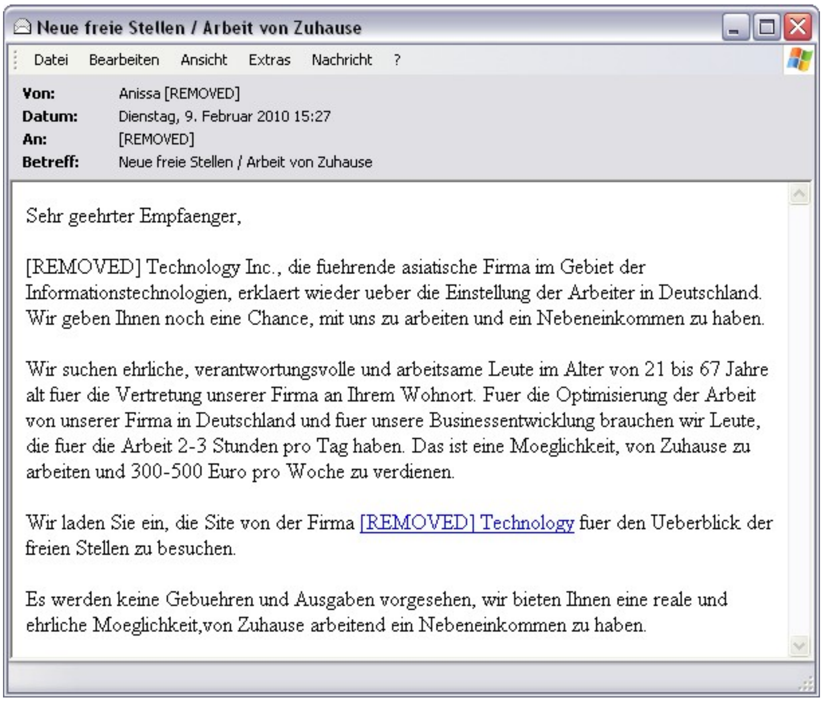
The promises in job e-mails talk up well-paid positions (with well-known companies) for doing little work. The salaries are high, the working hours low and the location is often your own living room. Such prospects are an effective attraction in these straitened economic times. This scam can be part of a 419 scam attack.

The target group: Any Internet user

Psychological starting points: Desire, self-love

The risk: Sometimes these e-mails are sent with attachments that, once opened, infect the computer with worms and are used to continue distributing the job spam e-mails. However, there is another risk lurking behind the technical one: the jobs being offered are often for money-laundering purposes or forwarding illegally purchased goods. Frequently, the use of a private account is one of the main criteria in the job description and all too often gullible job seekers make themselves guilty of money-laundering or dealing in stolen goods through the fraudsters' practices. Identity theft is another possibility, if all kinds of personal data are handed over to the fraudsters, e.g. for the purposes of completing a supposed contract.

Subject line examples: Job offer. Contract. Part-time/Full-time. 8 years in business
Consumer service/Job offer/UPS/MBE
Sideline
Work for us
You can be hired
Organisation seeks colleagues
Management seeking work colleagues



Von: Anissa [REMOVED]
Datum: Dienstag, 9. Februar 2010 15:27
An: [REMOVED]
Betreff: Neue freie Stellen / Arbeit von Zuhause

Sehr geehrter Empfaenger,

[REMOVED] Technology Inc., die fuehrende asiatische Firma im Gebiet der Informationstechnologien, erklaert wieder ueber die Einstellung der Arbeiter in Deutschland. Wir geben Ihnen noch eine Chance, mit uns zu arbeiten und ein Nebeneinkommen zu haben.

Wir suchen ehrliche, verantwortungsvolle und arbeitsame Leute im Alter von 21 bis 67 Jahre alt fuer die Vertretung unserer Firma an Ihrem Wohnort. Fuer die Optimisierung der Arbeit von unserer Firma in Deutschland und fuer unsere Businessentwicklung brauchen wir Leute, die fuer die Arbeit 2-3 Stunden pro Tag haben. Das ist eine Moeglichkeit, von Zuhause zu arbeiten und 300-500 Euro pro Woche zu verdienen.

Wir laden Sie ein, die Site von der Firma [REMOVED] Technology fuer den Ueberblick der freien Stellen zu besuchen.

Es werden keine Gebuehren und Ausgaben vorgesehen, wir bieten Ihnen eine reale und ehrliche Moeglichkeit,von Zuhause arbeitend ein Nebeneinkommen zu haben.

Screenshot 12: *A job scam e-mail trying to lure unsuspecting users into a trap*

2.11 Russian bride scam (ripping off)

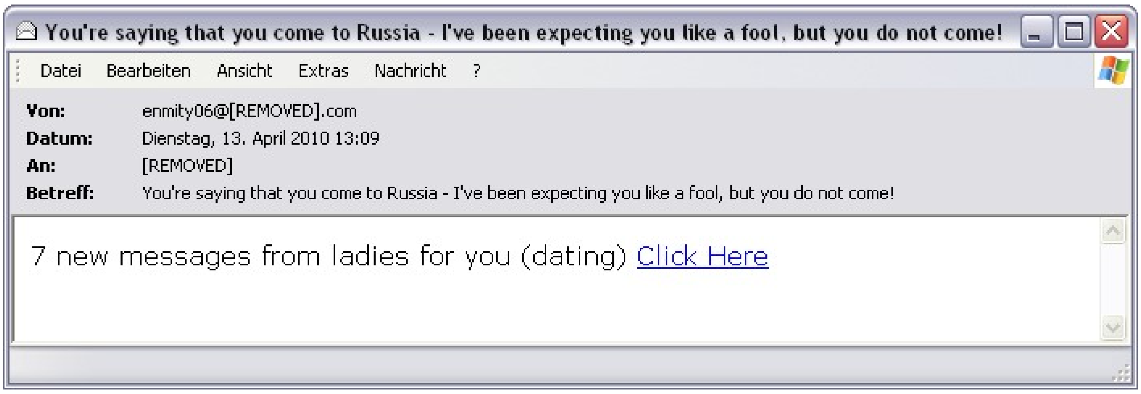
These e-mails promise true love or just a brief affair, usually with one of the proverbial young, blonde women from Russia. The women have been waiting for a response for a long time and ultimately want to meet or marry their beloved. Such dates are also used for money-laundering. The "lovebird" is asked to forward goods and transfer foreign money via his account to his "beloved", so she can visit him. 419 scammers often use this scam too.

The target group: Any Internet user, but especially single western European men

Psychological starting points: Lust, reciprocity

The risk: Anyone who responds to the e-mail and initiates contact with the supposed single women will soon find that the subject quickly turns to money, visas and marriage. The lady needs money to travel, spending money, money for bribes and yet more money - transferred to an anonymous cash account. If the gullible man sends the money, he won't see it again and he will probably never actually set eyes on his "beloved".

Subject line examples: 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.



You're saying that you come to Russia - I've been expecting you like a fool, but you do not come!

Von: enmity06@[REMOVED].com
Datum: Dienstag, 13. April 2010 13:09
An: [REMOVED]
Betreff: You're saying that you come to Russia - I've been expecting you like a fool, but you do not come!

7 new messages from ladies for you (dating) Click Here

***Screenshot 13:** One of many bait-mails based around dating*

2.12 Lottery scam (ripping off)

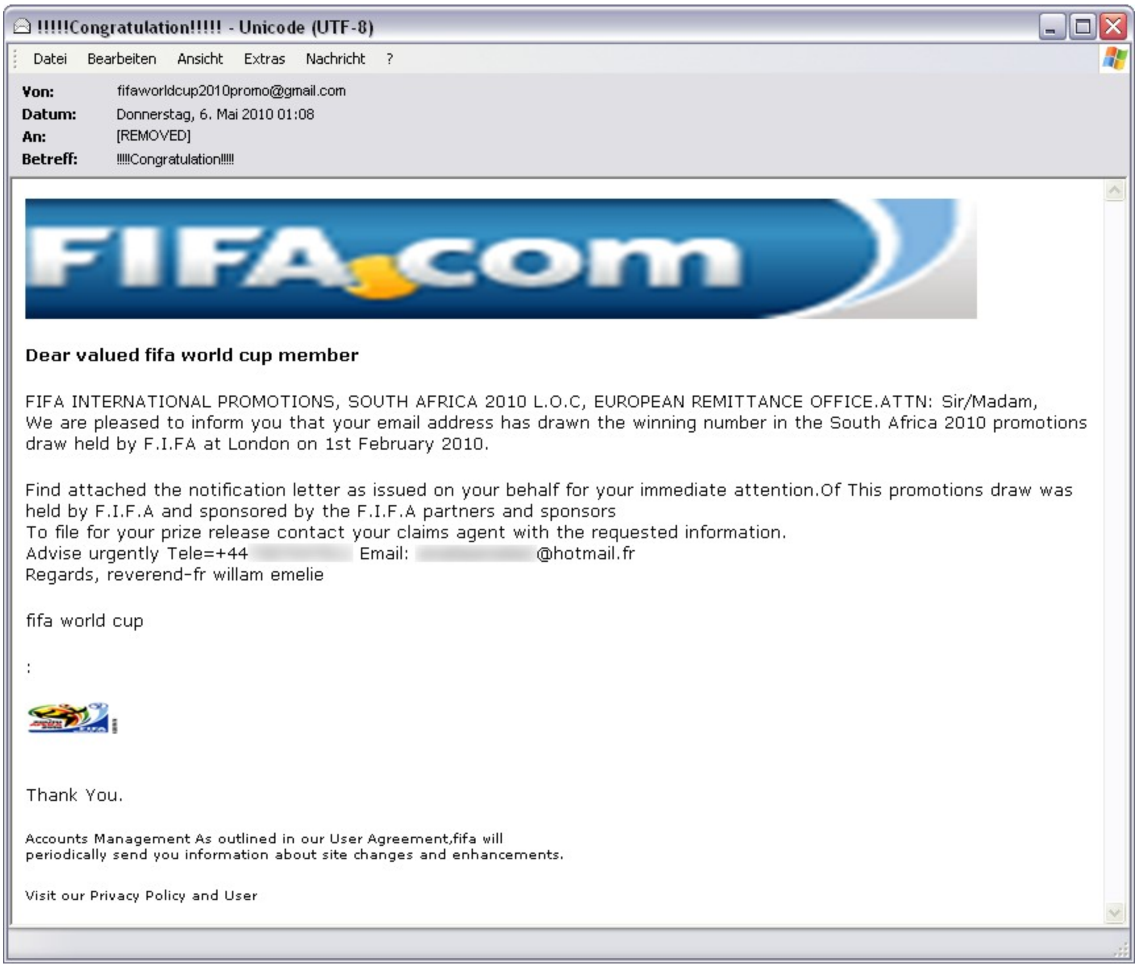
The recipient of such an e-mail is told that he has won a large amount of money in Euros, Dollars or some other currency. All he needs to do is supply details of his personal data to person XY. The lotteries are supposedly run by reputable companies and the banks involved are known all over the world. This scam can also be part of an attack along the lines of Nigerian spam.

The target group: Any Internet user

Psychological starting points: Greed, desire

The risk: To receive this sum, the alleged winner must first transfer fees to the fraudsters - usually to a foreign and/or anonymous bank account. One fee follows another; the victim keeps paying out but never sets eyes on either the winnings or (again) the fees he has already paid.

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



Von: fifaworldcup2010promo@gmail.com
Datum: Donnerstag, 6. Mai 2010 01:08
An: [REMOVED]
Betreff: !!!!!Congratulation!!!!!

Dear valued fifa world cup member

FIFA INTERNATIONAL PROMOTIONS, SOUTH AFRICA 2010 L.O.C, EUROPEAN REMITTANCE OFFICE.ATTN: Sir/Madam,
We are pleased to inform you that your email address has drawn the winning number in the South Africa 2010 promotions draw held by F.I.FA at London on 1st February 2010.

Find attached the notification letter as issued on your behalf for your immediate attention.Of This promotions draw was held by F.I.F.A and sponsored by the F.I.F.A partners and sponsors
To file for your prize release contact your claims agent with the requested information.
Advise urgently Tele=+44 [redacted] Email: [redacted]@hotmail.fr
Regards, reverend-fr willam emelie

fifa world cup

:

Thank You.

Accounts Management As outlined in our User Agreement,fifa will
periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User

***Screenshot 14:** A supposed notification of winnings*

3 Tips and tricks

To avoid becoming a victim of one of the scams described here, the following points should be observed.

3.1 Useful rules of conduct

- E-mail from unknown senders should be treated with caution. If an e-mail looks very strange, here's what to do: ignore it, delete it, but under no circumstances open attachments or click on URLs.
- Spam e-mail should never be responded to either. All a response does is indicate to the fraudsters that the address they wrote to is actually valid.
- Never disclose any personal information and/or bank data - either via e-mail or on dubious websites.
- Never transfer money to an unknown person.
- Never thoughtlessly publish your own primary e-mail address online, e.g. in forums and guest books, as it can be accessed by fraudsters there. It is useful to enter a secondary address for these purposes.

3.2 Technical measures

- A security solution for the computer with an integrated spam function will use a filter to protect the PC against such incoming e-mail.
- Opening file attachments, especially from unknown senders, harbours risks. Attachments should first be scanned with an antivirus program and, if necessary, deleted without being opened.
- Links in e-mails should never be clicked on without thinking. Check the URL. Many e-mail programs permit the actual target of the link to be seen by hovering the mouse over the visible link without actually clicking on it - the so-called mouse-over function.

4 Glossary

Bot: Bots are small programs that generally run unnoticed in the background on the victim's computer. Depending on the range of functions, they then carry out various tasks, from DDoS attacks to spam e-mail, recording keystrokes and much more. The range of functions essentially depends on how much someone wants to spend on a bot. Naturally, bots with a very large range of functions are more expensive than somewhat simpler bots that can do very little. For example, they can be purchased in underground forums.

Botnets: A botnet is a network of so-called zombie PCs. Command and Control Servers (C&C Servers) are used to administer the botnet. Amongst other things, botnets are used to launch overload attacks on web servers (DoS and DDoS attacks) and to send spam.

Social engineering: Social engineering refers to persuasion tactics used by a hacker to get a user to divulge information that he can use to cause damage to the user or his/her organisation. This often involves faking a role of authority, in order to gain access to data or passwords.

Spam: In the mid-1990s, spam described the inordinate dissemination of the same message in Usenet forums. The term itself comes from a sketch by Monty Python. Nowadays, spam has several meanings. As a generic term, spam stands for any mass-distributed, unsolicited e-mail. In a narrower sense the term 'spam' is limited to advertising e-mails, meaning that worms, hoaxes, phishing e-mails and autoresponders are not included in this.

Zombie PC: A zombie PC is one which can be controlled via a backdoor, using a remote controlling computer. Just like the cinema model, the zombie PC only obeys the hidden master and carries out the latter's often criminal commands. Usually a number of zombies are combined into so-called botnets.