

Viruses, Scams and Spyware

A comprehensive guide to recognizing these scourges of the web

After reading this guide, you will be better off than 99% of Internet users.

The purpose of this guide is to give you the power to recognize current and upcoming threats to your well being on the Internet. The primary goal is **recognition** and **prevention**. For those of you that have already been affected by spyware or viruses, various curative measures will be explained. Keep in mind that in 2004, spyware and viruses are a serious concern, and the measures one takes to rid themselves of them are also quite serious. So much so, that we must provide a disclaimer.

Warning / Disclaimer: Any attempt to “cure” your PC of viruses or spyware can result in the destruction of your PC. The best thing to do is to not get infested in the first place, and to have your important data backed up to CD.

Again, if you run Windows Update or any kind of anti-spyware utility, you can easily destroy your PC. Major updates and spyware removal attempts can have a huge destabilizing effect on your computer.

Kelso Consulting Group, LLC (owner of PCGuidebook.com) takes no responsibility for any loss of any kind that may occur on your PC. Companies mentioned do not endorse the PCGuidebook. Company and email examples are for illustrative purposes only.

Ready to broaden your mind? Prepare to be fully enlightened!

Viruses:

Usually, they come as an attachment in an email. You click on the attachment, and boom!

You're infected.

Countless throngs of people click on useless attachments every single day – flooding the web with still more viruses. Why does this happen? Here are the top reasons:

1. Failure to recognize the last three letters in the file name as ‘useless’
2. Failure to run an anti-virus program AND get daily virus definition updates
3. Failure to keep their PC updated with Windows Update

Note how the top reason has nothing to do with anti-virus software. Your greatest protection is **your own recognition** of potential viruses. How does one recognize a virus?

Very easily- it's the last three letters of the attachment that tell all, otherwise known as the *extension*.

File Extensions 101:

“101” refers to an American college course denoting “basic” or “beginner” – an introductory course. Most of you have seen digital pictures attached in an email – people send photos through email all the time. Photos sent through email are safe. Here are a few examples:

Beach1.jpg
My_vacation.jpg
350chevy.jpg

What's common with the above? They all have the .jpg extension. The .jpg (or .jpeg) extension tells your PC that this is a photo, and it will treat it as such. Files you work with have extensions that are familiar, such as this very document, a PDF file. Here are some examples of other file extensions you may be familiar with:

Resume.doc (A Microsoft Word file)
Directions.pdf (an Adobe PDF file)
Spreadsheet.xls (an Excel file)

Keep in mind that although usually safe, .doc and .xls files can contain macro viruses. Make sure Office is up to date. Besides, it's rude of someone to send you .doc or .xls files – you'll need Office installed on your PC.

The point is this: The list of “safe” attachments is short, so they won't be hard to remember. Let's take a look at the ‘useless’ (or ‘virus’) extensions:

.pif
.exe
.scr
.vbs
.zip (yes, if you get a ZIP file in an email, it's probably a virus)
.com
.bat
.com

The above list is by no means comprehensive, but it does cover the major extensions used by viruses.

Evaluate!

You'll need to evaluate the from, subject, body, and attachment of any incoming email. The four fields must make 100% total sense. If anything seems out of character, it's a virus. If the attachment is not a jpg, basically it's a virus.

The "From" field:

Sadly, the "from" field means absolutely nothing in 2004. Viruses usually forge the 'from' field to the following values:

- Your boss's email address
- Your bank's email address
- Bill Gate's email address
- Your email address (yes, you'll get a virus from yourself)
- admin@yourdomain.com – in other words, if you use Hotmail, you'll get a virus from admin@hotmail.com begging you to click on a useless attachment.

The old "I don't open attachments from people I don't know" should be expanded:

"I won't open attachments from ANYONE that have useless file extensions."

Keep in mind that the 'from' field can be absolutely anything or anyone. Your defense lies in your ability to look at all 4 fields to form a cohesive picture of what the email is trying to do.

The "Subject" field:

Threatening subject lines like "I have your password" or "I have your credit card" are dead giveaways that it's a virus. Your boss telling you "I love you" is a dead giveaway. Vague subject lines like "Hi", "Important", "re: word file", are all viruses.

Keep in mind that the 'Subject' field can be absolutely anything. Again, your defense lies in your ability to look at all 4 fields.

The "Body":

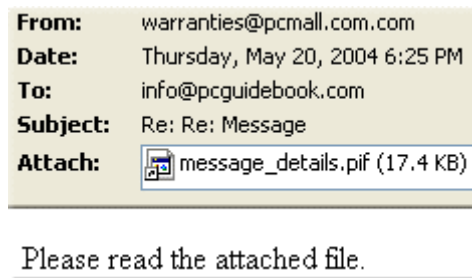
"See attached file" or other vague garbage that wants you to open the attachment or click on a link is a virus. The text will be accusatory, threatening, promise to fix your PC, or get you curious. Any of those are dead giveaways that it's a virus. No one wants to help you in an email – no one.

The attachment:

When the from, subject and body have you so seduced that you MUST click on the attachment, remember this: IF THE ATTACHMENT HAS A USELESS EXTENSION, IT'S A VIRUS. There are no exceptions to this. Re-read the "File Extensions 101" until it's burned into your memory. Recognition of the extension of the attachment is your last defense!!

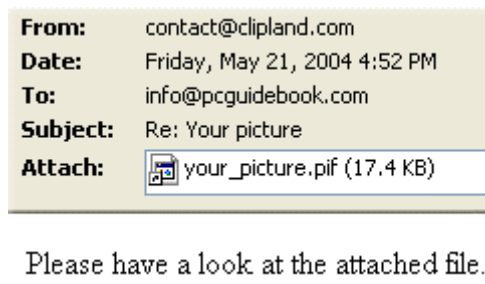
It cannot be emphasized enough that recognizing the file extension in an email attachment is CRUCIAL.

Now that you have some background, let's take a look at some actual emails. We'll start with the most obvious, then work our way gradually to the more "creative":



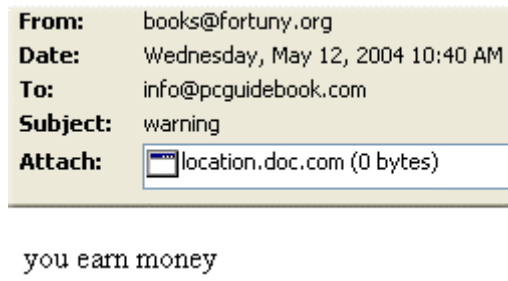
First off, I don't know the sender – big points off. Take a look at the subject. What message? I didn't send any message! It looks like this email is trying to get me curious, a bad sign. It tells me to read the attached file. Why didn't they put the message in plain text in the body of the email? It looks like I have to click on something to 'learn more' about what these people are talking about – another bad sign. The final analysis – the LAST THREE LETTERS of the attachment – "pif". If this does not SCREAM virus at you, nothing will. File extensions 101.

Let's step it up just a bit:



Again, junk sender. Looks like somehow this person has my picture. Or do they? Are you curious? Riddle me this: If this is a picture, how come the attachment is not a jpg? I'll tell you why: It's a virus. Again, file extensions 101. The reason why this is a step up is because "picture" instills more curiosity than "message". Come to think of it, wouldn't "illegal", "your bill", and "I have your password" generate even more curiosity? Indeed they do, and viruses (as well as scams) use them all the time.

Stay with me on this one:



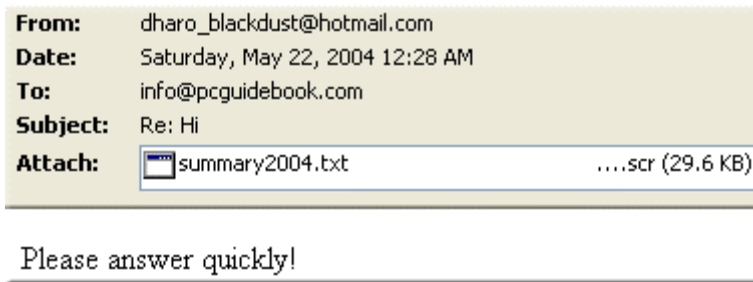
I earn money. Most of us do. Warning? About what? This makes no sense, and no sense = virus. Take a look at the attachment – the LAST 3 LETTERS of the attachment. I don't care if it says "word doc" or "excel file" or "list". I don't care how many spaces there are in the file name (I'll show that next). I don't care if there's a .doc or .jpg in the file name. All I care about is the last three letters. Com? Obviously a virus. This is the old "double extension" trick, one of the oldest in the book.

Remember the Anna Kourikova virus back in February 2001? Here's what you would have gotten in your email:

Annakournikova.jpg.vbs

Who in their right mind would click on a vbs file? The answer is thousands upon thousands. If you don't know the difference between a jpg file and a vbs file, you'll be contributing to the endless ocean of viruses in circulation.

Let's get a bit more fanciful:



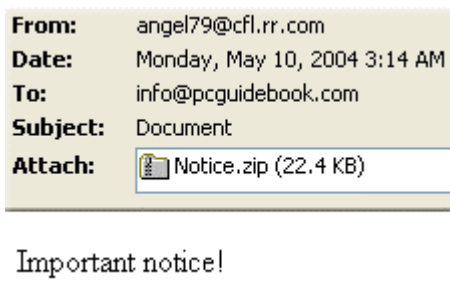
Looks like a summary of some kind is being offered to me, and I'd better answer quickly! A quick look reveals the file extension, .txt, which is quite safe, and the file will be opened in Notepad. But wait – did you know that there could be spaces in a file name? Did you know that there could be many *consecutive* spaces in a file name? Looks like this is an scr file, which screams virus. Again, sorry to repeat this – but it's the FINAL 3 LETTERS that matter.

Virus writers adapt to the latest protective measures – it's a constant tug of war. Mail servers and corporate networks are “wising up” and they are starting to automatically delete the obvious viruses before they even make it to your inbox. They do this in two ways:

1. Pre-scanning the attachments for known viruses, and deleting them before they get to you. This is flawed – antivirus software depends on ‘knowing’ the exact virus, and needs to be updated daily with a list of known viruses. What about the brand new virus that was released 8 hours ago?
2. Automatic blocking or deletion of the obvious ‘bad’ file types: pif, bat,vbs, etc. This is flawed as well – all ZIP files will make it through.

That's right. 99% of all zip files being sent via email are viruses. There's a saving grace here: a zip file is not executable; it's an archive or grouping of other files. Once unzipped, the true contents will be revealed – garbage files like exe, scr, pif, and the like.

Here's a zip file virus:



Many virus emails are flagged with “High Priority” and claim to be “important” or “mandatory”. They are flagged this way to let you know that it’s really important for you to get infected as quickly as possible. Here’s a cardinal rule: Nothing important ever comes through an email. If you went ahead and opened the zip file, you would find a .bat, .exe, .pif, or other garbage file. File Extensions 101 tells you that such files are viruses – no exceptions. Guess what – emails that provide a password for you to open a “protected” zip file are viruses too!

The best practice is to ignore/delete attachments that you were not expecting to receive, and not have the extension you expected – no matter who it’s from.

Enable “show file extensions”:

Windows has sheltered you from having to know about file extensions – by default it does not display them. This is dangerous. To be able to see file extensions – go to Control Panel, Folder Options, View tab, and UNCHECK “Hide extensions for known file types”

What can happen to me?

I’ve gone 6 pages without even describing the possible effects of opening a virus. Here’s a short summary:

Destroy your PC by formatting the hard drive or ruining the boot sector (Chernobyl virus, 1999) Ah, the good old days.

Simply replicate, and in doing so cause general web/email slowdowns (Netsky virus, Apr 2004)

Bring down a website with 'zombie' computers on a specific date (MyDoom virus, Feb 2004)

Overwrite some files with all zeros, send random files from your PC to others (Klez virus, Jan 2002)

Logs your keystrokes (credit card, banking, etc) and emails them to thief (Stawin, Jan 2004)

Reboots your PC by force every 5 minutes (Sasser worm, May 2004)

... what will they think of next?

Virus hoaxes:

A quick aside here. Emails warning of viruses are usually viruses themselves, or they want you to delete a file and 'pass the email to everyone on your address book'. Take a look at this one, it's been around for years and is still around even in 2004. As you read, keep in mind that NO ONE wants to help you in an email – whether you know them personally or not.

I'm sorry about this; but I received this E-mail from a client regarding a virus that was inadvertently passed on to everyone in their address book. I followed the instructions and YES, IT WAS ON MY COMPUTER.

Since you are in my address book, I am sending this on to you as a precaution. NORTON 2002 DID NOT DETECT IT!

Here are the instructions on how to check for this virus and delete it if you have it too. It only took a few minutes, following these instructions. Be sure to notify all in your address book too (which will take longer than deleting the virus from your computer).

Since you are in our address book, there is a good chance you will find it in your computer too unless you have an Apple or MAC. The virus (called jdbgmgr.exe) is not detected by Norton or McAfee anti-virus systems. The virus sits quietly for 14 days before damaging the system. It is sent automatically by messenger and by the address book, whether or not you sent Emails to your contacts. Here's how to check for the virus and how to get rid of it:?

YOU MUST DO THIS

1. Go to Start, Go to Find or Search option
2. In the File Folder option, type the name: jdbgmgr.exe
3. Be sure you search your C: drive and all sub-folders and any other drives you may have.
4. Click "Find Now"
5. The Virus has a Teddy Bear icon with the name jdbgmgr.exe DO NOT OPEN IT
6. Go to Edit (on menu bar), choose "Select All" to highlight the file without opening it.
7. Now go to File (on the menu bar) and select Delete. It will then go to the Recycle Bin.
8. Go to the Recycle Bin and Delete it

IF YOU FIND THE VIRUS, YOU MUST CONTACT ALL THE PEOPLE IN YOUR ADDRESS BOOK, SO THEY CAN ERADICATE IT IN THEIR OWN ADDRESS BOOKS.

To do this:

- a) Open a new e-mail message
- b) Click the icon of the address book next to the "TO"
- c) Highlight every name and add to "BCC"
- d) Copy this message enter subject paste to e-mail


Am very sorry about this nuisance. This age of technology is not that great sometimes. We are victims!

No one bothers to look up the specific file name – jdbgmgr.exe – in Google. If they had, the first 20 results are “hoax”, “hoax”, and “hoax”. Strangely enough, the file does indeed have a teddy bear icon. I won't go into more details – look the file name up on the web.

I want to show you a few more viruses, so that you get a flavor for current trends and how these viruses can come at you from different angles. Remember this: 2 weeks after you read this, they'll be a "different" kind of email that's not mentioned here. It will try to seduce/threaten you into clicking on an attachment or go to a website – in other words, **the email does not fully describe itself in the plain text of the body; it wants you to do something.**


Don't do it.

Here are a couple of scary emails that had me shaking in my boots:

From:	abuse@gov.us
Date:	Thursday, April 22, 2004 1:35 PM
To:	info@pcguidebook.com
Subject:	Illegal Website
Attach:	 judge_info.doc ...pif (29.6 KB)

You have visited illegal websites.
I have a big list of the websites you surfed.

+++ Attachment: No Virus found
+++ MessageLabs AntiVirus - www.messagelabs.com

From:	abuse@gov.us
Date:	Wednesday, May 26, 2004 1:52 AM
To:	info@pcguidebook.com
Subject:	Internet Provider Abuse
Attach:	 abuselist.zip (29.9 KB)

You have visited illegal websites.
I have a big list of the websites you surfed.

Here's the 'fear' part of it. Abuse@gov.us certainly looks like a threatening email address.

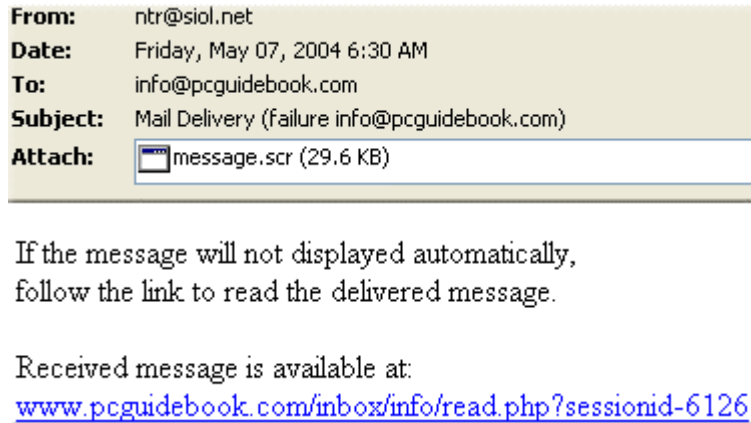
What's the cardinal rule of the "from" field? **IT'S ALWAYS FORGED. You'll be getting viruses "from" the President, yourself, your co-workers, anyone and everyone. It's a free-for-all as far as what shows up in the 'from' field.**

Again, the "from" field can be easily forged.

One of the emails is nice enough to proclaim that no virus was found. Indeed, MessageLabs is a legitimate anti-virus company. This could have also said “Norton Anti-Virus” with a link to the real Norton website.

It all comes down to the attachment. Not a jpg? IT’S A VIRUS. The madness is never ending.

Here’s a tricky one, one of the useless “mail router delivery failed” emails:



Take a look at the blue hyperlink. It’s using my actual website, pcguidebook.com. If this came to you, your website or email domain would be shown instead, lending a seductive realism to the whole adventure. The rest of the link, /inbox/info/read.php?session-id, certainly looks the part of an official link to an email message. Note how “info” is part of the actual email address as well. That link sure looks enticing...

But what is that message.scr attachment doing there? I never sent anything to ntr@soil.net, so why am I getting a deliver failure? What’s up with the “if the message will not displayed automatically”, shouldn’t it be “display automatically”? Turns out that clicking on the link will not go to a website, but instead execute the attachment.

There are 3 types of “mail router” or “delivery failure” messages:

1. Most likely, it’s a virus like above. Delivery failures, along with pictures, passwords, credit cards, and account suspensions/investigations are PERFECT subjects for getting you to fall for the garbage.
2. It could also be a legitimate, automated message from a mail server falsely accusing you of “sending” a virus. Rest assured, viruses have been sent to people in your name.
3. The least likely is that it really, truly is a delivery failure. Here’s how you can tell: You remember sending the email to that person, and your ‘sent’ text is displayed in the body of the email. You REMEMBER sending it!

It makes no sense to warn people about specific attachment names or subject lines. It's 2004, and viruses use VARIABLE texts and attachments, at times using YOUR DOMAIN or an "official" domain as part of their attack. When plying your way through the endless sea of email garbage, keep this in mind:

Guilty until proven innocent: Somebody sending you something via email that you did not initiate? It's junk. If an email doesn't make sense, it's junk. Analyze all 4 fields: from, subject, body and attachment. They all must come together in concert to form a "100%" email. If not, it's junk. Most email is junk anyway.

Know your file extensions: Click on a pif, exe, vbs, htm, hta, com, scr, zip or bat file and doom will most certainly befall you. Ask yourself this:

What business does this person / company / head of state / police officer / FBI / CIA / KGB / relative / boss /co-worker have sending me a zip file? More often than not, it's a virus.

Run an anti-virus program AND UPDATE THE DEFINITIONS DAILY.

What about the worms that take advantage of unpatched computers? You don't even have to have email – the worm simply finds you while you're connected to the Internet. The only way to defend yourself against this is the following:

1. Run a personal firewall like ZoneAlarm.
2. Make sure you are up to date with all service packs and critical updates from windowsupdate.microsoft.com.

HUGE DISCLAIMER:

Running Windows Update, especially for the first time on an older machine, can lead to disaster. I have seen computers not come back up from a reboot. That's right- they bluescreened. The PC had to be formatted and Windows had to be re-installed from scratch. All data was lost. Can someone say "MAKE SURE YOUR STUFF IS BACKED UP TO CD?" How about "KEEP YOUR RESTORE/INSTALL DISKS HANDY".

Running Windows Update invokes massive changes to your system, and THERE IS A RISK INVOLVED.

However, failure to run Windows Update will leave you vulnerable to the many worms still out on the web, looking for victims.

Personal story: In May of 2004, the big ‘sassser’ worm weekend, I installed Windows 2000 from CD on a spare PC – a sparkling clean install. I was on the web, looking for drivers and such, when all of a sudden I get a “Windows has encountered an error in lsass.exe, and your PC will reboot in 30 seconds”. I type in those words into Google, and that’s when I found out about Sasser. I re-installed Windows, but this time I kept it off the web, and installed ZoneAlarm from cd. That protected me long enough to get the critical updates to defend against Sasser.

You’ve been warned. Owning a PC requires diligence and maintenance.

Viruses are no joke, and defending against them is no joke. Gone are the “feel good” days of the early web.

Scams:

Concerned about your credit card number or bank account? Want to know the number one reason why “identity theft” is so common? 4 words:

They ask, you give.

People freely giving out their information when requested to do so by an email is so common, the thieves actually have too many credit card /bank account numbers than they know what to do with. It certainly is a land of plenty. This is called “phishing”.

But wait – the emails don’t say, “I’m a thief and need your account number to steal from you”. Indeed, they don’t – the email has to come across as legitimate, seductive, and forceful.

Here’s some background of what you can expect from an email that wants your information.

The from: field, as we know from the Virus section, can be faked. Expect to see the following:

accounts@ebay.com
admin@paypal.com
credit@citibank.com
verify@mastercard.com

Let’s make this real. Think about the bank you do business with. You can make your own “scamilicious” fake email address. Let’s say it’s BankOne. Here’s a possible email I would receive:

customerservice@bankone.com

Well, we've got the 'from' field covered. What about the subject line?

Re: Your account
Account suspension
Account investigation
Account activation
ATM Card Expired
Account update
Mandatory account update
Pending Approval
Your loan default
Re: transaction failure

Let your imagination run wild, you get the idea – any fear producing or concerning subject line will do. What about the body of the text?

How about themes like this:

Your account needs to be updated for your protection.
Your ATM card is about to expire, so give us the PIN number.
You can't sell any more on Ebay till you update your information.

Basically, bad things will happen if you don't do what the email tells you to do. Let's take a look at an actual scam email:

From: Support [mailto:support@citibank.com]
Sent: Tuesday, May 04, 2004 4:27 PM
To: info@pcguidebook.com
Subject: Your Citibank Account Must Be Confirmed

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:

https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

Thank you for using Citibank

Very seductive indeed. This is one of the milder ones; there are even more clever emails that threaten your account status. Note the hyperlink. It looks like a valid 'Citibank' page, but when you hover over the link, it tries to take you to "accountverify.us", which of course is bogus. Just because you see a long web link with a bunch of forward slashes and 'official' words does not mean you'll go to that site. Clicking on unsolicited web links from email is very dangerous. Bogus sites are up for a day or two until they get caught, then they simply register a new URL.

Let's get more creative – can you see the incoming flood of account numbers on this one?:

Citi® Identity Theft Solutions

Recently there have been a large number of identity theft attempts targeting Citibank customers. In order to safeguard your account, we require that you update your Citibank ATM/Debit card PIN.

This update is requested of you as a precautionary measure against fraud. Please note that we have no particular indications that your details have been compromised in any way.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely update your Citibank ATM/Debit card PIN please go to:

https://www.citibank.com/signin/citifi/scripts/login2/update_pin.jsp

Please note that this update applies to your Citibank ATM/Debit card - which is linked directly to your checking account, not Citibank credit cards.

Thank you for your prompt attention to this matter and thank you for using Citibank!

Regards,

Riley Buckner
Head of Citi® Identity Theft Solutions

A member of  Citigroup

Copyright © 2004 Citicorp. All rights reserved.

Do not reply to this email as it is an unmonitored alias.

Again, same fake hyperlink. Note how this one is far more threatening, and most likely “phished” far more ATM numbers. Looks like they want to ‘safeguard’ my account.

No one wants to help you through email – they just want your money.

If you allow yourself to be threatened by an email, kiss your money goodbye.

If you “update” or “confirm” by clicking on a link in any email, your money is as good as gone.

Look up “phishing samples” in Google to get a broader idea of what words will be used in an email to seduce you. Here are a few more phishing emails, keep in mind they’ll be sent with ACTUAL OFFICIAL LOGOS, lending to the realism. The idea is to get you concerned about what might happen to you if you don’t do what the email tells you to do:

Actual subject lines:

'Important.'
'MSN HOTMAIL Account Verification'
'Your request for Express Transfer'
'Found error! Please resubmit UsBank.com urgent'
'Westpac Bank users warning'
"Credit Card Request from Federal Deposit Insurance Corp."
"Notification of PayPal Unauthorized Account Access"
"Problems with your account"
"Verify your E-mail with Citibank"
"AOL billing center"
"Visa Security Update"
"Billing Issues"
"eBay Member Billing Information Updates"

Actual text bodies:

"During our regular and verification of the accounts we couldn't verify your current information... if the account is not updated to current information within 5 days then your access to Buy or Sell on eBay will be restricted."

"Due to technical update we recommend you to reactivate your account."

"Your bank account has been temporarily closed cause of explicit fraud activity... You can find all the details about this incident in the attached file and if you still have any questions until the police start investigation, please contact us as soon as possible..."

"...to enjoy your AOL experience and keep your account active, you must enter new, *valid* credit card information..."

"... The inactive customers are subject to restriction and removal... confirm your email address and credit card information by clicking the link below..."

"login to your account and go to the Account Maintenance to read about changes in our policy"

"You have been pre-indefinitely suspended from eBay because credit cards information incorrect ... we offer you the ability to place or change the information you submit to us by click here and entering the correct information yourself in your account"

"Due to the new changes made regarding user registration, we are making this security check in order to prevent future sign in problems."

"Please install our special software, that will remove all the keyloggers and backdoors from your computer..."

The above is especially amusing. If you installed the “special software”, you would have installed the very keylogger that they supposedly want to protect you from. **NO ONE WANTS TO HELP YOU IN AN EMAIL.**

Again, **NO ONE WANTS TO HELP YOU IN AN EMAIL.**

This next one is quite extreme, but bear in mind, it’s all designed to get you to give up your information:

"Your credit card will be billed at \$22.95 weekly and free 3 pack of child porn CD is shipping to your billing address. To cancel your membership and CD pack please email full credit card details to cancel@shadowcrew.com."

"Ebay offer this month a great prize for members. All you need to do is to login in your account and enter this number...."

"We regret to inform you that we were unable to charge your card...We need you to re-enter valid payment and verification information."

"Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.."

"During one of our regular automated verification procedures we've encountered a problem caused by the fact that we could not verify the data that you provided to us"

You may now be saying to yourself, if emails can look legitimate with official logos, and web sites can be doctored to look real, how can I trust anything or anyone on the web? Certainly a valid question. Let's take pcguidebook.com. Here are some clues that PCGuidebook is legitimate:

1. **YOU** found PCGuidebook through a search engine – **you initiated the contact.**
2. PCGuidebook is not advertised via email or popups. It's just out there on the web for you to find.
3. A search on Google for "pcguidebook" does not reveal negative content.
4. If you contacted us, we would get back to you, and we'd make sense doing it.

Remember that the "from" field in an email is ALWAYS forged in a scam or virus. Therefore, some of you may have gotten a virus "from" info@pcguidebook.com. Hopefully you didn't fall for it.

Phishing scams are the biggest thing out there currently – it's so easy to scam people out of their credit card numbers with a fake email address, some pretty logos, and the threat of "suspension", "account compromised", or whatever.

Overseas lotteries and other "advance fee" fraud are also common. Break this cardinal rule and you are sure to be a victim:

Never pay any "fees" to claim your "lottery" winnings, or pay any fees in the hopes of getting a sum of money.

Read the above sentence again. Millions yearly are lost by people paying "fees" in the hopes of getting more money. The pretenses vary, from lottery winnings to your 'payment' for helping get funds out of a foreign country.

"419" Scam:

You get an email from a relative of a foreign president/king/important person. This important person died in a plane crash / assassination / whatever. There's \$50 million that this person left, but the emailer needs your help getting it out of the country. For your trouble, you keep 30%.

Back and forth emails progress. Fake documents abound. Eventually, you're asked to pay fees to bribe corrupt government officials, pay certain taxes, bank fees, whatever. The scam ends when one of the following conditions is met:

1. You wise up and stop sending the money.
2. You run out of money.

3. You travel to the foreign country, and end up dead.

Note that “you collect 12 million dollars” is not one of the outcomes. For an idea of how these emails are structured, www.scamorama.com provides hours of entertainment.

How about winning a lottery? Forget it:

Ref. Number: 639/898/002

Batch Number: 430456543-DD23

Sir/Madam,

We are pleased to inform you of the result of the Lottery Winners International programs held on the 30th March, 2004. Your e-mail address attached to ticket number 278541465006-4872 with serial Number 1772-554 drew lucky numbers 5-14-18-23-33-39 which consequently won in the 1st category, you have therefore been approved for a lump sum pay out of US\$1,000,000 (One Million United States Dollars) CONGRATULATIONS!!! Due to some numbers and names, we ask that you keep your winning information confidential until you file for your claim.. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants.

All participants were selected through a computer ballot system drawn from over 20,000 companies and 30,000,000 individual e-mail addresses and names from all over the World. This promotional program takes place every year. This lottery was promoted and sponsored by some eminent personalities who do not wish to declare their identity for security reasons.

To file for your claim, please contact our fiducial Agent:

Mr. James Peters

Email: dtrustagency@netscape.net

Remember, all winning must be filed not later than 3rd May,2004 or when authentic proof is given for the delay of filing. Please note in order to avoid unnecessary delays and complications, remember to quote your reference number and batch numbers in all correspondence.

Furthermore, should there be any change of address do inform our agent as soon as possible. Congratulations once more from our members of staff and thank you for being a Winner in our promotional program.

Note: Anybody under the age of 18 years is automatically disqualified.

Sincerely yours,
Mrs. Jane Fish,
Lottery Coordinator.

Money from out of the clear blue sky? Not really. Anything good or bad happening to you from an email? Nope.

Keep these thoughts in mind:

updates@microsoft.com sending you a patch? Fake.

Ebay suspending your account? Fake.

You've violated the Patriot Act and you're under investigation? Fake.

Someone wants you to delete a virus on your PC? Fake.

You've won something? Fake.

You've committed fraud and need to do something about it? Fake.

Your account has been compromised and you need to 'verify' or 'update'? Fake.

A popup tells you that spyware is on your machine? Fake

A huge window pops up telling you you've been "tracked"? Fake.

Someone wants to give you something, money or whatever? Fake.

The list is endless.

The web and email only want to TAKE from you, not give. This concept is crucial. Since when do you think people want to give you money or advice? They don't care about you.

Someone calls you to give you free software, and asks what kind of PC you have for a survey? Beware! If your PC is good enough, they'll come over and steal it when you're not home.

This ends the Scams section. Remember this:

No one wants to help you in any way from an email.

No one can threaten you with an email – no matter what the email says.

If you allow yourself to be threatened, concerned, or hopeful of an email – no matter who it's from – you've been scammed. These are the very emotions scammers use to prey on you.

Spyware:

It's on about 80% of all home computers. Sure signs of a spyware infestation:

1. Excessive pop-up ads
2. Home page changed to [www.spam me to oblivion.com](http://www.spam.me.to.oblivion.com)
3. Extra toolbars at the top or bottom of your browser
4. Freezing, crashing, slow machine
5. Useless 'free' programs like mem boosters or 'toolbar' search helpers (the list is endless)

How it all began:

Imagine you're a software developer, and you have a site on the web. You've developed a little "memory booster" utility that frees up memory on your machine. It doesn't really work that well, and you can't charge much for it, so you decide to offer it for

FREE.

People love free stuff, and hundreds daily are being downloaded from your site. If only you could make some money....

Enter adware!

By bundling advertising with the software utility, you can make some money even though the customer is getting the product for free.

Early versions of adware simply generated random popup ads, or displayed ads within the interface of the product itself. Fairly harmless, you could almost say the free product was worth it, even though you got more ads. Someone came up with a more aggressive idea:

Enter spyware!

What if we could deliver targeted pop-up advertising, based on the users' surfing habits? Advertisers would pay much more money! Spyware, bundled as part of a "free" web utility of varying uselessness, spies on your web surfing. Looking at a car on the web? Pop-up ads will show competing vehicles. This is on-demand, targeted advertising and it is **VERY PROFITABLE**. This is why we've had an explosion of spyware. It is an epidemic. When spyware gets too rough and too aggressive,

Enter malware!

Home page hijacking, system instability, and huge amounts of popups can be attributed to malware. It's also very difficult – and dangerous – to get rid of.

Spyware is not developed with your system's stability in mind. It has one purpose: to choke your screen with ads.

Some rules of the road:

If it's free, it's spyware.

If it's a free product being offered by a popup, it's spyware.

If a message pops up telling you that you have spyware, it's spyware.

If it promises to increase your PC's performance, it's spyware.

If it's a free popup blocker, it's spyware.

If it's a spyware removal tool, it's spyware.

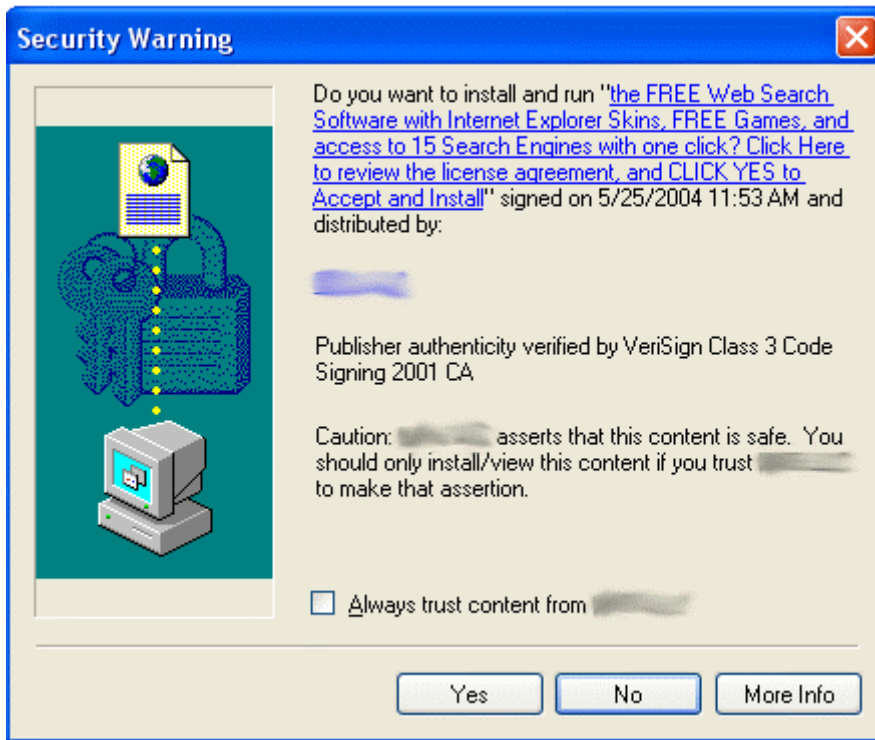
If it's silly, it's spyware.

If it's useless, it's spyware.

Only download programs off the web that you intentionally researched and searched for, or products that were specifically recommended to you by a computer person. Anything else usually masquerades as being a helpful utility, but in fact is junk. Remember – no one wants to help you over the web – they just want your money.

Anything popping up on your computer to “install and run” something is mostly spyware. Popup ads for free cursors, free this or free that are all spyware.

Let's take a look at how spyware gets on your PC. You're surfing the web, then you're hit with this:

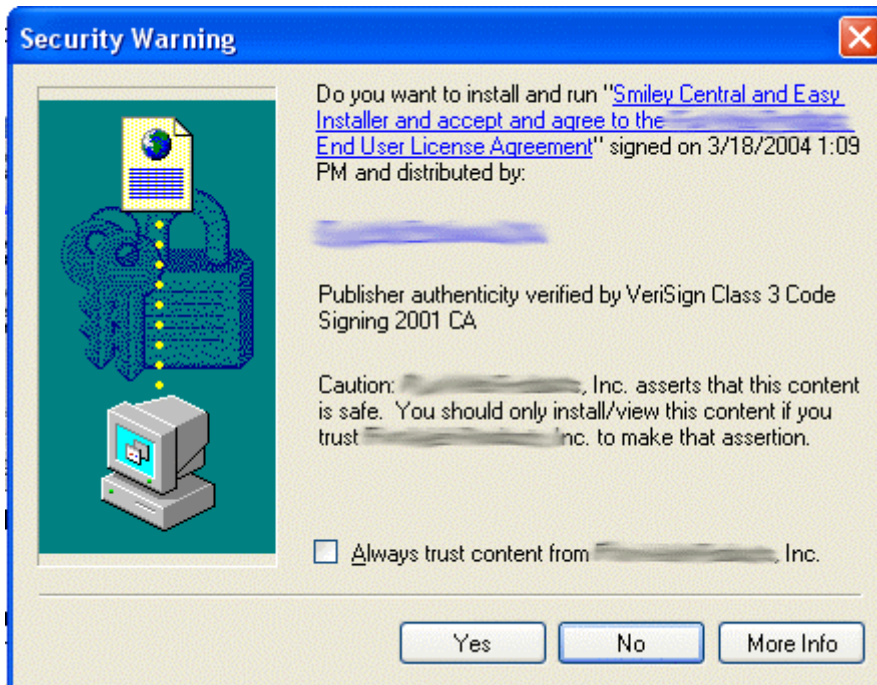


The company name is blurred for privacy reasons. This is the standard

“do you want to install junk?”

dialog box. Say Yes to this, and you’ve just sentenced your PC to a slow death. Search utilities, browser add-ons, browser “updates”, games, clock syncs, password savers and the like offered through this type of dialog are 100% pure spyware. The word “FREE” also lends itself to spyware.

Here’s another:



Who in their right mind would install smilies? Junk.

The above are obvious junk. However, there are those dialog boxes that disguise themselves as “official” downloads or other coercive messages designed to get you to click.

Critical point here: If you did not initiate the dialog, it’s spyware.

With very few exceptions, the only valid “install and run” items are:

Macromedia Flash
Macromedia Shockwave

The dialog **MUST MENTION MACROMEDIA**. Similar product names have been used to trick those familiar with Flash and Shockwave. If it does not say Macromedia, it’s spyware.

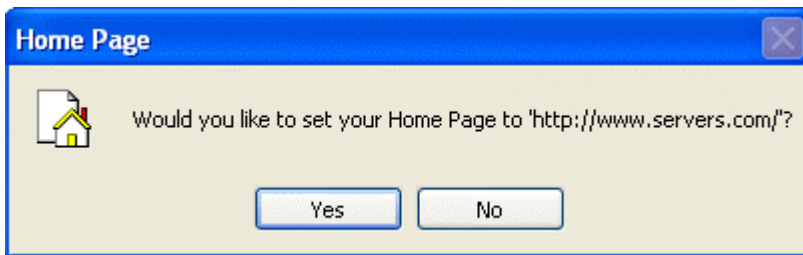
There are, of course, exceptions to this. Whenever you get a popup asking you to install something, type the name of the program (or the company offering it) and “spyware” into a search engine and see what you find.

Spyware and advertising love to take advantage of mistyped URL’s of popular sites. Leave out the “o” in Lycos, and you’ll get hit with this:



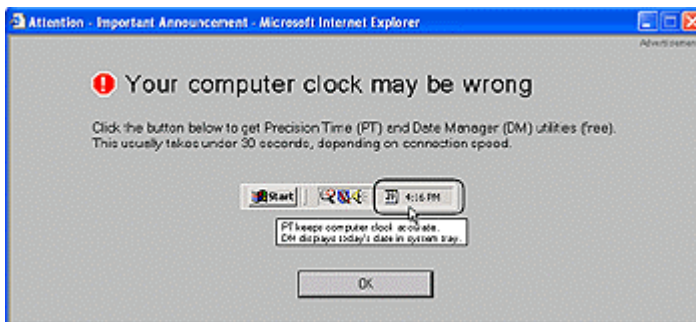
Anything that saying “you’ve won”, “congratulations” or the like is junk. What makes you think people want to give you something?

Here’s another, when you leave out the “e” in Google:



Never, ever respond to this kind of request to change your homepage. Avoid sites that use it, and for that matter avoid sites that throw spyware at you.

How about “Googll.com”:



Any popup or email telling you something is wrong or may be wrong with your computer is nothing but spyware. Again, no one wants to help you or your computer – all you are is a source of advertising revenue.

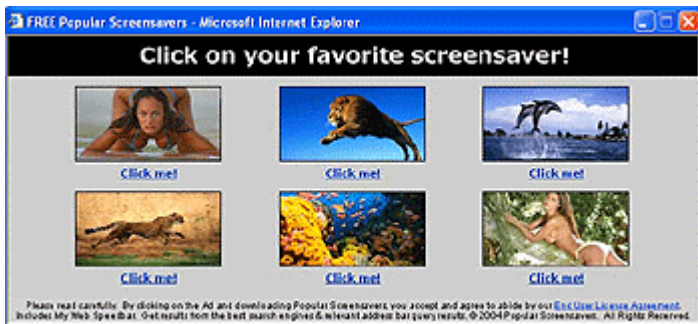
Adding an “n” to msn.com reveals a risqué directory page, as well as more garbage to click on:



Again, no one wants to give you anything – they just want your money.



The example above is becoming far more common. Variants include “Who is this pop star?”, with three to choose from. Using current topics and asking you questions that you feel strongly about, you’re more likely to click. Did you ever notice that it doesn’t matter where you click, and those really aren’t “yes” and “no” buttons? More junk.



Above, we have 6 delightful screensavers to choose from. It doesn't matter where you click, you'll be taken to a page where you can download the screensavers – and the spyware that comes with it. Again, if it's free, it's spyware.

Pop-up blockers:

I don't run one. The reason is this: it takes money to run websites. To stay in business, you can either charge for content (like PCGuidebook.com), or have advertising on your site.

Of note, PCGuidebook runs no advertising of any kind. If you get popups during a visit or when exiting from PCGuidebook, you've got spyware. Same thing with Google.

Popups, when done tastefully, are just a little bothersome. You can certainly deal with a “commercial” every once in a while in return for that sites content – it's a fair trade.

When popups become intrusive, you may be inclined to get a popup blocker. This is wrong – the reason why you're getting a lot of popups is the spyware on your PC. If you get a popup blocker, now you have two opposing forces running on your PC – one that says “give me popups” and the other that says “I will block all popups”. That's like being in a car and hitting the gas and brake at the same time – more work for nothing.

Also, without a direct recommendation, most popup blockers are spyware in themselves! If you simply must get a popup blocker, consider the Google Toolbar or any blocker recommended by pcworld.com.

What can you do?

Sadly, most who read this will already have spyware on their PC. The best thing to do is not to download junk on the web, or respond to advertisements or “warnings”. However, if you've been infested, there are 3 main tools I use:

Ad-Aware
Spybot Search and Destroy 1.3
Hijackthis

A search on Google and you'll find where to download them – they are all free.

Before running any of these utilities, make sure you have documents and pictures backed up to CD. Think I'm kidding? Why is it that everyone trusts their hard drive, with billions of ones and zeros, to last forever without the slightest possibility of corruption or data loss?

You've been warned.

Ad-Aware and Spybot 1.3 work much like virus scanners, they search your hard drive against a list of known spyware. You can also update them with the latest "definitions". At the end of the scan, you can 'clean', and that will delete most of the spyware. For really bad cases, all three tools, with multiple passes, as well as registry or safe mode work may be necessary. No single tool is 100%. Here are some specifics:

Ad-Aware:

When it finds more than 50 items, you'll need to manually check off each item. "Tracking cookies" are harmless, so if it finds tons of entries, you can save time by only checking off the folders, registry values, etc. After the scan and you give it the 'clean up' button, it tends to hang on very large infestations as it tries to quarantine/delete. Leave the room for a half hour, then come back. If it's still frozen, bring up the Task Manager and end it.

Spybot 1.3:

I've never seen this crash. Ad-Aware and Spybot, when applied in sequence (I'd run Spybot first, reboot, then Ad-Aware), provide a solid performance against spyware. Spybot even includes protection against future spyware infestations, by running in the background (teatimer.exe).

Hijackthis:

When you really need to get nasty, this is the tool. It does not detect spyware, but outputs all of your registry entries pertaining to startup and your browser home page. Be careful what you check off for deletion, because even your anti-virus program will be on the chopping block – it's in the startup too.

Even with all 3 tools, and multiple passes of all 3 tools, you may still have to boot to safe mode and manually delete certain files, or directly modify the registry. Spyware is nasty!

The main point is to not fall victim in the first place.

Remember this:

No one wants to help you on the web – it's all about hurting you or taking your money – by deceiving you.

Click on a useless attachment in an email, and get a virus. There are no exceptions.

Don't bother running Windows Update, and get a worm. There are no exceptions.

Refuse to back up your family photos, and eventually you'll lose them. There are no exceptions.

Read this guide over again – the main points it tries to deliver are the concepts of how you are taken advantage of.

Be safe out there!

©June 2004

Kelso Consulting Group, LLC

www.pcguidebook.com