Personal Security Attacks

WHAT IS SPYWARE?

Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

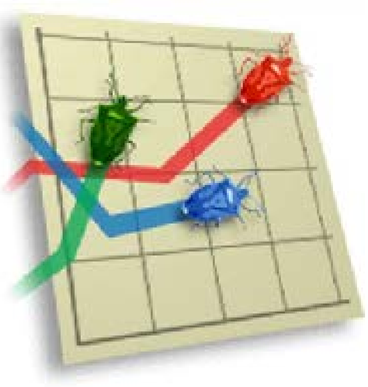
- Advertising
- Collecting personal information
- Changing the configuration of your computer

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information.

http://www.microsoft.com/security/spyware/whatis.aspx

SPYWARE STATISTICS

Click on the image or link below to view some interesting spyware statistics:



http://www.lavasoft.com/support/spywareeducationcenter/spyware_statistics.php

SPYWARE SYMPTOMS

You could have spyware if:

Your computer is slow and occasionally crashes. Spyware is not designed to be efficient. The resources these programs use to track your activities can slow down your computer and errors in the software can make your computer crash.

You could have spyware if:

You have additional toolbars added to your Web browser that you don't want or need – and are difficult to remove.

You could have spyware if:

You get bombarded with pop-up ads that aren't related to a particular Web site you're visiting. These ads are often for adult or other Web sites you may find objectionable. If you see pop-up ads as soon as you turn on your computer or when you're not even browsing the Web, you might have spyware or other unwanted software on your computer.

You could have spyware if:

Your home page or search page settings get changed, and sometimes you are not able to change them back.

Often times when your home page is changed it is changed to direct you to a malicious web site.

COMMON SPYWARE ATTACKS

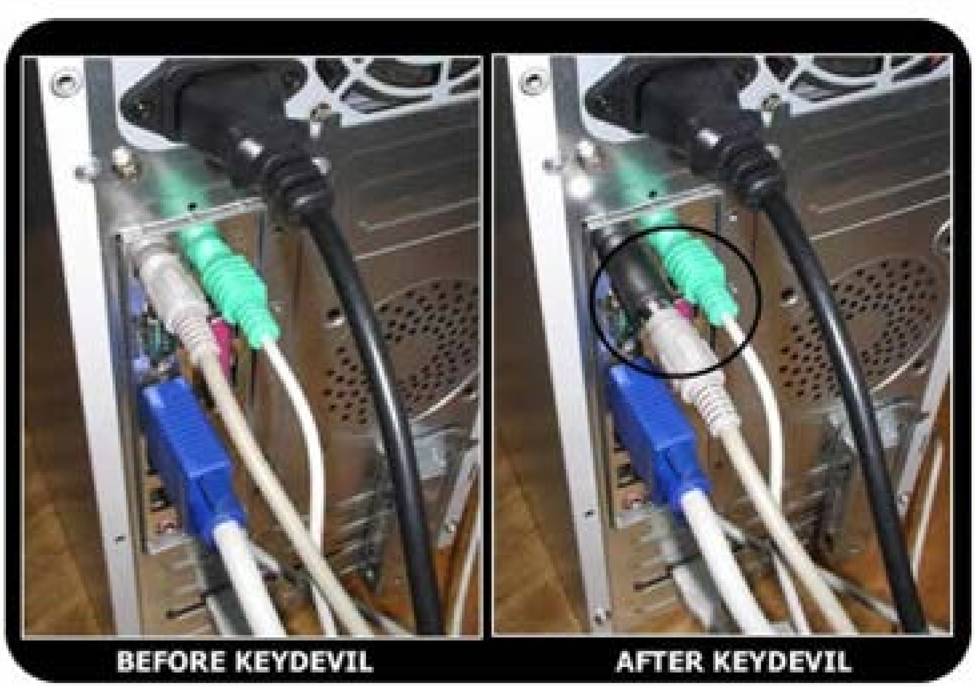
With the growing popularity of Online Banking, Blogging and sites and services like PayPal, Amazon and eBay, personal data becomes more and more valuable to thieves.

There are several different spyware tools, two common tools are **Keyloggers** and **Browser Hijackers.**

HARDWARE KEYLOGGERS

Keyloggers are “Keystroke Loggers”, they record your keystrokes, which could reveal valuable personal data.

Hardware keyloggers, like the picture shown below, are most commonly found in public places on public accessible computers – like Internet Cafés, schools, libraries, airports, hotel lobbies, etc.



SOFTWARE KEYLOGGERS

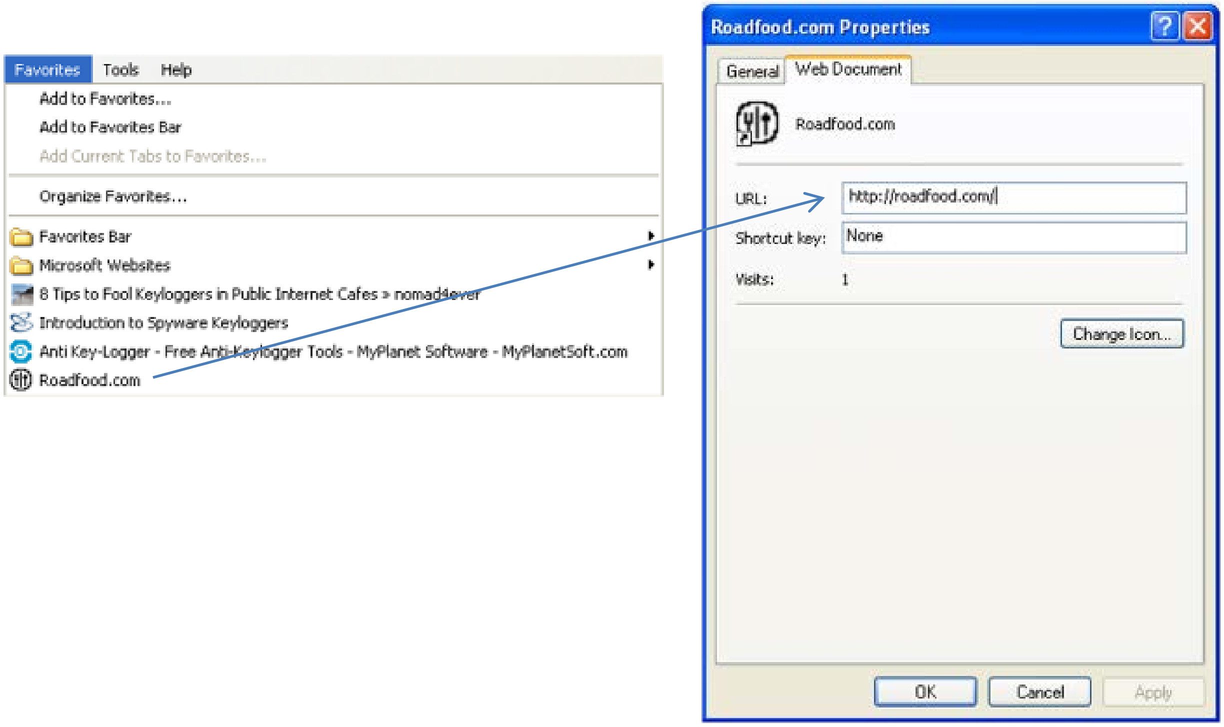
This type of logging is accomplished by using the Windows function **SetWindowsHookEx()**that monitors all keystrokes. The spyware will typically come packaged as an executable file that initiates the hook function, plus a DLL file to handle the logging functions.

Some keyloggers are legitimate, downloadable programs (i.e. for parents that want to monitor their children's Web activity). These programs are sometimes found packaged in with other programs that are detected as spyware.

BROWSER HIJACKERS

If your home page changes, your browser probably got hijacked. Your new, unwelcome, home page will often time be pornographic or at least shower you with advertising – to the point of no return where you cannot get rid of it!

Your browser may get hijacked yet another way, in a way that may not seem worth the effort. This is when your browser's favorites are changed to purposely increase activity to a particular web site. This is often done simply to increase usage to a site and thus increase search rankings to elevate the site on everyone's search results.


Favorites
Tools
Help
Add to Favorites...
Add to Favorites Bar
Add Current Tabs to Favorites...
Organize Favorites...
Favorites Bar
Microsoft Websites
8 Tips to Fool Keyloggers in Public Internet Cafes » nomad4ever
Introduction to Spyware Keyloggers
Anti Key-Logger - Free Anti-Keylogger Tools - MyPlanet Software - MyPlanetSoft.com
Roadfood.com
Roadfood.com Properties
General
Web Document
Change Icon...
OK
Cancel
Apply

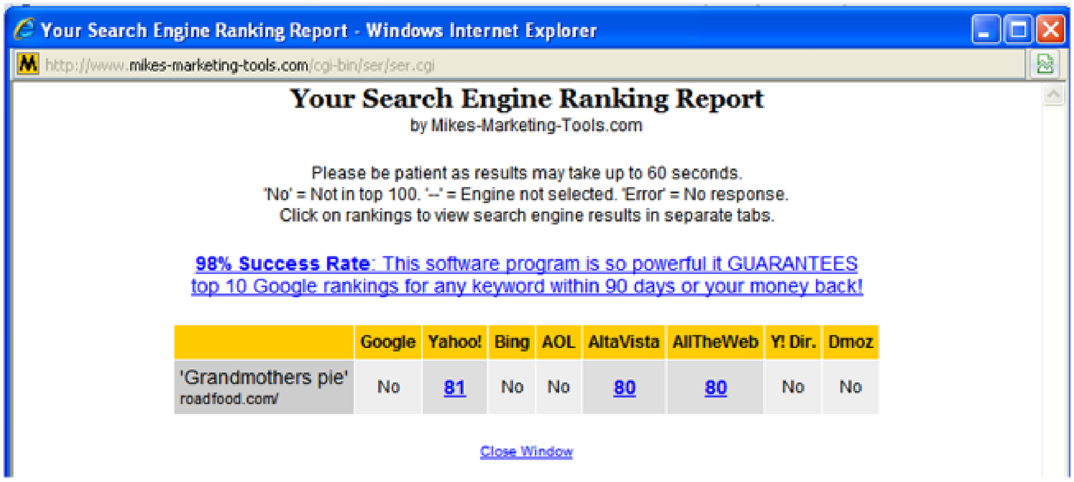
Roadfood.com

URL: http://roadfood.com/

Shortcut key: None

Visits: 1

You can see by the image below, http:**//roadfood.com** used with the search criteria "Grandmothers pie" is ranked at about 80. Great marketing statistics!


Your Search Engine Ranking Report - Windows Internet Explorer
http://www.mikes-marketing-tools.com/cgi-bin/ser/ser.cgi

Your Search Engine Ranking Report

by Mikes-Marketing-Tools.com

Please be patient as results may take up to 60 seconds.
'No' = Not in top 100. '--' = Engine not selected. 'Error' = No response.
Click on rankings to view search engine results in separate tabs.

98% Success Rate: This software program is so powerful it GUARANTEES top 10 Google rankings for any keyword within 90 days or your money back!

	Google	Yahoo!	Bing	AOL	AltaVista	AllTheWeb	Y! Dir.	Dmoz
'Grandmothers pie' roadfood.com/	No	81	No	No	80	80	No	No

Close Window

PASSWORDS

There are three means by which you can prove to a computer that you are who you say you are.

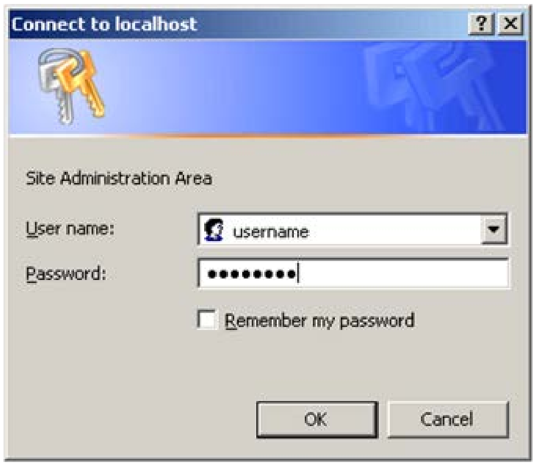
1. What you know.
2. What you have.
3. What you are.

WHAT YOU KNOW

For example, what you know could be your username and password.

Passwords are required by computer users every single day. Sometimes a user has multiple passwords. In some cases, users make their passwords weak to aid in remembering them.

Access the links below to check the strength of your NTC password and to find out how Microsoft recommends that you create a strong password.


Connect to localhost

Site Administration Area

User name: username

Password: ●●●●●●●●●

□ Remember my password

http://www.microsoft.com/protect/fraud/passwords/checker/aspx

http://www.microsoft.com/protect/fraud/passwords/create.aspx

There are numerous reasons why people don't use strong passwords and because of this, passwords are a frequent focus of attacks.

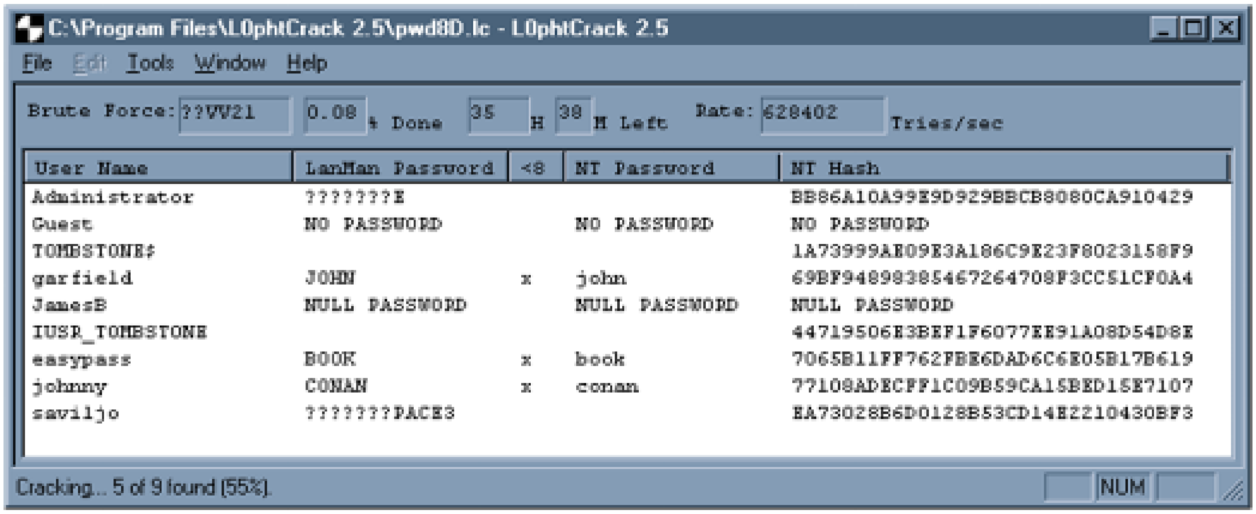
Password attacks include three common procedures: a brute force attack, a dictionary attack, and attacks using rainbow tables.

BRUTE FORCE ATTACK

Generally, it would take a person too long to break a password by attempting to login multiple times with different passwords. Most times the computer would lock you out after a set number of times.

The trick: obtain the hashed (encrypted) password file from the computer you are trying to break into and use a specially designed program designed to formulate passwords, hash them, and then compare the manufactured hashed password with the hashes in the stolen password file. When a match is found, an attacker can then log into the account associated with the matched password -

providing the user did not change their password since the file was stolen (and is the reason passwords should be changed often).


C:\Program Files\L0phtCrack 2.5\pwd8D.lc - L0phtCrack 2.5
File Edit Tools Window Help

Brute Force: ??VV21 0.08 % Done 35 H 38 M Left Rate: 628402 Tries/sec

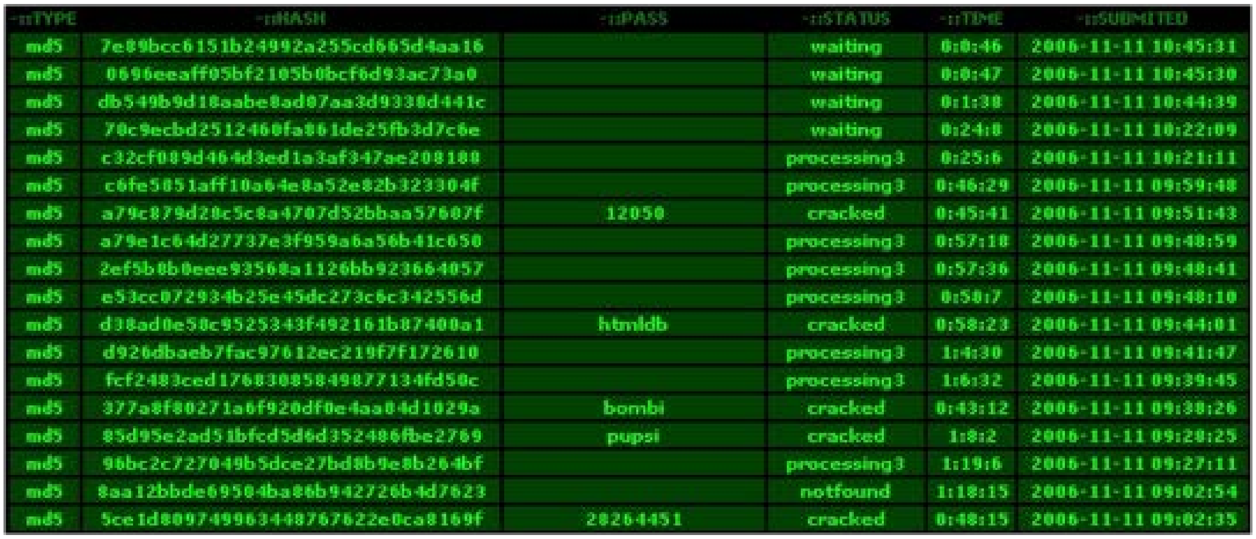
User Name	LanMan Password	<8	NT Password	NT Hash
Administrator	???????E			BB86A10A99E9D929BBCB8080CA910429
Guest	NO PASSWORD		NO PASSWORD	NO PASSWORD
TOMBSTONE$				1A73999AE09E3A186C9E23F8023158F9
garfield	JOHN	x	john	69BF948983854672647 08F3CC51CF0A4
JamesB	NULL PASSWORD		NULL PASSWORD	NULL PASSWORD
IUSR_TOMBSTONE				44719506E3BEF1F6077EE91A08D54D8E
easypass	BOOK	x	book	7065B11FF762FBE6DAD6C6E05B17B619
johnny	CONAN	x	conan	77108ADECFF1C09B59CA15BED15E7107
saviljo	???????PACE3			EA73028B6D0128B53CD14E2210430BF3

Cracking... 5 of 9 found (55%).

DICTIONARY ATTACK

This is another type of brute force attack that uses prebuilt dictionaries consisting of hashed values of common words. This database is compared against a stolen database of hashed passwords. If there are any weak passwords, these will be cracked within seconds.

A dictionary file can be tuned and compiled to cover words probably used by the owner of the account that a malicious user is going to attack. The attacker can gather information (via dumpster diving, social engineering, Internet research) to understand the user and then build a list of all unique words relating to the user.



::TYPE	::HASH	::PASS	::STATUS	::TIME	::SUBMITED
md5	7e89bcc6151b24992a255cd665d4aa16		waiting	0:0:46	2006-11-11 10:45:31
md5	0696eeaff05bf2105b0bcf6d93ac73a0		waiting	0:0:47	2006-11-11 10:45:30
md5	db549b9d18aabe8ad07aa3d9330d441c		waiting	0:1:38	2006-11-11 10:44:39
md5	70c9ecbd2512460fa861de25fb3d7c6e		waiting	0:24:8	2006-11-11 10:22:09
md5	c32cf089d464d3ed1a3af347ae208188		processing3	0:25:6	2006-11-11 10:21:11
md5	c6fe5851aff10a64e8a52e82b323304f		processing3	0:46:29	2006-11-11 09:59:48
md5	a79c879d20c5c8a4707d52bbaa57607f	12050	cracked	0:45:41	2006-11-11 09:51:43
md5	a79e1c64d27737e3f959a6a56b41c650		processing3	0:57:18	2006-11-11 09:48:59
md5	2ef5b0b0eee93560a1126bb923664057		processing3	0:57:36	2006-11-11 09:48:41
md5	e53cc072934b25e45dc273c6c342556d		processing3	0:58:7	2006-11-11 09:48:10
md5	d38ad0e58c95253 43f492161b87400a1	htmldb	cracked	0:58:23	2006-11-11 09:44:01
md5	d926dbaeb7fac97612ec219f7f172610		processing3	1:4:30	2006-11-11 09:41:47
md5	fcf2483ced176830885849877134fd50c		processing3	1:6:32	2006-11-11 09:39:45
md5	377a8f80271a6f920df0e4aa84d1029a	bombi	cracked	0:43:12	2006-11-11 09:38:26
md5	85d95e2ad51bfcd5d6d352486fbe2769	pupsi	cracked	1:8:2	2006-11-11 09:28:25
md5	96bc2c727049b5dce27bd8b9e8b264bf		processing3	1:19:6	2006-11-11 09:27:11
md5	8aa12bbde69504ba86b942726b4d7623		notfound	1:18:15	2006-11-11 09:02:54
md5	5ce1d8097499634487676 22e0ca8169f	28264451	cracked	0:48:15	2006-11-11 09:02:35

RAINBOW TABLES

With computer processors being really fast these days, the more common and preferred approach to password attacking is by using rainbow tables.   These tables are prebuilt (and freely available on the Internet) databases of hashed values of every possible combination of passwords. This database is then compared against a stolen copy of a system's hashed password database as would be done with a dictionary attack.

WHAT YOU HAVE

What you may have are tokens that you insert into the computer or wave in front of a scanner.

WHAT YOU ARE

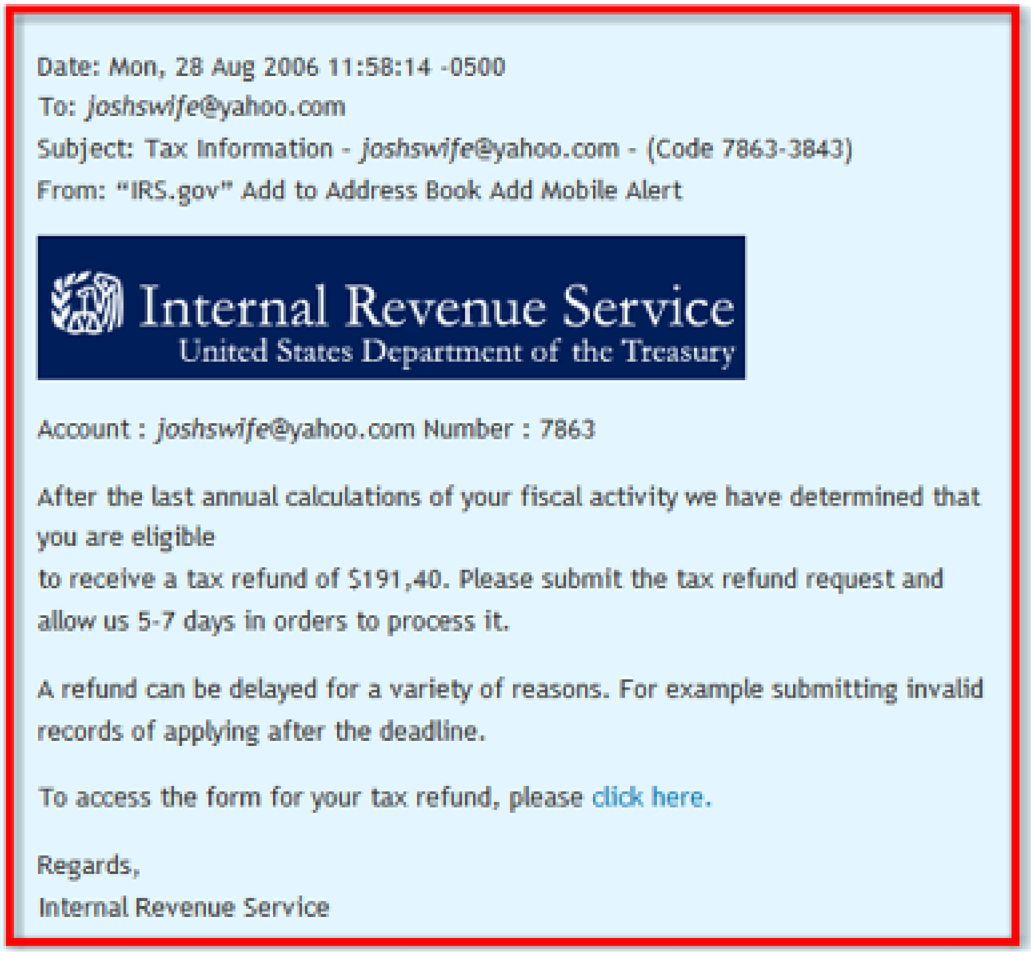
Only you can provide your own finger print scan, retinal scan or palm scan.

PHISHING

Are you a fish in a big Phishing pond?

Phishing is a social engineering technique to obtain personal information from you, like your social security number, credit card number, passwords, bank account numbers, to name a few. The techniques used are phony emails and certain phishing web sites.

Even the most educated can be fooled by phishing attacks. The example on the right fooled A WOMAN that had A PhD from Harvard.



Date: Mon, 28 Aug 2006 11:58:14 -0500
To: *joshswife@yahoo.com*
Subject: Tax Information - *joshswife@yahoo.com* - (Code 7863-3843)
From: "IRS.gov" Add to Address Book Add Mobile Alert

Internal Revenue Service
United States Department of the Treasury

Account : *joshswife@yahoo.com* Number : 7863

After the last annual calculations of your fiscal activity we have determined that you are eligible
to receive a tax refund of $191,40. Please submit the tax refund request and allow us 5-7 days in orders to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records of applying after the deadline.

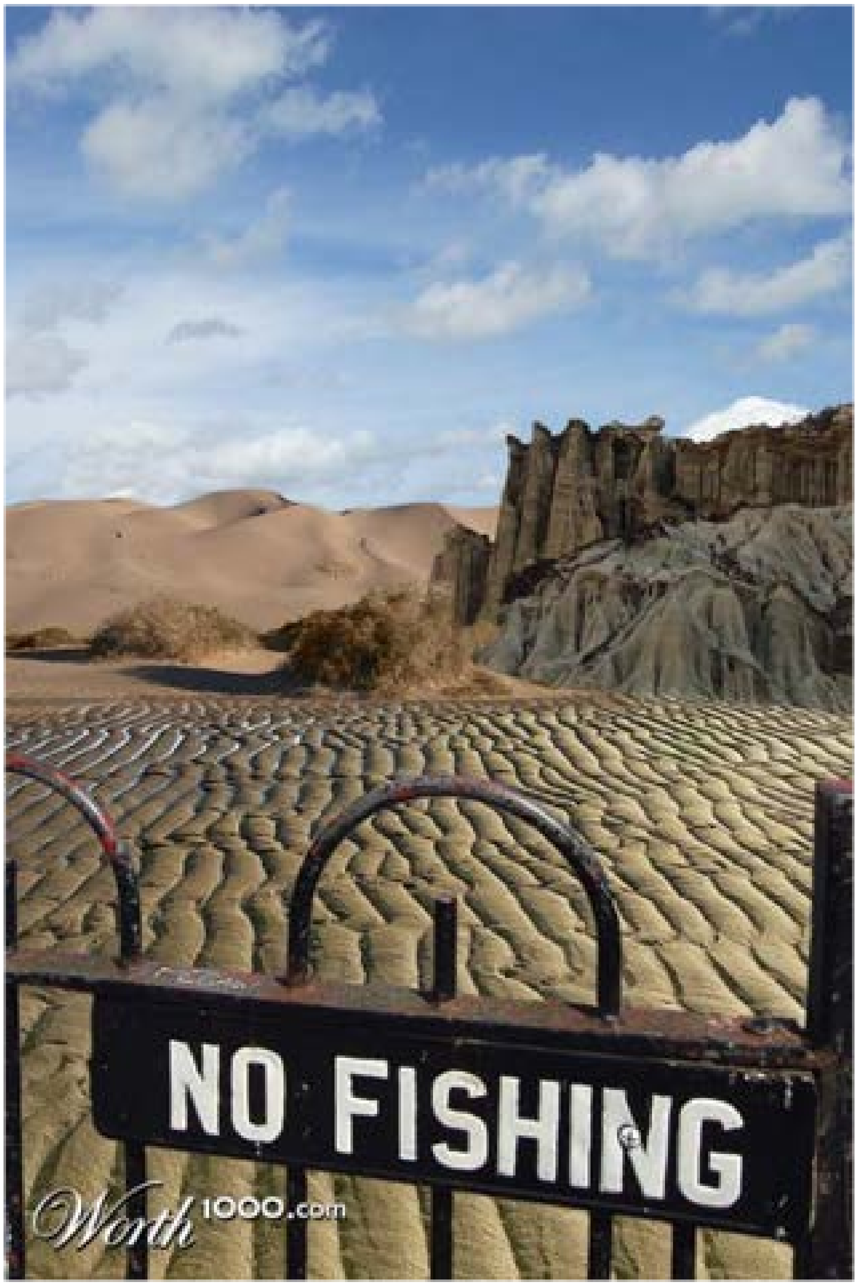
To access the form for your tax refund, please click here.

Regards,
Internal Revenue Service

A WORD OF WARNING!

If a web site or an email is asking for personal information then it is a scam.

Legitimate institutions that need personal information would not ask for it using email or a web site.   Don't be fooled.



SOCIAL NETWORKING ATTACKS

If you belong to Facebook, or to similar social networking sites, then you belong to a social networking group and you are a target.

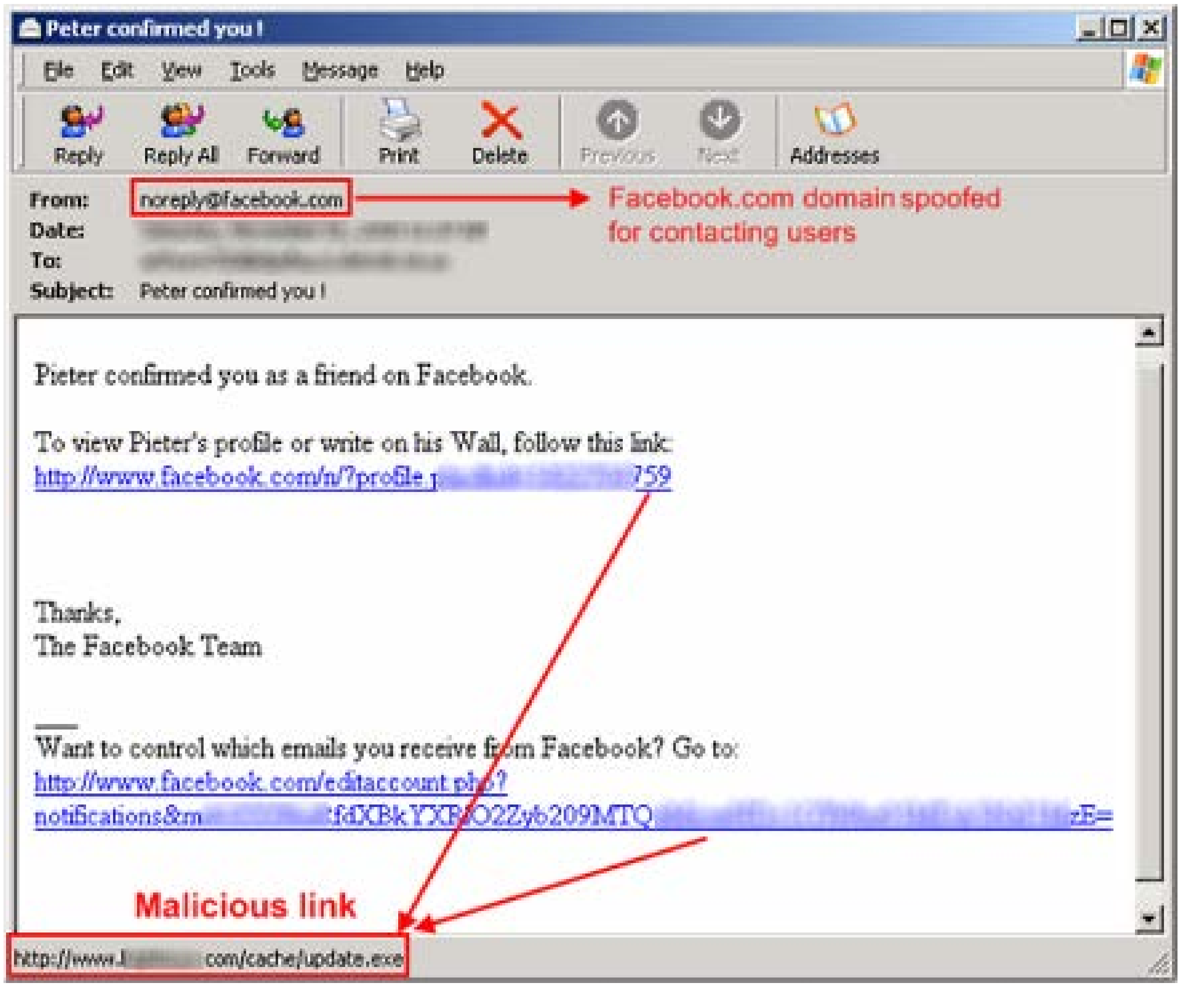
Generally, if you are cautious about who you have in your group (who you trust) and what you click on, your risk of attack is reduced.

DO NOT MAKE YOUR PERSONAL INFORMATION PUBLIC!

You are a target because of the wealth of information that can be obtained from a social networking group.   Personal information that you place on these sites can be obtained easily if you make the information public and can be obtained either through a vulnerability in the web site or through someone impersonating a friend.

Click on the link below to find out how to make Facebook more secure and safe.

http://personalweb.about.com/od/makefriendsonfacebook/a/faceprivsetting.htm



From: noreply@facebook.com

Date: [redacted]

To: [redacted]

Subject: Peter confirmed you !

Facebook.com domain spoofed for contacting users

Pieter confirmed you as a friend on Facebook.

To view Pieter's profile or write on his Wall, follow this link:
http://www.facebook.com/n/?profile.p[redacted]759

Thanks,
The Facebook Team

Want to control which emails you receive from Facebook? Go to:
http://www.facebook.com/editaccount.php?notifications&m[redacted]fdXBkYXRlO2Zyb209MTQ[redacted]zE=

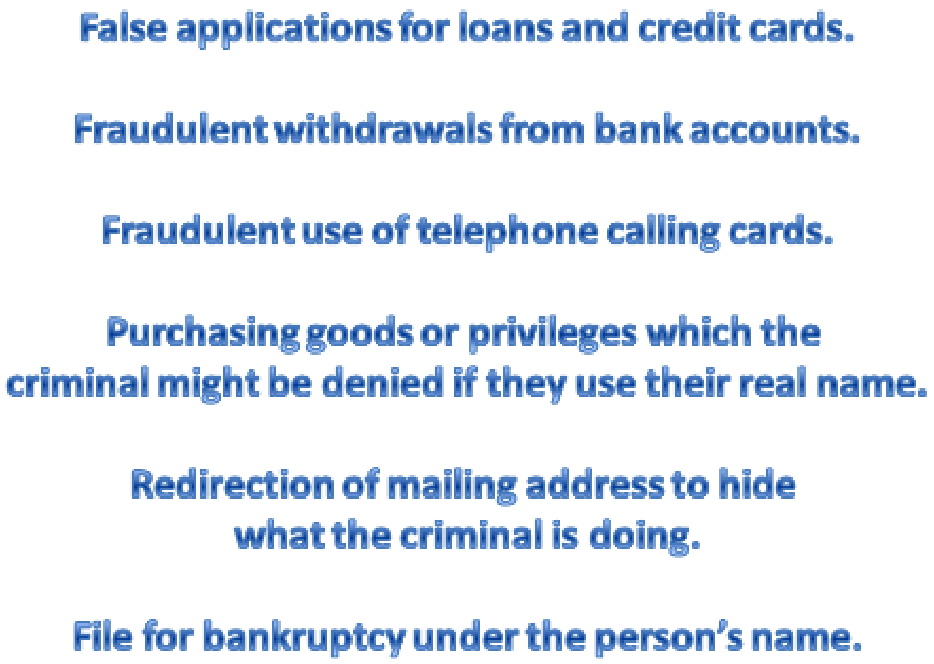
Malicious link

http://www.J[redacted]com/cache/update.exe

IDENTITY THEFT

Identity theft is a crime and a federal offense (1998). It is when someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

So, what does the criminal use with your identity? See the list of possible uses below:



False applications for loans and credit cards.

Fraudulent withdrawals from bank accounts.

Fraudulent use of telephone calling cards.

Purchasing goods or privileges which the
criminal might be denied if they use their real name.

Redirection of mailing address to hide
what the criminal is doing.

File for bankruptcy under the person's name.

The sections below describe how your identity could be stolen:

SHOULDER SURFING

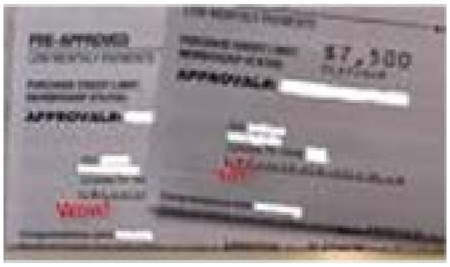
Criminals can watch you from nearby while you punch in your telephone calling card number or credit card number. They can listen to you give you credit card number to a sales agent on the phone. They can follow you into the schools administrative offices and listen and watch for you to reference you Social Security Card number.

DUMPSTER DIVING

Criminals pick through your garbage or a communal dumpster or trash bin – to obtain copies of your checks, credit card, and bank or investment statements.   This is an easy way to obtain control of your accounts and assume your identity.

PREAPPROVED CREDIT

Through dumpster diving, criminals can obtain discarded, “preapproved” credit cards and then activate and use them without your knowledge.



THROUGH SPAM

Criminals engage in sending unsolicited E-mail (spam) to obtain personal information as mentioned in the Phishing section.   When you are asked for personal information in an E-mail the E-mail generally requests identifying data. In return a promise is made that you hope you will benefit from. Some users don't realize that in many cases the requester has no intention of keeping their promise.