



Ethical Hacking and Countermeasures

Version 6



Module XIII

Hacking Email Accounts

Email scammers target university students

By Shaun Nichols in California
VNU Net - Monday, February 4 09:00 am

A new targeted phishing attack is being used to the email accounts of American university students.

Researchers at Sans said that the attacks are being disguised as messages from administrators who are performing a "database update".

The messages state that in order to keep their email accounts, the students must "verify" the accounts by replying to the message with such account details as user names, passwords, and the student's date of birth.

Researcher Mark Hofman wrote in a report posted on the Internet Storm Center blog that the attacks appear to be similar to a wave of phishing attacks on European ISPs that were spotted earlier this year.

The attackers use email addresses with the name of the [school](#), though the accounts are hosted by an external e-mail service such as Hotmail.

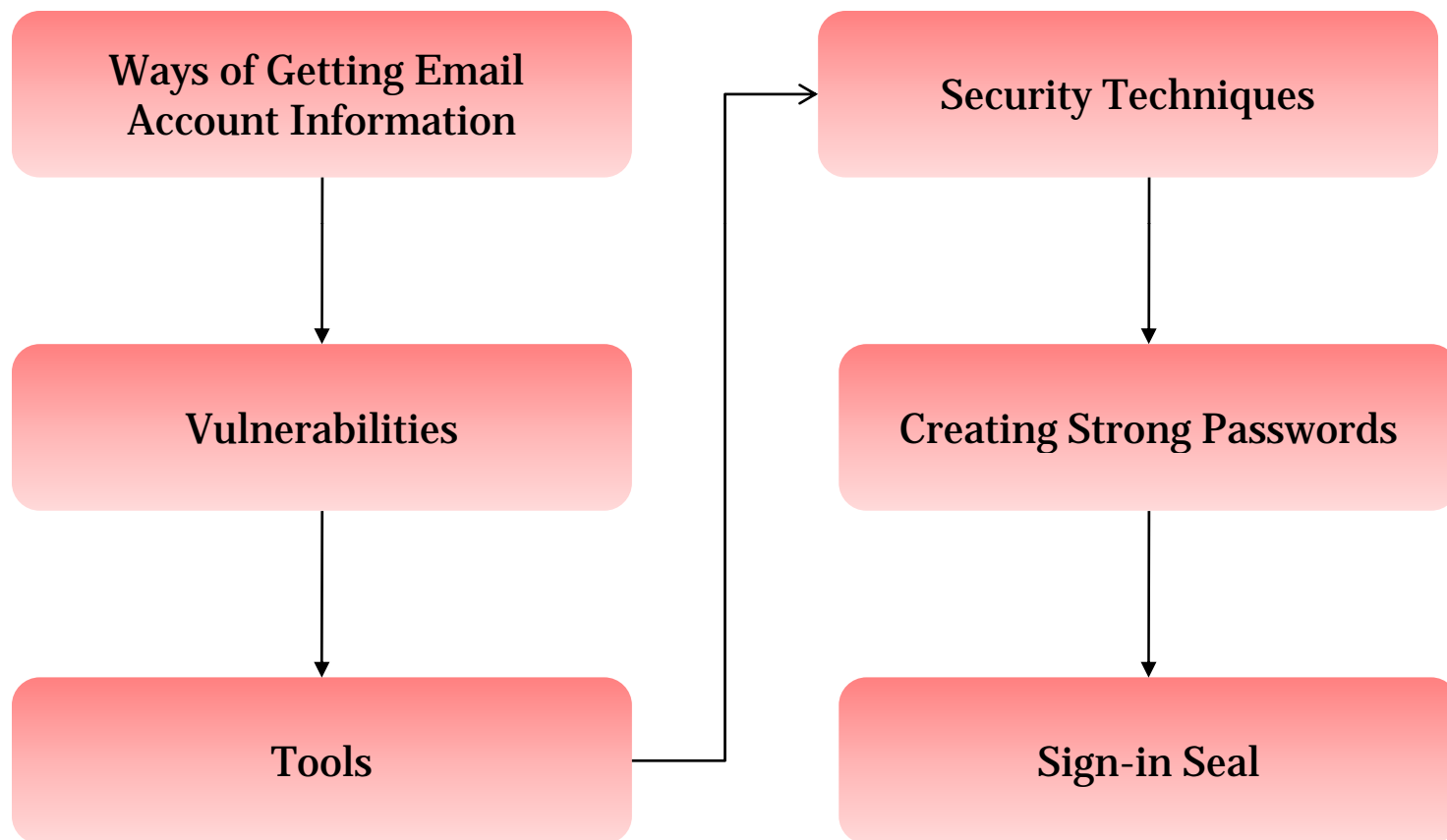
Hofman noted that because the attack targets individual students, few messages are sent and the emails will often slip past spam filters.

The researcher suggests that administrators should be on the lookout for a large volume of incoming messages from the same address, as well as a large volume of messages with multiple recipients. Students should also be warned about the attacks, said Hofman.

Source: <http://uk.news.yahoo.com/>

This module will familiarize you with:

- Ways of Getting Email Account Information
- Vulnerabilities
- Tools
- Security Techniques
- Creating Strong Passwords
- Sign-in Seal



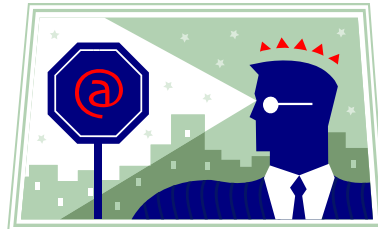


Introduction

Hacking email accounts has become a serious threat

Email accounts are the repositories where people store their private information or even their business data

Due to the widespread use of the Internet techniques and tools hacker can access the user ID and email password



Ways for Getting Email Account Information

Stealing Cookies

Social Engineering

Password Phishing



Stealing Cookies

If a web site uses a cookie, or a browser contains the cookie, then every time you visit that website, the browser transfers the cookie to that website

If a user's cookie is stolen by an attacker, he/she can impersonate the user

If the data present in the cookies is not encrypted, then after stealing the cookies an attacker can see the information which may contain the username and the password



Social Engineering

Social engineering is defined as a “non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.”

Social engineering hackers persuade a target to provide information through a believable trick, rather than infecting a computer with malware through a direct attack

Most of the persons unwittingly give away key information in an email or by answering questions over the phone such as names of their children, wife, email ID, vehicle number and other sensitive information.

Attacker use this information for hacking email accounts



Password Phishing

The process of tricking user to disclose user name and password by sending fake emails or setting up fake website which mimics sign-in pages is called phishing

After gaining Username and password, fraudsters can use personal information to:

Commit identity theft

Charge your credit card

Clear your bank account

Change the previous password



Fraudulent e-mail Messages

You might receive an e-mail message from bank asking for updated information

The message provides the target user with a link to a legitimate site but redirects the user to a spoofed one

That message ask for Login, password, and other sensitive information

Attacker can use this information for hacking email accounts



Caution: Scam Warning Is A Scam

'Warning' asks bank customers to call a toll-free number

By Mark Huffman
ConsumerAffairs.Com

February 11, 2008

You've got to hand it to those identity thieves - they're usually a step ahead of the banks whose customers are their primary targets.

When a [spam email](#) went out last month, disguised as a message from Valley National Bank's security department, the bank quickly responded, posting a warning on its Web site.

"A fraudulent e-mail has circulated to some Valley customers claiming that the bank has temporarily suspended their account due to "Billing Failure," the warning states. "This e-mail also provides a link to click on in order to complete an account update to unlock their account."

Source: <http://www.consumeraffairs.com/>



Vulnerabilities

Vulnerabilities: Web Email

While using web based email service, after clicking a link present in the email body, it transfers from URL of the current page (webmail URL) to the next page (link present)

This information is transmitted through third party web servers

Information can include:

```
http://us.f97.mail.yahoo.com/ym/ShowLetter;box=Inbox  
&MsgId=240_1916298_12822_1346_654_0_3386&NEXT  
=2&inc=&num=&Search=&YY=82346&order=down&sort  
=date&pos=0
```

- Email address
- Login ID
- Actual name

```
http://my.mail.iname.com/scripts/mail/mesg.mail?login=  
morell:planetmail.com&folder=INBOX&order=Newest&  
msg_uid=1018455590&mview=
```

```
http://qmail.pdq.net/MBX/lsfranks@pdq.net/ID=  
5CB38F37/MSG:1
```

Vulnerabilities: Reaper Exploit

The confidentiality of email can be brought down by the micro virus like Reaper Exploit

Reaper Exploit works in the background and sends a copy of reply or forwarded mails to the hacker

This exploit uses the functionality of DHTML in Internet Explorer, used by Microsoft outlook

Email clients who make use of the internet explorer as their HTML engine are vulnerable

Email scripting should be turned off, to prevent from this attack





Email Hacking Tools

Tool: Advanced Stealth Email Redirector

This program monitors outgoing traffic of the target PC's email client and intercepts all the messages sent from it

Intercepted emails are forwarded to a pre-specified email address

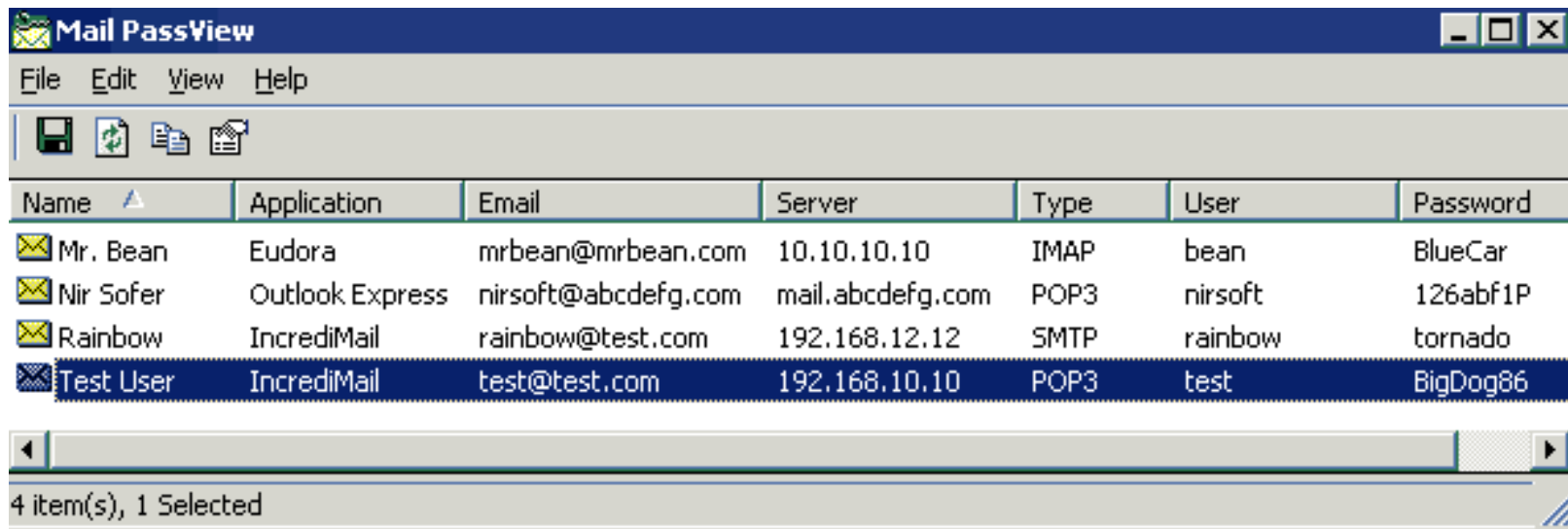
Advanced SER does not intercept emails sent from web-based email services like www.yahoo.com, www.hotmail.com etc



Mail PassView is a small password-recovery tool that reveals the passwords and other account details for the following email clients:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003/2007 (POP3, IMAP, HTTP and SMTP Accounts)
- Windows Mail
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail - If the password is saved in Yahoo! Messenger application
- Hotmail/MSN mail - If the password is saved in MSN Messenger application
- Gmail - If the password is saved by Gmail Notifier application, Google Desktop, or by Google Talk

Mail PassView: Screenshot



The screenshot shows the Mail PassView application window. The title bar reads "Mail PassView". The menu bar includes "File", "Edit", "View", and "Help". Below the menu bar is a toolbar with icons for saving, opening, printing, and deleting. The main area contains a table with the following data:

Name	Application	Email	Server	Type	User	Password
Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
Rainbow	IncrediMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
Test User	IncrediMail	test@test.com	192.168.10.10	POP3	test	BigDog86

At the bottom of the window, a status bar indicates "4 item(s), 1 Selected".

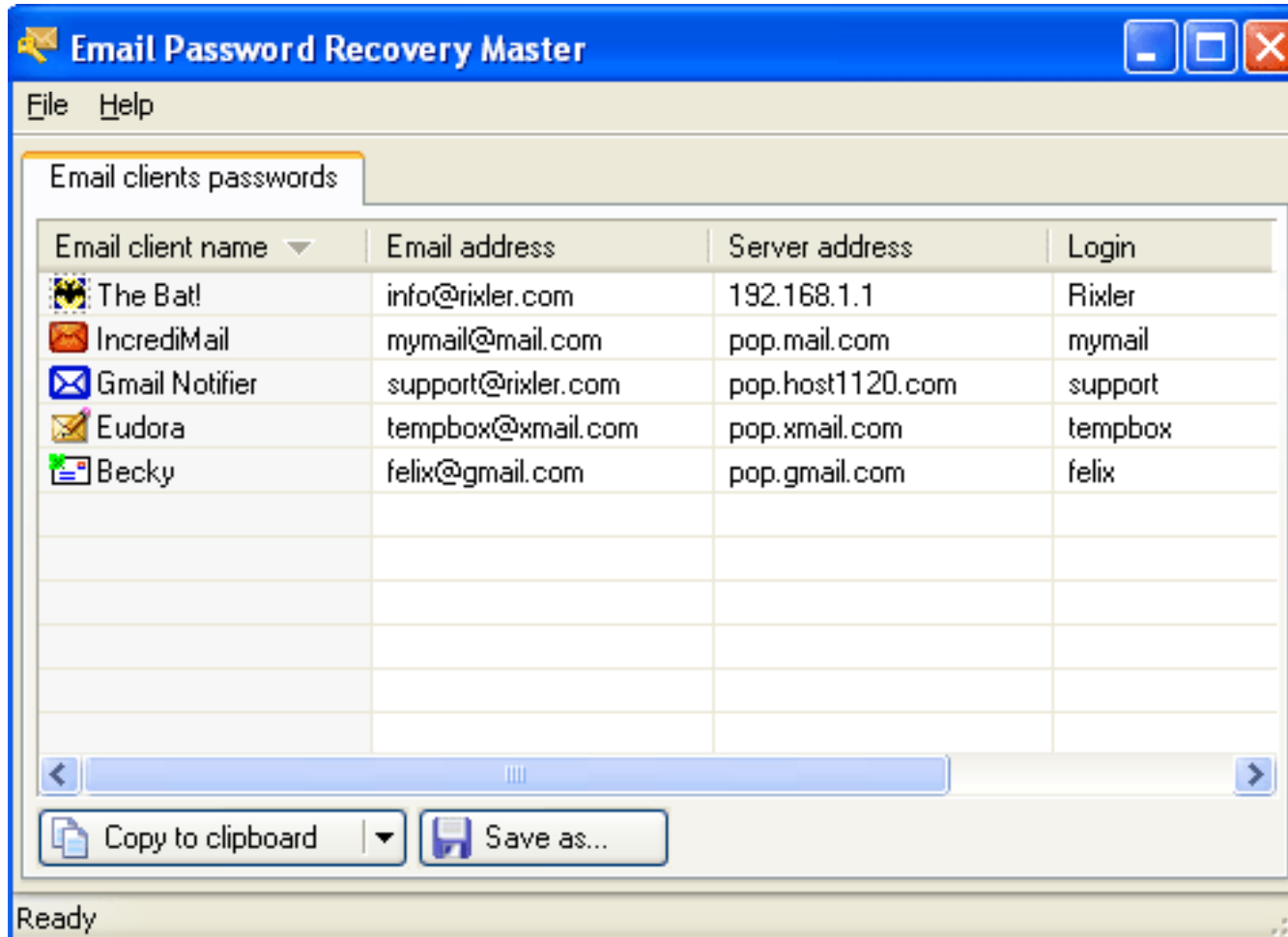
Tool: Email Password Recovery Master

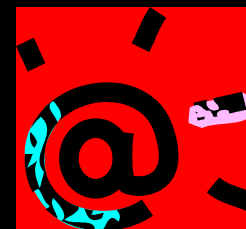
Email Password Recovery Master is a program that displays logins and passwords for email accounts stored by:

- Eudora
- The Bat!
- Becky
- IncrediMail
- Gmail Notifier
- Group Mail Free
- PocoMail
- Forte Agent
- Mail.Ru Agent
- Scribe



Email Password Recovery Master: Screenshot





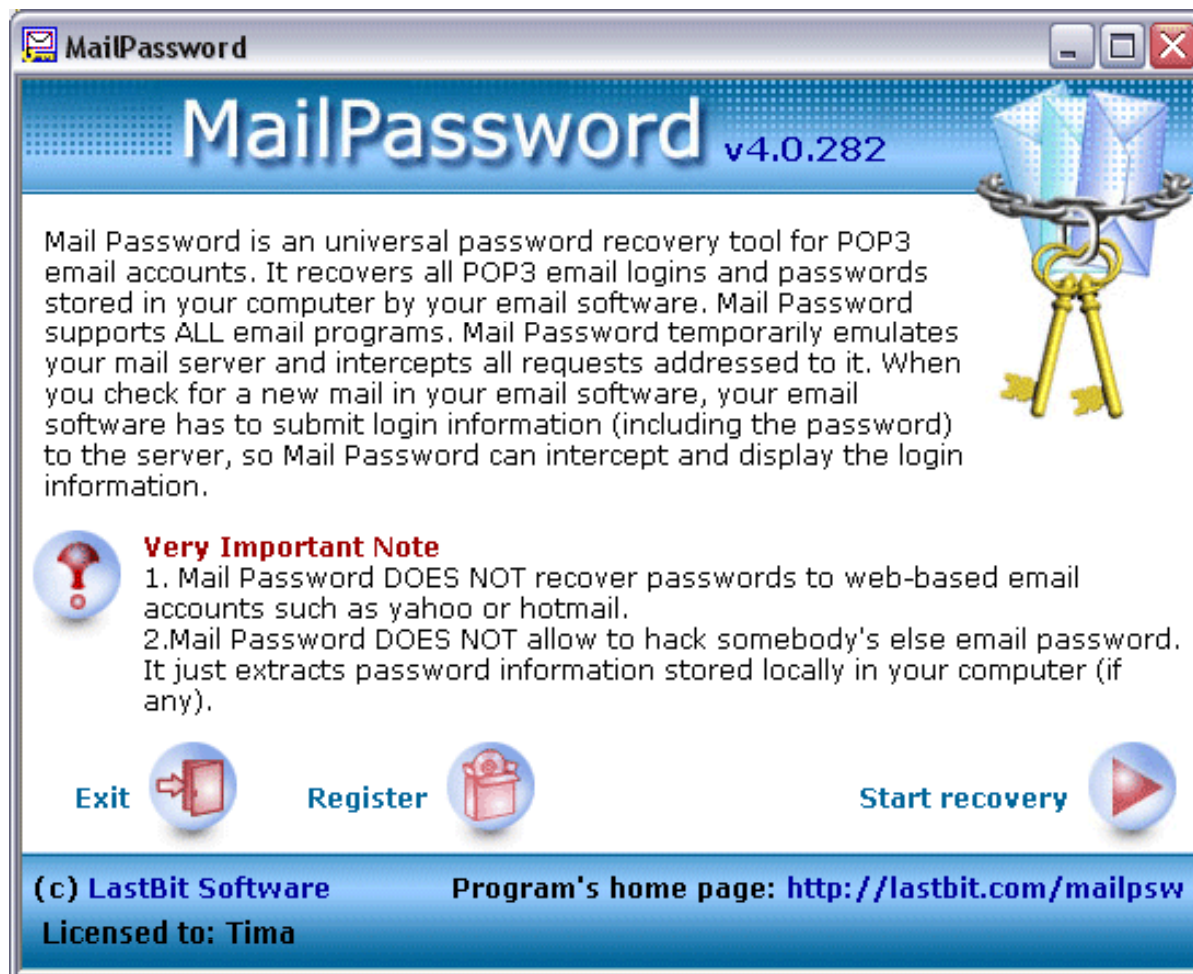
Mail Password is a universal password recovery tool for POP3 email accounts

It recovers all POP3 email logins and passwords stored on your computer by your email software

Mail Password emulates a POP3 server and the E-mail client returns the password

It supports all email programs, including Outlook, Eudora, The Bat! and more

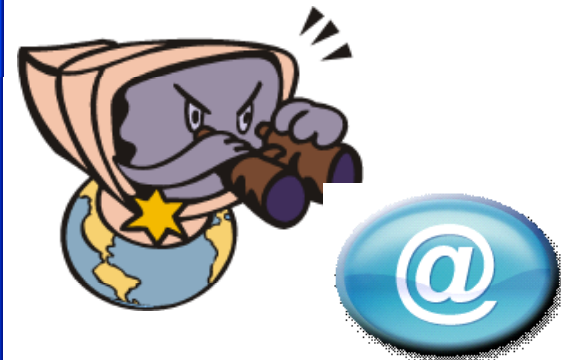
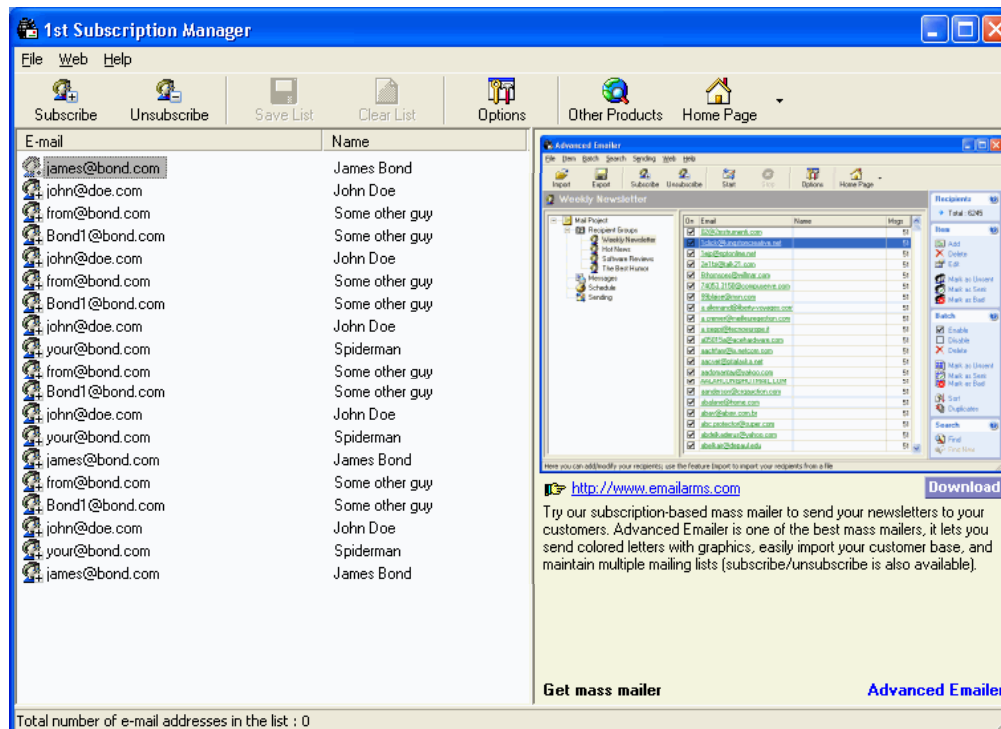
Mail Password: Screenshot



Email Finder Pro

Email Finder Pro extracts business emails from a file or a directory containing files

Fast and simple email address extraction utility



Email Spider Easy

Email Spider Easy is a targeted bulk email marketing software

Quickly and automatically search and spider from search engine to find e-mail addresses

Integrated with 90 top popular search engines: Yahoo, Google, MSN, AOL, and so on

Fast search speed allows upto 500 email extraction thread simultaneously



Email Spider Easy: Screenshot

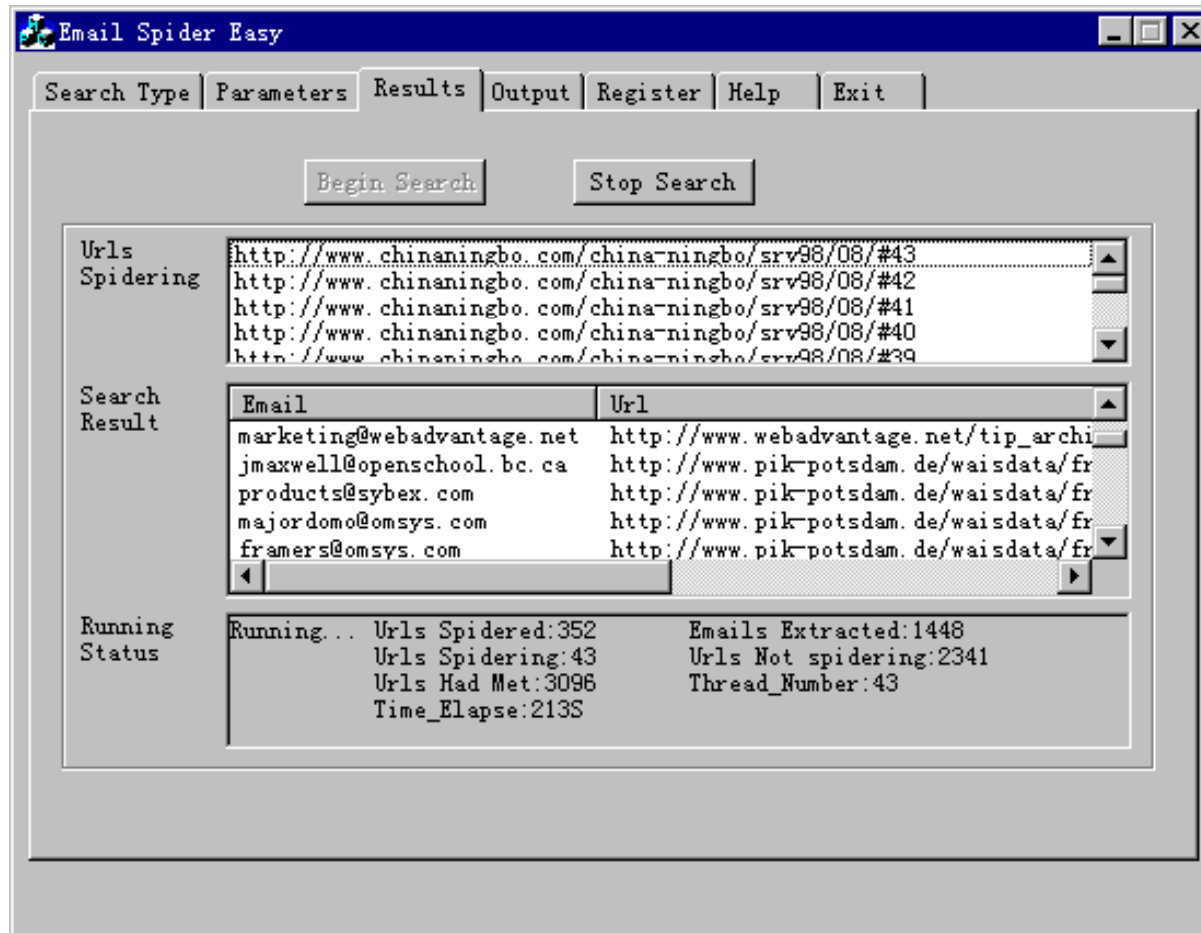
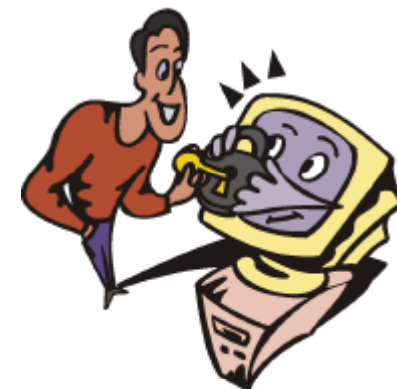


Figure: Email Spider Easy

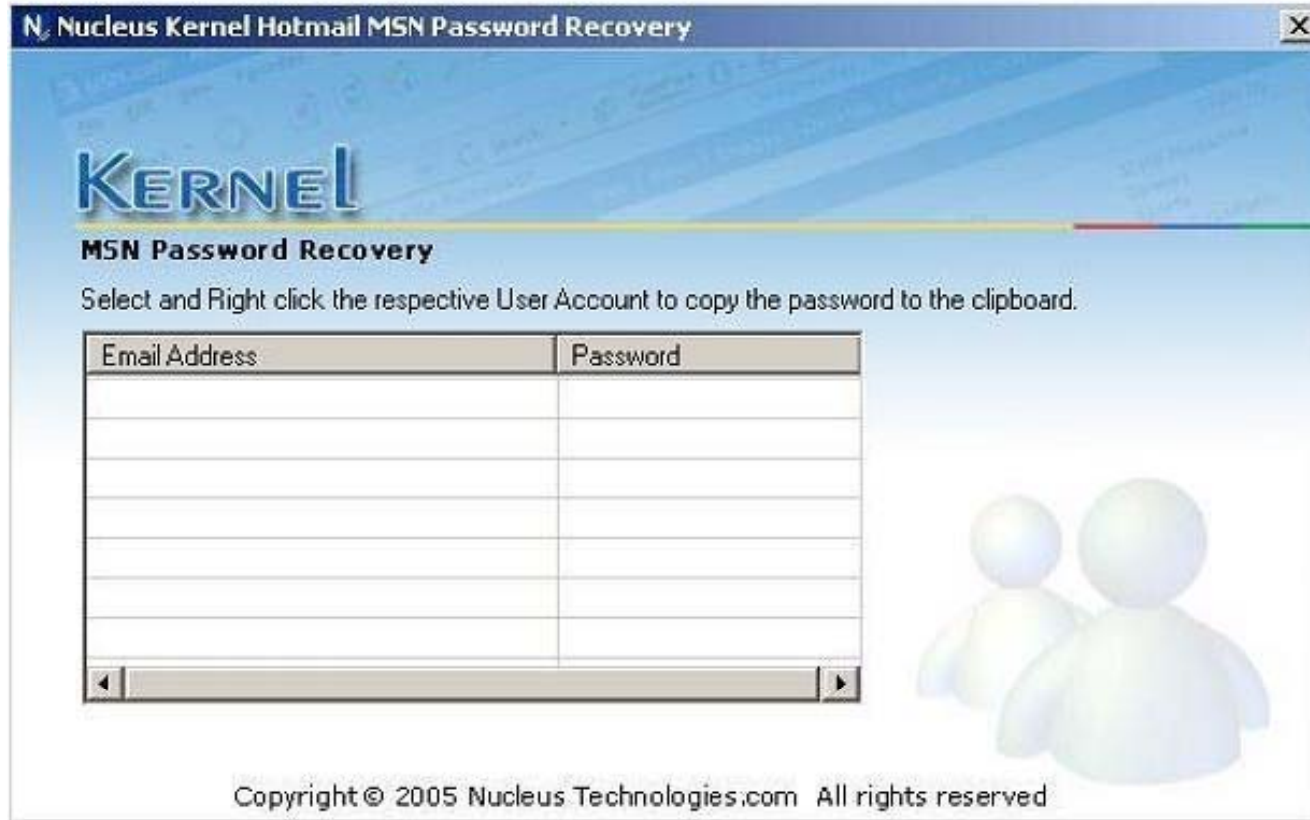
Kernel Hotmail MSN Password Recovery

Kernel Hotmail & MSN Password Recovery software recovers the stored or saved password of the Hotmail and MSN Messenger account from your computer

Supports all versions of MSN Messenger



Kernel Hotmail MSN Password Recovery: Screenshot



Retrieve Forgotten Yahoo Password

Retrieve Forgotten Yahoo Password cracks Gmail, Yahoo passwords

It retrieves encrypted characters hidden behind asterisk****

It restores hacked pop3 email IDs and passwords

Features:

- Decodes the coded user and owner password which provides the standard security to prevent PDF files from copying, printing, and editing
- It reveals the Yahoo, Hotmail, Gmail, Indiatimes, Rediffmail, and MSN account passwords

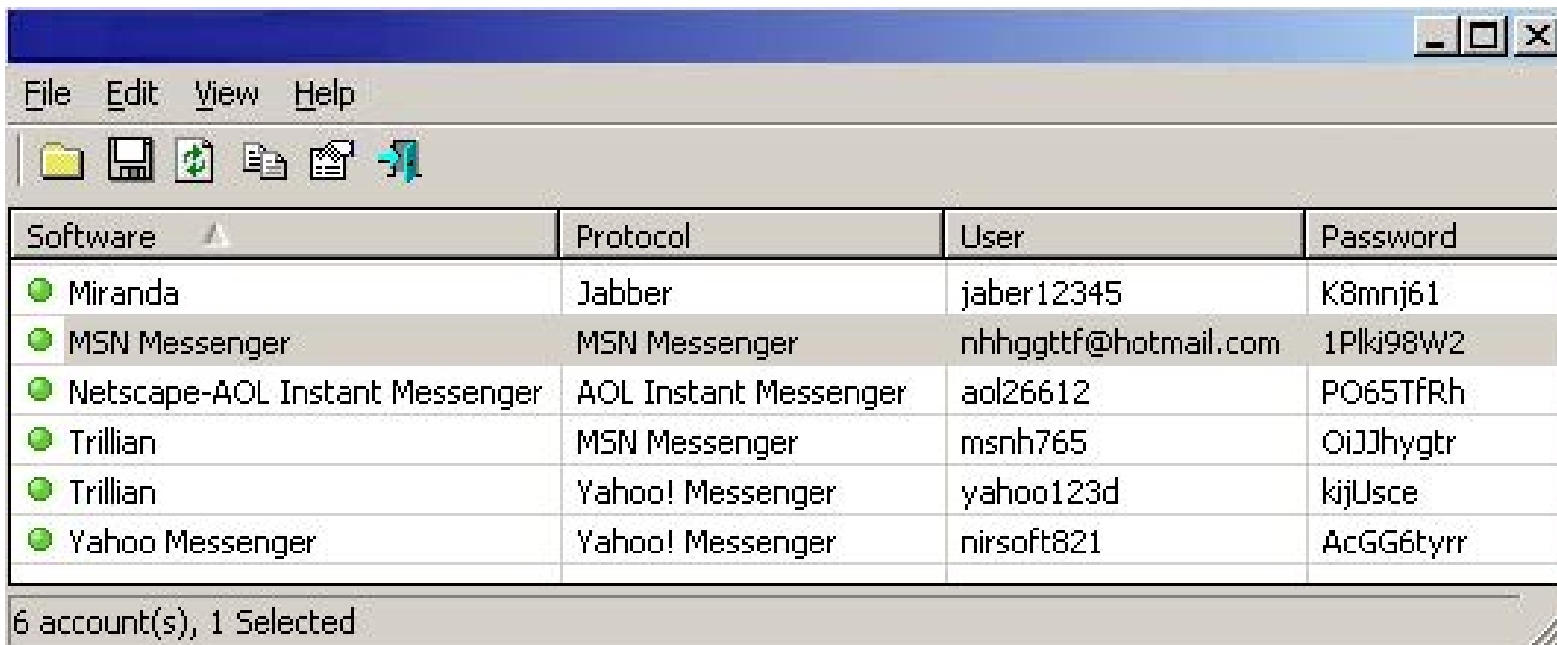
Retrieve Forgotten Yahoo Password: Screenshot



Figure: Retrieve Forgotten Yahoo Password

MegaHackerZ helps you crack passwords to any email address

It will help you to get the password you desire, instantly



The screenshot shows a window with a menu bar (File, Edit, View, Help) and a toolbar with icons for file operations. Below the toolbar is a table with four columns: Software, Protocol, User, and Password. The table contains six rows of data, each with a green circular icon in the first column. At the bottom of the window, a status bar indicates '6 account(s), 1 Selected'.

Software	Protocol	User	Password
Miranda	Jabber	jaber12345	K8mnj61
MSN Messenger	MSN Messenger	nhhggttf@hotmail.com	1Plki98W2
Netscape-AOL Instant Messenger	AOL Instant Messenger	aol26612	PO65TFRh
Trillian	MSN Messenger	msnh765	OiJJhygtr
Trillian	Yahoo! Messenger	yahoo123d	kjJUsce
Yahoo Messenger	Yahoo! Messenger	nirsoft821	AcGG6tyrr

6 account(s), 1 Selected

The Email Password hacking software will get you any Password you need

It allows to take command and control of any email





Securing Email Accounts

Creating Strong Passwords

Best way to protect from hackers is to use the strong password

A strong password is one which cannot be determined by automated programs

A strong password contains:

- Seven to sixteen characters
- Choose a phrase or combination of words
- Uses three of the following four types of characters:
 - Uppercase letters (A, B, C)
 - Lowercase letters (a, b, c)
 - Numerals (1, 2, 3)
 - Special characters (` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /)



Creating Strong Passwords: Change Password Screenshot

Change password

To reset your password, provide your current password OR the answer to your security question.

Current password:

OR

What was your first phone number?

New password: Password strength: **Strong**

Confirm new password:

Creating Strong Passwords: Trouble Signing In Screenshot

YAHOO! [Yahoo! - Help](#)

Sorry That You're Having Trouble Signing In

We know that not being able to sign in can be frustrating, so we'll try to make this as quick and easy as possible. To get started, enter your Yahoo! ID and let us know if you've ever used a credit card with Yahoo!.

What's your Yahoo! ID?

Yahoo! ID:

[I don't know my Yahoo! ID](#)

Verify your identity with a previously-used credit card

I have never used a credit card with Yahoo!

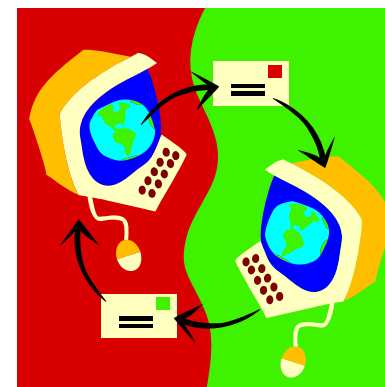
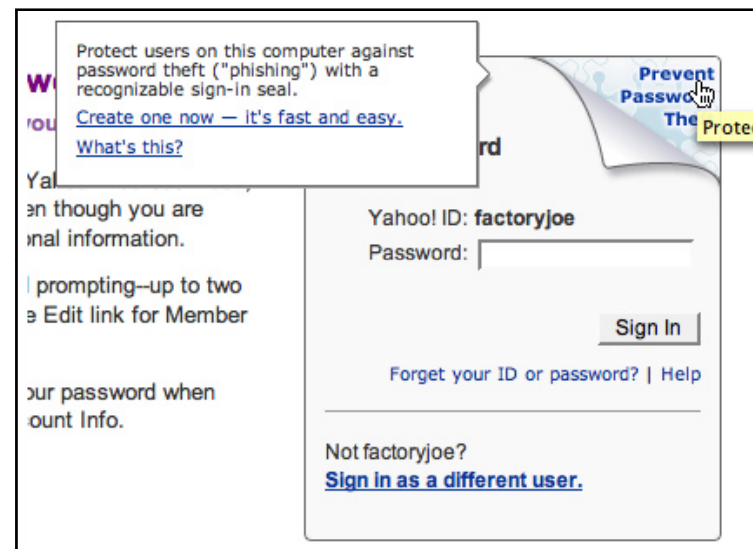
I have used a credit card with Yahoo!

Sign-in seal protects account from phishing

Sign-in seal is a custom text or image set up by the user on the computer

User needs to create different sign-in seal for different browsers and computers

Do not create sign-in seal on networked computer



Alternate Email Address

Alternate email address are prompted at signup

At the time of password recovery, passwords can be sent to the alternate email address

In case you forget your ID or password...

Alternate Email

Security Question

Your Answer

Use 4 characters or more — not case sensitive.

Keep Me Signed In/ Remember Me

When you login on any site, there is checkbox like "Keep me signed in" or "Remember Me"

If you select this option, next time it will automatically open your account in same computer

If attacker handles such a system, he will get access to the email account

If you are using a public computer, it is recommended that you uncheck the checkbox

Already have a Yahoo! ID?

Sign in.

Yahoo! ID:

Password:

Keep me signed in
for 2 weeks unless I sign out. *New!*
[Uncheck if on a shared computer]

Tool: Email Protector

Email Protector protects password and automatically logs off your email account

Email Protector shows you how to add password protection to your Outlook Express email

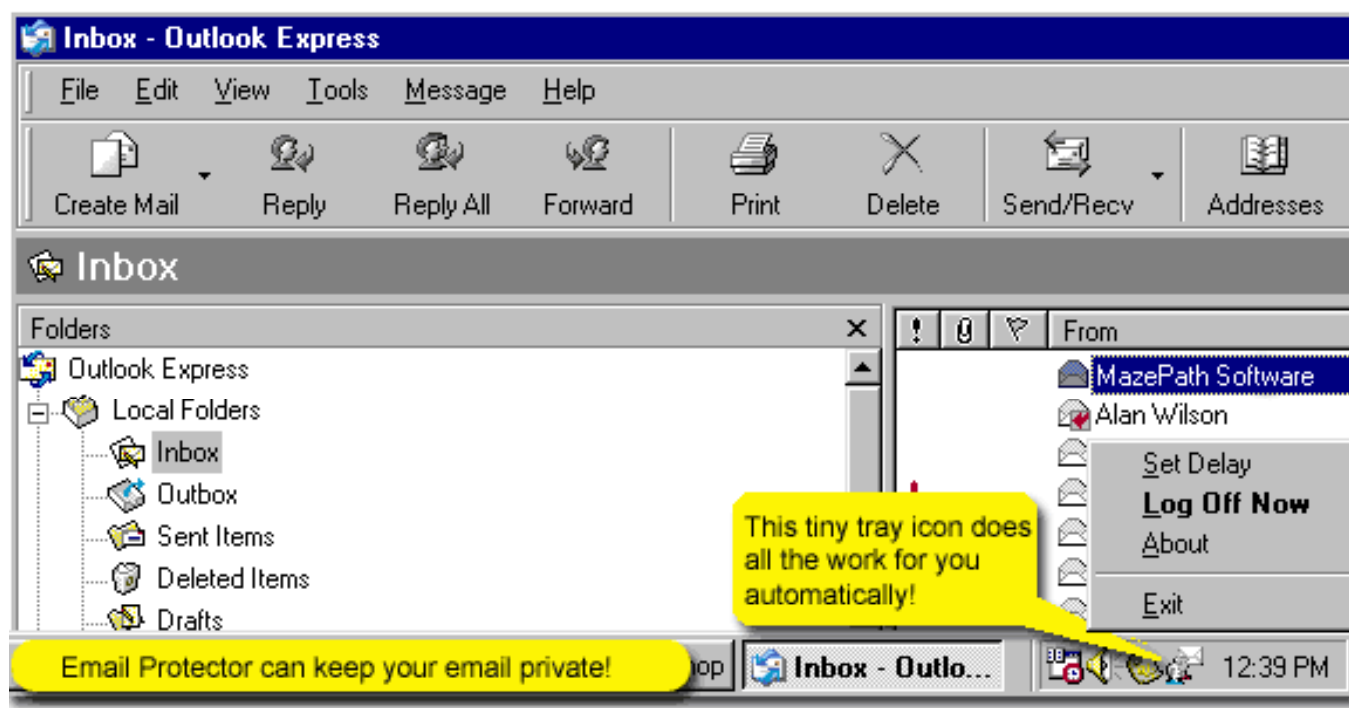


Figure: Email Protector

Internet Service Provider (ISP) stores copies of all your email messages on its mail servers

All the information kept on the servers can be easily used against you

Email Security always breaks email messages addressed to a group of people to individual messages to ensure your as well as respondent's security



Email Security: Screenshot

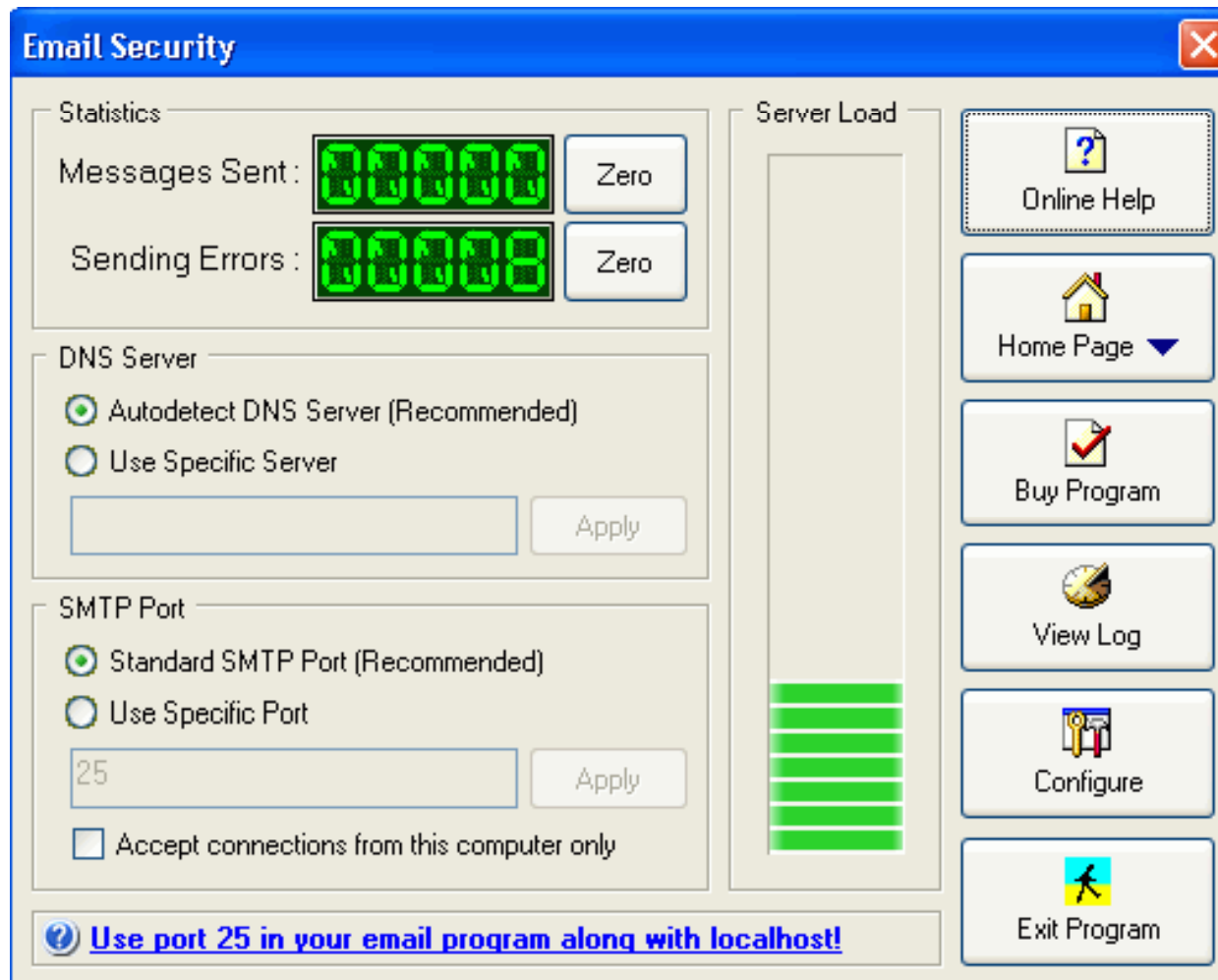


Figure: Email Security Main Window

Tool: EmailSanitizer

EmailSanitizer is a filter between the incoming email server, and your computer

EmailSanitizer Lets you keep track of how much spam is being stopped and how many viruses are being destroyed



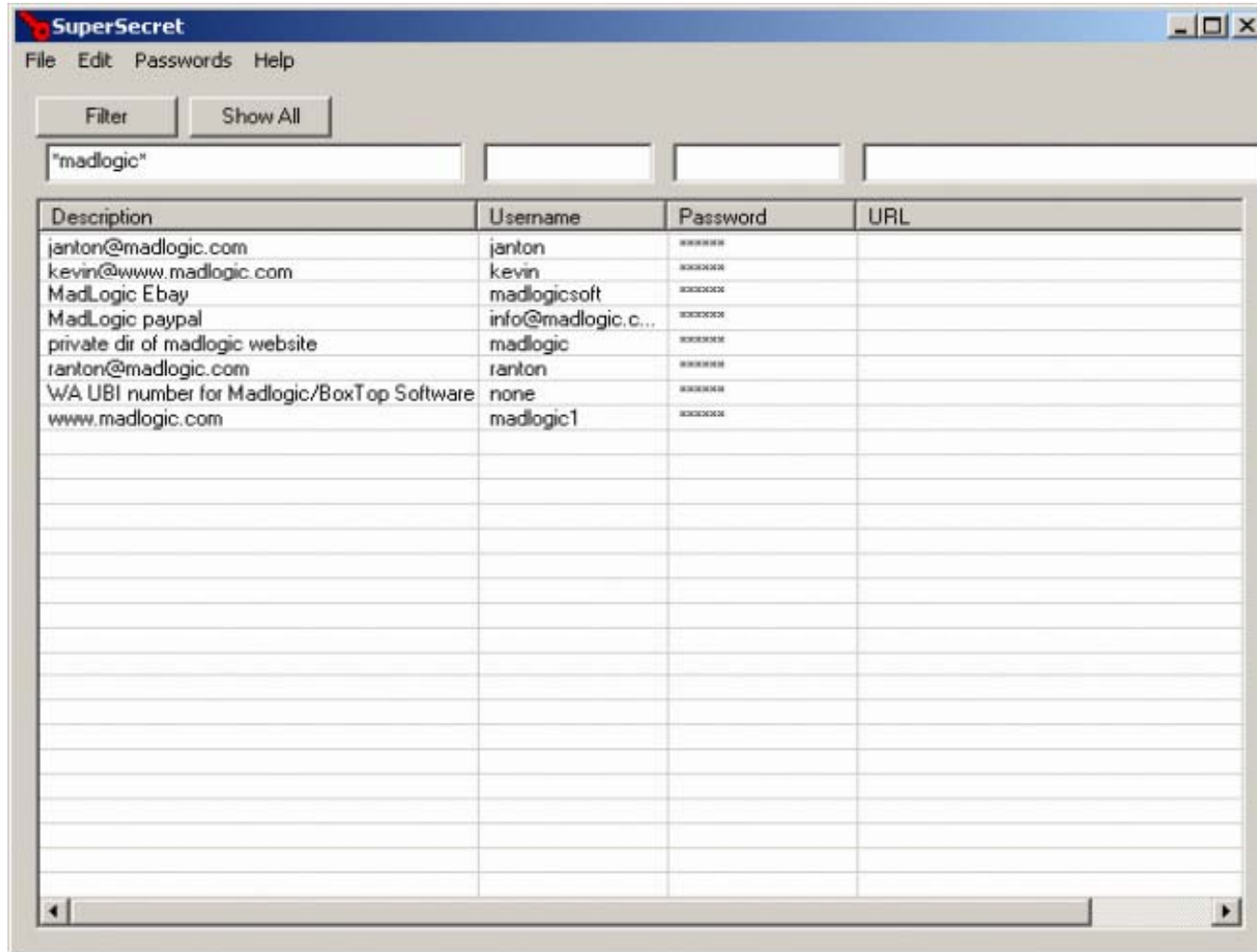
Tool: SuperSecret

SuperSecret provides secure storage for all of your logins and passwords so that you only have one password to remember from now on

Only one password is required to use SuperSecret

All of your other account and password information is stored securely in an encrypted format on your computer and can be accessed only with your one and only password

SuperSecret: Screenshot



Username and password can be revealed if it is stored in cookie and is not encrypted

The confidentiality of email can be brought down by the micro virus like Reaper Exploit

A strong password is one which cannot be determined by automated programs

Copyright 2005 by Randy Glasbergen.
www.glasbergen.com



“For security purposes, the information should make no sense at all to spies and hackers. We’ll bring in someone later to figure out what you meant.”

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



**“The boss is worried about information security,
so he sends his messages one alphabet letter
at a time in random sequence.”**