A close-up photograph of a man's face in profile, looking slightly down. A large snake is draped over his forehead and eyes. The background is a blurred green, suggesting an outdoor setting.

# HOW 2 KILL THE CYBER CRIME SNAKE B4 IT KILLS U

Written By

Research Team

[www.uniqueebook.com](http://www.uniqueebook.com)



# HOW 2 KILL THE CYBER CRIME SNAKE B4 IT KILLS U

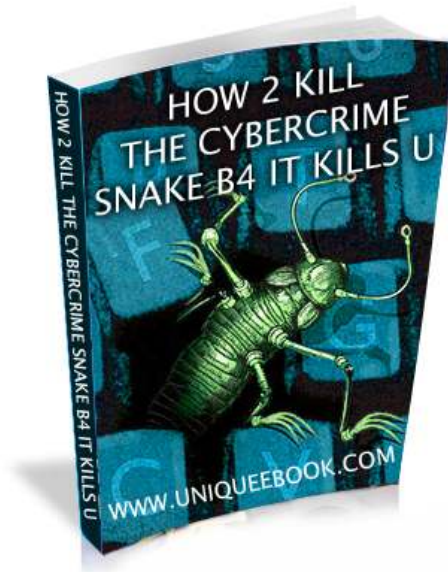
**Written By**  
Research Team  
[www.uniquebook.com](http://www.uniquebook.com)

© 2007-08 [www.uniquebook.com](http://www.uniquebook.com)

**Published by**

UniqueEbook.com  
5715 Will Clayton # 6078  
Humble, TX 77338  
USA

[sales@uniquebook.com](mailto:sales@uniquebook.com)



ALL RIGHTS RESERVED. No part of this report may be reproduced or transmitted in any form whatsoever, electronic, or mechanical, including photocopying, recording, or by any informational storage or retrieval system without express written, dated and signed permission from the author.

**DISCLAIMER AND/OR LEGAL NOTICES:**

The information presented herein represents the view of the author as of the date of publication. Because of the rate with which conditions change, the author reserves the right to alter and update his opinion based on the new conditions. The report is for informational purposes only. While every attempt has been made to verify the information provided in this report, neither the author nor his affiliates/partners assume any responsibility for errors, inaccuracies or omissions. Any slights of people or organizations are unintentional. If advice concerning legal or related matters is needed, the services of a fully qualified professional should be sought. This report is not intended for use as a source of legal or accounting advice. You should be aware of any laws, which govern business transactions or other business practices In your country and state. Any reference to any person or business whether living or dead is purely coincidental.

# CONTENTS

**Introduction** **Page 05**

**CHAPTER 01** **Page 07**  
**GENERAL FEATURES**

- Spamming & Criminal Copyright Crimes
- Unauthorized Access Threats
- Theft of Service
- Social Engineering Frauds
- Virus / Worm Attacks

**CHAPTER 02** **Page 14**  
**INFORMATION TRAPPING**

## **Safety Measures**

## **Spam Features**

## **Major E-Mail Felonies**

- **Scam**
- **Phishing**
  - How to identify Phishing e-mail
  - Company
  - Spelling and Grammar
  - Missing account information
  - Deadlines
  - Links

## **What to do if you're not sure If an E-mail is Official**

## **Commonly Address Issues of Phishing E-mails**

- Account issues
- Credit card
- Confirming orders

## **Common Companies Affected by Phishing**

## **Frequently Received Spams**

- Work-at-Home Scams (Easy Earning Scams)
- Weight Loss Scams (Fake online Pharmacies)
- Cure-All Products (Miracle Cures)
- Check Overpayment Scams
- Pay-in-Advance Credit Offers (Pay First Scams)
- Debt Relief
- Investment Schemes
- The Nigerian Email Scam

**Unauthorized Access – Outsiders**

- **Terminology**
  - Hacker
  - Cracker
  - Phreaker
- **Hacker's Dictionary**
  - Serialz
  - Key Generators
  - Crackz
  - Anonymous Senders
  - Bombers
  - Flooders
  - Sniffing Tools
  - Key Loggers
  - Spoofing Tools

**Unauthorized Access – Insiders**

- **Glimpses of Creative Felony**
- **Minimizing Risks**
  - Enable WEP
  - Change your SSID
  - Change default password
  - Enable Filtering
  - Turn off

**The Nature of the Problem**

**Whispering Facts**

**How Does Identity Theft Occur?**

**Investigation & Prosecution**

- Federal Criminal Laws
- Other Federal Offenses
- Recent Federal Cases
- Federal Credit Laws

**Preventive Measures**

- Only Share Information When Necessary
- Exercise Caution Providing Information Publicly
- Exercise Caution Providing Information Publicly
- Secure Mailbox
- Secure Personal Computer
- Confirm a Secure Location

- Shred Nonessential Material Containing Identity Information
- "Sanitize" the Contents of Garbage and Recycling
- Shredding Identity Information
- Remove Your Name from Mailing Lists
- Carefully Review Financial Statements
- Periodically Request Copies of Credit Reports

**CHAPTER 5**  
**PASSWORD, SECURITY & CONVENIENCE**

**Page 71**

**Useful One-liner**  
**Designing A Password**  
**Number of Users Per Password**  
**Design of the Protected Software**

**Bibliography**  
**CYBER CRIME LAWS**

**Page 77**

# INTRODUCTION

It is hard to say what forms the organized crime will take in the future, but the reality is not very far from some science fiction movies. The growing danger from crimes committed ‘against’ computer or ‘by’ the Computer, is beginning to claim attention worldwide. In most countries, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable digital information. The perception that cyber-crime is perpetrated by hackers, who are loners, and are therefore not inclined to engage in group criminality; and the fact that, to date, most documented cyber-crime reveals that a majority of incidents involve individuals, not groups. Although there are a few reported instances of organized cyber-crime, there is generally no indication that cyber-criminals have attained the gang level of organization.

Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as haven run the risk of having their electronic messages blocked by the network. Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

Cyber crimes differ from most terrestrial crimes in four ways —

- Easy to learn how to commit
- Require few resources relative to the potential damage caused
- Can be committed in a jurisdiction without being physically present in it
- Are often not clearly illegal

Internet criminals don't have to rob banks. With currently available technology, they can just as easily rob tens of thousands of individuals, with less chance of being caught. Cyberspace, in other words, will become the marketplace in which online offenders can prey on legitimate citizens as well as conducting their own income-generating activities. As to the operational advantages cyberspace offers, it gives criminals the chance to conduct their activities with a fair degree of anonymity, to exploit gaps in the laws of various countries and to exploit the lack of resources and other constraints many law enforcement agencies suffer under when trying to deal with online offenders.

# CHAPTER 01

## GENERAL FEATURES

Nowadays Cyber Crime is much known to Internet users. It is essentially a criminal activity where the computer or Internet is a basic tool, target or a place of this misdeed.



The case of the Cyber Crime can be more clearly understood by these following examples:

- Spamming & Criminal Copyright Crimes
- Unauthorized Access Threats
- Theft of Service
- Social Engineering Frauds
- Virus / Worm Attacks

**Spamming & Criminal Copyright Crimes:** One of the things about the Internet that irritates you the most is probably discovering 30 junk mails sitting in your mailbox in the morning. You have to say to yourself, “Oh no! Not again!”.... And you spend the next 5 minutes deleting these uncalled for advertisement mails. Bad way to start your day, isn't it?

Spamming & Criminal Copyright Crimes needs computer or network as a tool to conduct the business, especially those connected through peer-to-peer (p2p, or rarely, ptp) network. Spamming is the kind of abuse to electronic messaging systems to uselessly send unwanted bulk messages. Though E-mail Spam is the most recognized form of Spam, the term is also applied to similar abuses in other media — instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

Spamming is economically viable because advertisers have no operating cost beyond the management of their mailing lists, and it is also virtually impossible to hold senders accountable for their mass mailings. But gradually the Spam is being included in many jurisdictions as a subject of legislation.

**Unauthorized Access Threats:** Now this is also a feature you often encounter while accessing your own mail accounts even at secured servers. You feel real disgust when your own account acts as unfamiliar as others. Imagine a great hurried situation when your id is refusing to take settled passwords, loved and easily remembered, by you. After some consecutive attempts you get tensed and suffer difficulties to re-gain permission in almost all the cases.

This kind of Unauthorized Access Threats includes defeating access controls, malicious code, and denial-of-service attacks. Here computer or network is the target-place of their criminal activity.

Access control is the ability to accept or deny the use of something by a particular user. It is usually secured by authentication, authorization, password or audit. When one or more than one of these codes are hacked, a user receives the message ‘access denied or Unauthorized Access’.

**Theft of Service:** Almost all browsers nowadays provide a service by which you can call using your own network system. While users are getting habituated with this service, they are also struggling to accept the truncated calls and abusive languages as a result of those immoral calls.

In the case of Theft of Service (in particular, telecom fraud) and certain financial frauds, Computer or network is a place of activity. Theft of service, particularly Telecom Fraud, is known as Phreaking — a slang-term used to describe the malicious activity of those people who study, experiment with, or explore communication systems, like equipments and systems connected to public telephone networks. Moreover, it is often associated with Computer Hacking and thus sometimes called the HP Culture, where H stands for hacking and P refers to Phreaking.

**Social Engineering:** Sometimes you feel that your computer or e-mail is being spied by others. Those lucky ones who have not still experienced this kind of monitoring; believe me it's possible!! Researchers in this field call this Social Engineering and say that it is a collection of techniques used to manipulate people into performing actions or monitoring secured and confidential informations. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim. Like 'Nigerian 419', it is also an example of traditional crime which includes hacking-phishing, identity theft, child pornography, online gambling, securities fraud, etc.

**Virus / Worm Attacks:** To describe **Spyware**, it is computer software which if installed on your PC which restricts your interaction thus helping you keep the Computer safe! As the Spyware software developed, this industry has come up rapidly. Also, in response to the same, the anti- Spyware companies have sprung up in action. In order to keep your computers secure, the anti spy ware software's are extremely necessary. A number of laws have been passed to target the software which almost controls the user's functions on his computer.

To understand the functions and know more about the spyware you can log on to <http://www.spywareinfo.com/articles/spyware> . The spy ware program is often accompanied with many more components. The system often has a slow and degraded performance. It takes up most of the Disk place and also has a lot of significant CPU activity which in turn breaks down the computer and slows it. The system crashes are a common site in such cases. Logging on to the net becomes extremely difficult when the Spyware mingles with the networking software. Spy Ware is also called as the "data miner".

To elaborate on adware, it means the advertisements or the banners which are displayed but this happens without the consent of the user. Just like the Viruses or the other worms that affect the computers, the spyware does not do so. Just for the commercial use the spyware manipulates the computers that are infected just for the increase in the commercial gain. Not necessarily does

it spread like the other viruses, like the infected systems and again transmits the same to the other computers. Spyware gets on a system and also the lack in the functioning of the proper software's.

Normally the infected system does not spread from one computer to the other. Spyware comes wrapped up with the software's that can be downloaded. The downloadable software's also the music CD's. Not necessarily does the software do any harm. In any case, the people manufacturing and working on the packaging this software's add spyware.

Spyware or adware are the software which are secretly planted the system by some websites. The promoters and the marketers are even keener on supervising the online etiquettes. It would also want to reveal the web sites that one would want to visit. Most of the advertisers are keen to know more about what is being done by you on the net. Log on to [www.spyware.com](http://www.spyware.com) to get your spy ware!

Virus, Worm or Trojan Horses are malicious programs that can cause severe damage to your computer. Though these three are often pronounced in a breath, they are not the same.

Computer **Virus**, like human viruses, spreads from one computer to another, attaching itself to a program or file, and leaves infections in its journey.

- Almost all viruses are attached to an executable file
- It means that virus can live in your computer without causing any harm unless and until you run the program; therefore, virus can not act without a human action
- People, knowingly or unknowingly, spread viruses by sharing infected files or by sending infectious e-mails

**Worm** is also a programming system and like virus it also spreads from one computer to another.

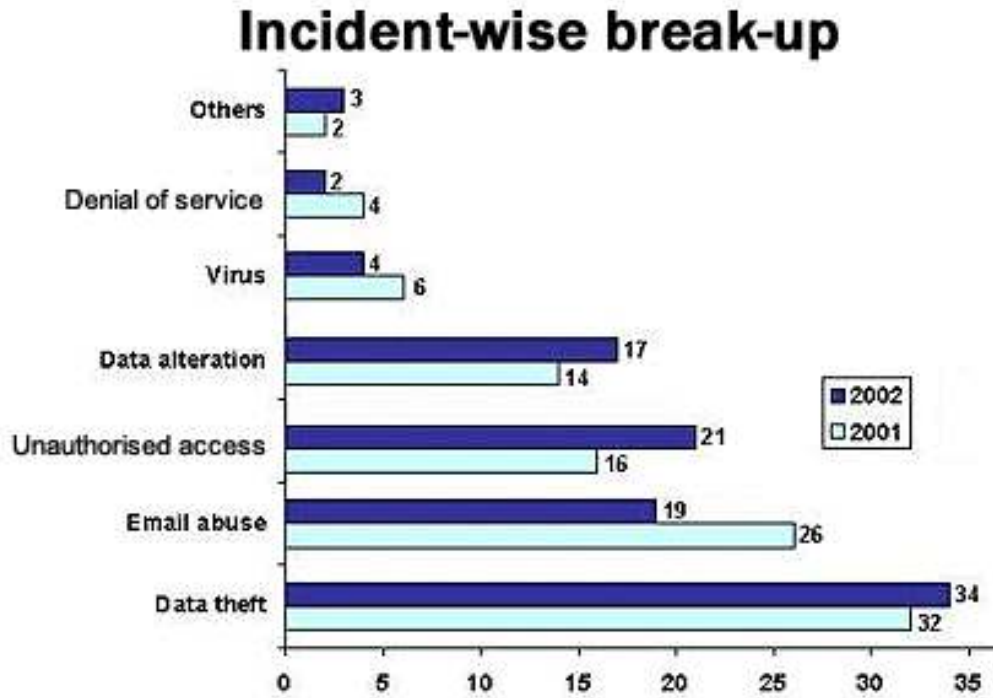
- But, Worm needs no human action to commence damage.
- A worm has the capacity to take advantage of file or information transport features on your system, which allows it to travel unaided.
- It has a great capability to replicate itself on your system; so from a single worm it can multiply itself into thousand clones.
- Due to the clone or copying nature of a worm and its ability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding.

One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line. In more recent worm attacks such as the much-talked-about 'Blaster Worm', the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

The **Trojan Horse**, at first glance will appear to be useful software but will actually do damage once installed or run on your computer.

- Those on the receiving end of a Trojan Horses are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.
- Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system.



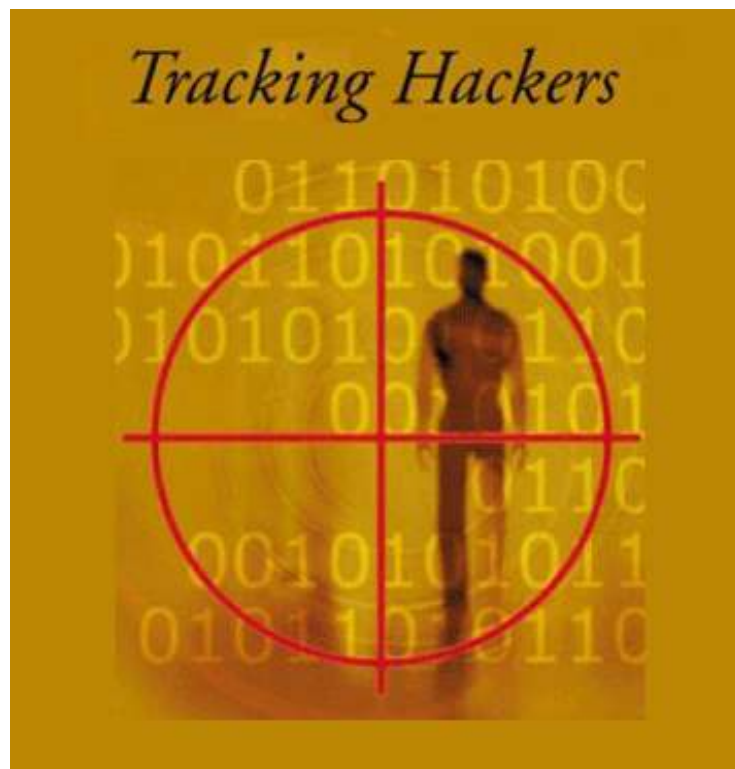
# CHAPTER 02

## INFORMATION TRAPPING

- It's all about Information Age

Are you tired enough of deleting Spam mails from your bulk folder? Have you now decided to send them warnings to stop this nonsense? Wait a click!! Think twice and read once to know more about spamming.

It is evident that Spam has grown as a major concern and a headache for both Internet service users and providers. The policy makers are constantly battling with this ever-growing crime not only to ensure a high quality service, but also to vault viruses and guarantee trust in Internet and digital economy.



Also well known as Junks, Spam mails are usually sent at a bulk, and you can almost identify those by its subject heading or content-matter. At just one time, these mails are sent to various recipients; therefore, in many cases, Spam mails have a long list of CCs and BCCs. Over the years, there has been a significant increase in the sending (and therefore receiving) of these Spam Mails. Most of the time, these Spam Mails have a lot of evil viruses and illicit images too. There are a range of precautions that you can personally take so that it does not affect you psychologically and your computer financially. You can delete the Spam mails as and when you see them in your inbox or the junk folder. By doing this, it would be easier to keep your mailbox safe. Deleting Spam also helps you to sort and avoid overlooking your useful mails. Spam mails are most of the times mails that are sent by the scam-stars. A huge number of Spam mails are into circulation nowadays, which is an area of concern.

## **Safety Measures**

In any case you want to keep yourself safe from these spam mails, you can follow some safety measures for yourself.

- Please do not ever try to reply any of those as the enthusiast scam-stars can crack your password via your reply-mail-path. You can only notify your email-service-provider, using its own system tools, about this annoying and dirty feature of your mailbox.
- Do not sign in for any newsletters as most of the times, these newsletters are also spamming. Unless and until you're sure about the site that you want to view, do not click on to any unknown link.
- Usually the scammers hunt for people who can fall prey to these scams. They trick the people in every possible way over the Internet. On request, these spammers get the required information from the servers. Scammers have web-spiders that work through web pages, looking for email addresses (e.g. email addresses contained in mailto: HTML tags). So do not ever trust or try to entertain spammers. Do not subscribe or buy anything that they want to sell.

## Spam Features

Now how will you, being a new user, be able to recognize Spam?

Researches reveal that Spam mails have some general characteristics —

- Adult contents and illicit images are often used as their subject matter. It includes fake dating and romance scams.
- Another kinds of Spam mails declare that you have won a huge prize-money by their online lottery; in these cases, they usually want to know your bank account or credit card number
- Some Spam mails dramatize some sort of emotional distress and plead you to play the role of a redeemer. Senders of most these spams are usually females who try to exploit the social norm of honor and justice.
- Spam mails can be received in forms of legal papers where a person declare that he is seeking your patronage to transfer money in his bank account via yours.
- And last but not the least are those spams which unhesitatingly announce that you will be a millionaire in just two weeks, or even less than that, by using their job references. These mails generally contain many intentional spelling mistakes of commonly used words so that you easily ignore those as a nominal mistake.



## Major E-Mail Felonies

### Scam

A term used to describe any type of fraudulent business or scheme that takes money or other goods from an unsuspecting person.

- Also known as **UCE (Unsolicited Commercial Email)**, **Spam** is commonly used to describe junk e-mail on the Internet.
- Spam is e-mail sent to thousands and sometimes millions of people without prior approval, promoting a particular product, service or a scam to get other people's money.
- The first Spam e-mail was sent by Gary Thuerk in 1978 an employee at Digital who was advertising the new DECSYSTEM-2020, 2020T, 2060, AND 2060T on ARPAnet.
- When talking in chat or a newsgroup, **Spam**, also known as **Flooding**, is the process of posting multiple lines of the same text two or more times.
- In a newsgroup, if a message is posted two or more times, this is also considered Spam or a flood of messages.

## Phishing

Pronounced like *fishing*, Phishing is a term used to describe a malicious individual or group of individuals scamming users by sending e-mails or creating web pages that are designed to collect an individual's bank or credit information. Below is an example of what Phishing e-mail may look like.

E-Bay Request: Your Account Has Been Suspended!!

Dear E-Bay customer,

Your Account has been **Suspended**. We will ask for your password only once. We will charge your account once per year. However you will receive a confirmation request in about 24 hours after the make complete unsuspended process. You have 24 hours from the time you'll receive the e-mail to complete this E-Bay Request.

**Note:** Ignoring this message will cause E-Bay TKO delete your account forever

**To make unsuspend process please use this link:** <http://fakeaddress.com/ebay>

E-Bay will request personal data (password; and so on) in this email. Thank you for using E-Bay! <http://www.ebay.com/>

---

This E-Bay notice was sent to you based on your E-Bay account preferences. If you would like to review your notification preferences for other types of communications, [click here](#). If you would like to receive this email in text only, [click here](#).

To a user who frequently uses E-Bay or any online service, these e-mails may appear as if they have come from the company described in the e-mail. However, Phishing e-mails are designed to deceive the user and trick them into visiting the links in the e-mail that are designed to steal personal information such as usernames, passwords, credit card information, etc. Below are some helpful tips on identifying these types of e-mails and how to handle them.

## How to identify Phishing e-mail

**Company** - These types of e-mails are sent out to thousands of different e-mail addresses and often the person sending these e-mails has no idea who you are. If you have no affiliation with the company the e-mail address is supposedly coming from, it's fake. For example, if the e-mail is coming from Wells Fargo bank but you bank at a different bank.

**Spelling and Grammar** - Improper spelling and grammar is almost always a dead give away. Look for obvious errors.

**Missing account information** - If the company was really sending you information regarding errors to your account, they would mention your account or username in the e-mail. In the above example the e-mail just says "E-Bay customer", if this really was E-Bay they would mention your username.

**Deadlines** - E-mail requests an immediate response or a specific deadline. For example, in the above example, the requirement to log in and change your account information within 24 hours.

**Links** - Although many Phishing e-mails are getting better at hiding the true URL you are visiting, often these e-mails will list a URL that is not related to the company's URL. For example, in our above E-Bay example: <http://fakeaddress.com/ebay> is not an E-Bay URL, just a URL with an E-Bay section. If you're unfamiliar with how a URL is structured, see our URL dictionary definition for additional information.

## **What to do if you're not sure if an e-mail is official**

Never follow any links in an e-mail you're uncertain about. Instead of following the link in the e-mail, visit the page by manually typing the address of the company. For example, in the above example, instead of visiting the fake ebay URL, you would type: <http://www.ebay.com> in your web browser and log in through the official web site.

Never send any personal information through e-mail. If a company is requesting you send them personal information about your account or are saying your account is invalid, visit the web page and log into the account as you normally would.

Finally, if you are still not sure about the status of your account or are concerned about your personal information, contact the company directly, either through an e-mail address provided on their web site or over the phone.

## **Commonly address Issues of Phishing e-mails**

Below are some of the issues a Phishing e-mail may inquire about in order to trick users.

**Account issues**, such as account or password expiring, account being hacked, account out-of-date, or account information needing to be changed.

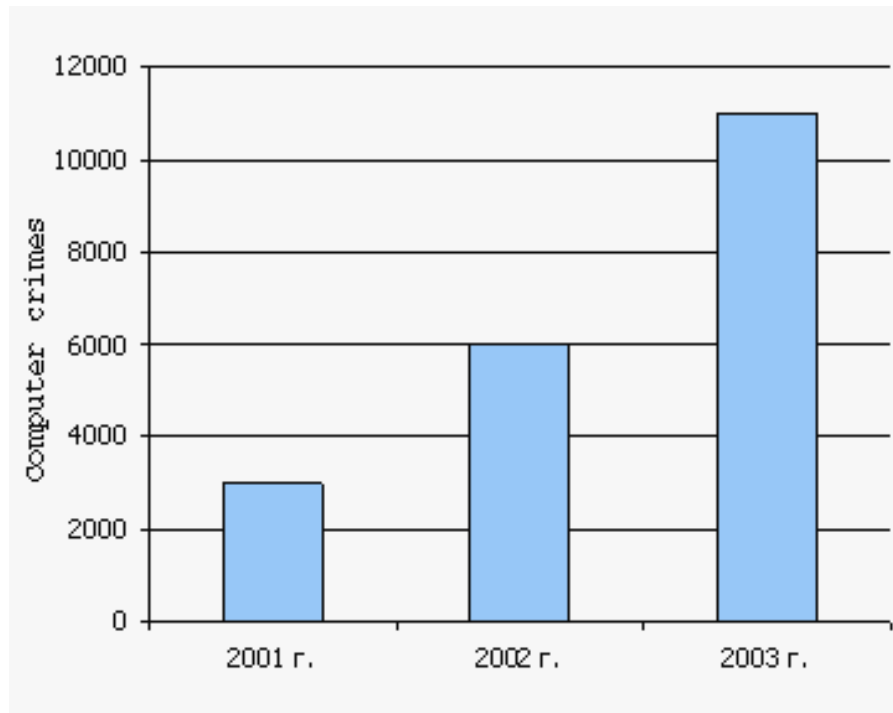
**Credit card** or other personal information, such as credit card expiring or being stolen, incorrect social security number or other personal information, or duplicate credit card or other personal information

**Confirming orders**, such as request that you log in to confirm recent orders or transactions.

## Common companies affected by Phishing

Below is a listing of some of the companies Phishers often send e-mails about.

- Any major bank
- Popular web sites such as: Amazon, MySpace, PayPal, eBay, Microsoft, Apple, Hotmail, YouTube etc
- Government: FBI, CIA, IRS, etc
- Internet service providers such as: AOL, MSN, etc
- Casinos and lottery
- Online dating or community web sites



## Frequently Received Spams

### Work-at-Home Scams (Easy Earning Scams)

Warning Signs:

- Labor & Intelligence are Constant in any Profit-Equation

Here the tricky advertisement is the working factor which lure the audience with the stable profits in turn of least labor — in the medical claims processing, envelope-stuffing, craft assembly work, data processing or other jobs. The amount of time or the hours are not mentioned but only the nature of the work to be done. The ads here use some one catchy phrases like: Fast cash, minimal work, no risk, consume time, homely business and also the advantage of working from home when it's convenient for you.

Possible outcomes:

After you put in your individual time and money, soon after you're most likely to find your promoters who in turn refuse to pay you, claiming that your work isn't up to their quality standards.

Homework:

1. Know whom you're dealing with.
2. Don't believe that you can make big profits easily.
3. Be cautious about emails offering work-at-home opportunities.
4. Get all the details before you pay.
5. Find out if there is really a market for your work.
6. Get references for other people who are doing the work.
7. Be aware of legal requirements.
8. Know the refund policy.
9. Beware of the old illegal pyramid "envelope stuffing" scheme.
10. Be wary of offers to send you an "advance" on your "pay."

March: You can forward work-at-home scams to [spam@uce.gov](mailto:spam@uce.gov)

## Weight Loss Scams (Fake online Pharmacies)

Warning Signs:

- Don't link Health with Pills

These Weight Loss Claims commit a revolutionary pill, patch, cream, or other product that will result in weight loss without diet or exercise. These products lure and block the absorption of fat, carbs, or calories; others guarantee permanent weight loss; and at the same time suggest that one would lose lots of weight at a lightening speed.

Possible Outcomes:

The weight loss scheme or product:

1. Lacks scientific evidence or demonstrated links between the result and the effects of the program, food, supplement, gadget or process being promoted
2. Is sold outside normal commercial distribution channels. For example, through the Internet, by unqualified individuals or mail order advertisements
3. Claims effortless, large or fast weight loss such as 'lose 30 kilos in 30 days' or 'lose weight while you sleep'
4. Claims that you can achieve weight loss without exercise, or without managing food or energy intake
5. Fails to recommend medical supervision, particularly for low-calorie diets
6. Claims to reduce fat or cellulite in specific areas of the body
7. Uses terms such as 'miraculous breakthrough'
8. Recommends the exclusive use of any type of gadget
9. Claims it is a treatment for a wide range of ailments and nutritional deficiencies
10. Promotes a particular ingredient, compound or food as the key factor of success
11. Demands large advance payments or require you to enter into long-term contracts.

Homework:

The experts also know for a fact that the most reliable way to cut the fat is to munch on a fewer calories and also gain any kind of physical activity so that you are capable to burn more energy. To set a goal to lose about a pound in a week is achievable. Most of us, which means that one, have to cut about 500 calories in just a day, by eating a variety of nutritious foods, and exercising regularly. As the lifestyle changes, the weight loss is expected. You can have a conversation with your health care provider about some nutrition and exercise plan, which can suit your lifestyle and metabolism.

March:

You can forward your weight loss emails to [spam@uce.gov](mailto:spam@uce.gov)

## **Cure-All Products (Miracle Cures)**

Warning Signs:

- Prevention is Better Than Miracle Cures

The mails which actually try to prove that a product is a “miracle cure,” a “scientific breakthrough,” an “ancient remedy” — or an instant quick and effective remedy for a large number of ailments or diseases. These normally announce the very short accessibility, and also require a payment, which has to be cleared off in advance, and that also offers a no-risk “money-back guarantee.” The case histories or testimonials by some vague people or doctors, which claim to have the amazing results, are not at all uncommon.

1. The treatment claims to be effective against a very wide range of ailments.
2. The miracle cure is suggested after a condition is diagnosed using a questionnaire (often on the internet).
3. The product is sold through unconventional means. For example, it might be sold over the Internet, by unqualified individuals, through mail order ads, or on television infomercials
4. The product relies on some guru figure, or a certain ingredient that is claimed to have mystical properties.
5. There is no scientific evidence to back up the claim that the miracle cure actually works.
6. Miracle cures usually include anonymous testimonials, for example ‘Mike, from Melbourne...’

### Possible Outcomes:

Miracle cure scams are particularly nasty because they usually increase health and emotional stress, they are costly, and they can be dangerous if they prevent you from seeking expert medical advice. They exploit people's hopes for improved health and end up causing more problems for people who already have enough to deal with.

### Homework:

When trying to evaluate any of the health-related claims give it a skeptical thought. If possible consult any of the health care professionals before buying of any "cure-all" packs which claim to find a wide range of ailments or also that offer some quick cures and easy solutions to the much serious illnesses. Frankly speaking, the cure all, cure none formula works here.

### Forward March:

You may forward spam with miracle health claims to [spam@uce.gov](mailto:spam@uce.gov)

## Check Overpayment Scams

Warning Signs:

- Cheques Cannot Be Auctioned

What can look like a net to trap you can be a response to the ad that you've posted or any of the online auction posting, offering to pay with a cashier's, personal, or corporate check. The so called buyer (or the buyer's "agent") makes up a valid reason for writing the check for more than the purchase price, and can also ask you to wire back the difference once you have deposited the check.

1. Somebody makes an offer to buy something you have for sale and wishes to pay more than the agreed price.
2. You are sent a cheque in excess of the agreed price and asked to send the balance to a specific bank account or through a wire transfer.

Possible Outcomes:

You lose just in case you deposit the check. Mostly the checks that are issued are counterfeit, but definitely they are good enough to dupe the unsuspecting bank tellers; and if in any case they bounce, you must pay the entire sum.

Homework:

1. Use your common sense: the offer may be a scam.
2. You can contact your local office of fair trading, ASIC or the ACCC for assistance.
3. Read all the terms and conditions of any offer very carefully: claims of free or huge offers often have hidden costs.
4. Do not open suspicious or unsolicited emails (spam): delete them.

5. Never enter your personal, credit card or online account information on a website that you are not certain is genuine.
6. Never send your personal, credit card or online account details through an email.

Do not agree to a check for any amount, which is more than your selling price. Do not succumb into any situation even if it tempts you. You can ask the buyer to give you the check for the purchase price. If the buyer gives you the incorrect sum, return the check. In such cases do not send the merchandise. If you are the vendor who accepts payment by check, you can ask for a check, which is drawn on your local bank, or a bank with your local branch. This way, you can also personally make sure that the check is ultimately valid. If this cannot be done call the bank from which the check was drawn and by using the phone number from directory assistance or an Internet site that you know and trust, not from the person who gave you the check. Find out whether the check is totally valid.

March:

You too can forward the check overpayment scams to [spam@uce.gov](mailto:spam@uce.gov)

## Pay-in-Advance Credit Offers (Pay First Scams)

### Warning Signs:

- Advance for Sufferings

The report that you've been “pre-qualified” to receive something like a low interest loan or credit card, or repair your bad credit even though banks have turned you down is the ultimate bait here. To take the benefit of this, you must first be ready to shell up a processing fee, which may be of some several hundred dollars.

### Possible Outcomes:

A lawful and pre-qualified take also means you've been given the chance to apply.

Firstly you must try and complete a form, which can still be turned down just in case. If you have paid a fee in advance for the promise of a loan or credit card, you've been hustled. There may be a list of lenders, but there's no loan, and the person you've paid has swiped off your money and run away.

### Homework:

If in case you think it's just a promise with no legal documents, do not pay! The legal lenders never base their cards on “guarantee” or talk about loans before you even apply. It may require that you pay for the application, appraisal, or credit report fees, but these fees rarely are required before the person who is lending is identified and the terms and conditions are completed. The plus is that the fees, which are generally paid to the lender and not to the middle man who arranged the much “-guaranteed” loan.

March: You can forward unsolicited email containing credit offers to [spam@uce.gov](mailto:spam@uce.gov)

## Debt Relief

Warning Signs:

- Online Relief, Offline Debts

This is when the mails advertise themselves in a way that one can combine their bills into their monthly payment without even borrowing; or the stop credit harassments, foreclosures, repossessions, tax levies and garnishments; or pay off your credits.

Possible Outcomes:

The offers, often involve a lot of bankruptcy proceedings, but rarely say so. The reason being, that it has a negative and at the same time a long-term impact on your creditworthiness. A bankruptcy stays on your credit report for 10 years, and can hinder your ability to get credit, a job, insurance, or even a place to live. To top it off, you will likely be responsible for attorneys' fees for bankruptcy proceedings.

Homework:

- Save money by deleting your Credit Card Debt Spam first
- Before actually resorting to the bankruptcy, get into a conversation with your creditors about arranging a modified payment plan, contact a credit counseling service to help you develop a debt repayment plan, or carefully consider a second mortgage or home equity line of credit.

Try getting the main idea from the mails. But you must take care that while a home loan may allow you to combine your debts, it may also require your home as security. And just in case you do not make your payments, you could unfortunately lose your home.

March:

You can forward debt relief offers to [spam@uce.gov](mailto:spam@uce.gov)

---

**This is just a sample of our e-book/book ghostwriting.**

**[www.uniquebook.com](http://www.uniquebook.com) is happy to offer you the heavily downloaded ebook**

**‘How 2 Kill The Cyber Crime Snake B4 IT Kills U’ absolutely FREE!!**

**Visit our home page to download now!!**

---