Leprechaun Technical Services

COMPUTER SECURITY

- What it is.
- What to look out for.
- How to protect yourself.

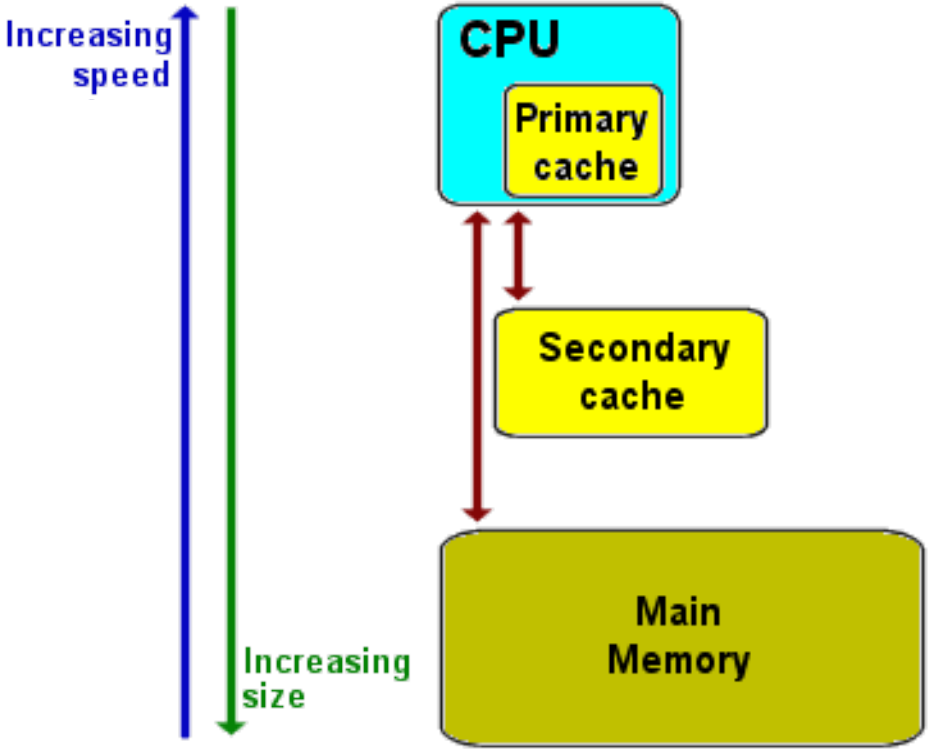
What is Computer Security?

- When you go online via email or through a website, your system is vulnerable to attack.
- There are hackers, cyber-criminals, various types of infections, malicious software, and more.
- You need to know what to look out for in order to protect yourself, and the best start is to be informed.

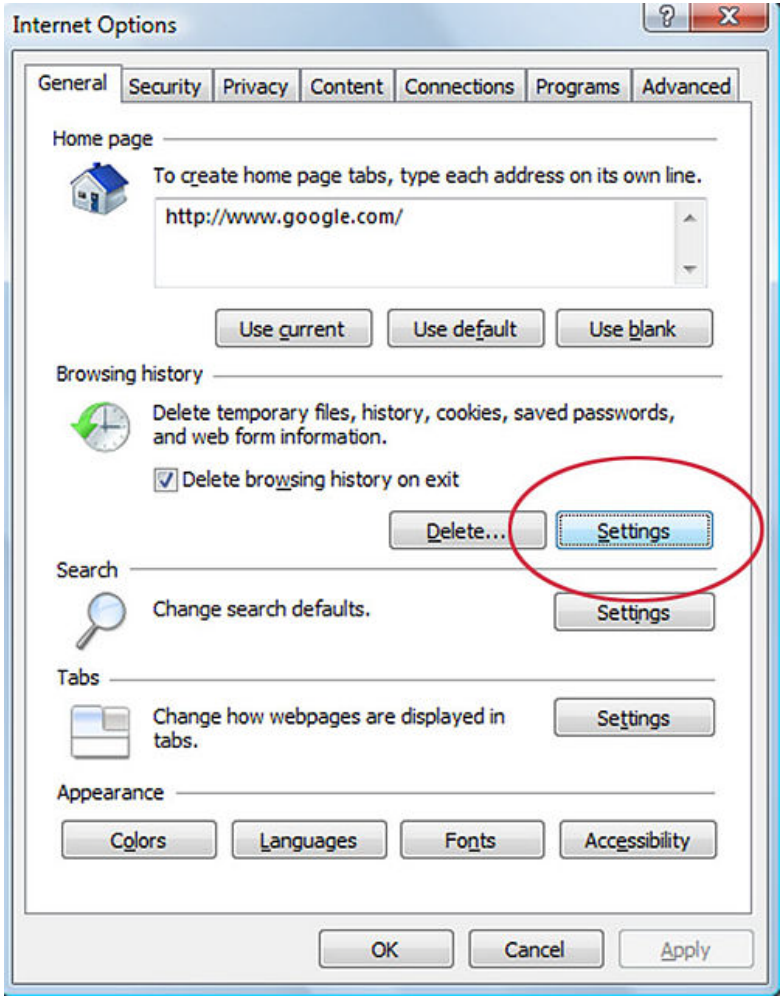
Basic Computer Terms

- **Cache** – Temporary Internet Files stored on your hard disk (such as graphics) to speed up display of web pages you frequently visit.

Downside: After time it slows down your computer if you don't clean it out regularly.



Basic Computer Terms



- **History** – Your internet history records all of the sites you have visited. If you don't remember what site you visited, you can find it in your history.

Downside: It also keeps and stores any data you typed into a form.

Basic Computer Terms (cont.)

- **Cookies** – Website code that collects data sent from a website and stored in a users web browser.
- **Tracking Cookies** - are commonly used to compile long-term records of individual's browsing histories. When a user accesses a website for the first time, a cookie is sent from the server and stored with the browser in the local computer. Later when that user goes back to the same website, the site will recognize the user because of the stored cookie with the user's information.

What Do I Do About That?

- To Delete Your Browsing History; Cookies, Temporary Internet Files, Website History, Form Data, Passwords, as well as your Recycle Bin, Clipboard, DNS Cache, Memory Dumps, etc.

- Download and Install:

Ccleaner is a system optimization program designed to improve the functionality and speed of your computer.

Computer Infection Terms

- **Malware** – Short for Malicious software.
- **Spyware** – Malicious software that gathers user information without your consent.
- **Adware** – Software that shows advertisements, sometimes as invasive pop-up windows.

Spybot Search & Destroy is an excellent spyware and adware removal tool which scans your computer's hard disk for malicious software and removes it.

Computer Infection Terms (cont.)

- **Virus** – Very Malicious software that is spread by opening infected files.
- **Trojan Horse** – A form of virus that appears to be valid but will damage your computer.
- **Worm** – Similar to a virus, capable of spreading thru email or networks.

Without protection, if your computer is compromised with a virus, worm or worse; it can steal your information, eat and destroy your files or kill your computer!

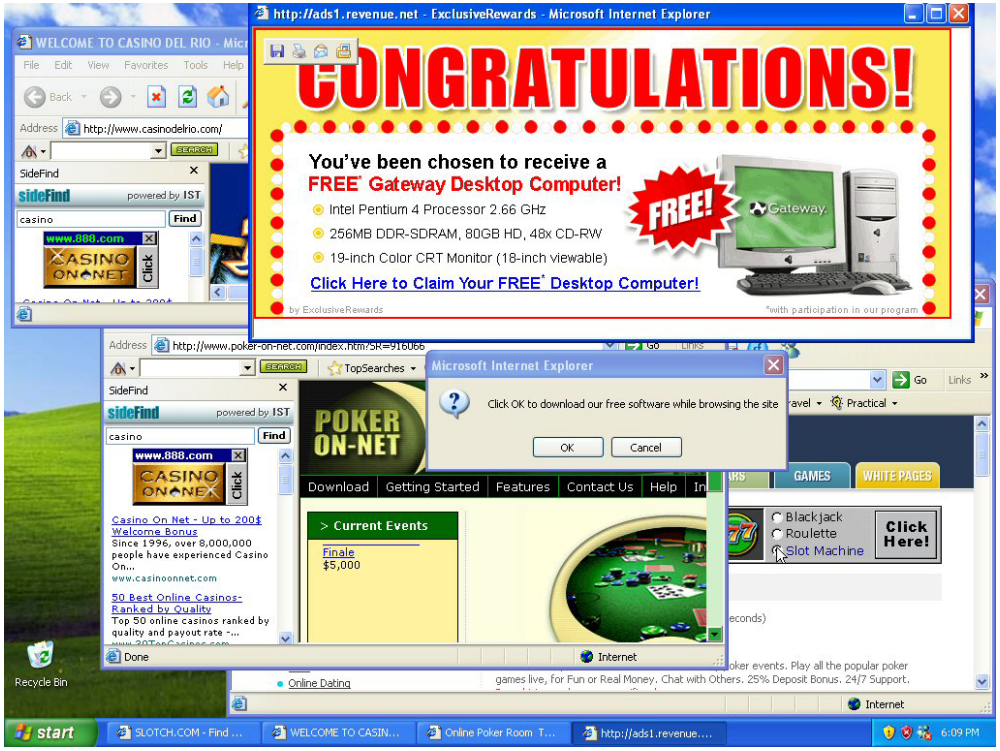
What do I do about those?

ZoneAlarm Firewall and AntiVirus Software protects your computer by blocking potential hackers attempting to break into your computer, catching malicious attacks and quarantining or removing viruses from your computer.

It is better and more advanced than Norton, MacAfee or TrendMicro.

Things To Look Out For:

- Computer Slowing Down or Acting Glitchy
- Your Home Page Changed
- Computer Freezing
- Website Redirects
- Excessive Pop-ups
- Infection Warnings
- Excessive Spam
- Email Hacked



Other Things to Look Out For:

- **ANYTHING** that pops up announcing you are infected (especially if it is NOT from your antivirus protection)

and that tells you to

download their spyware

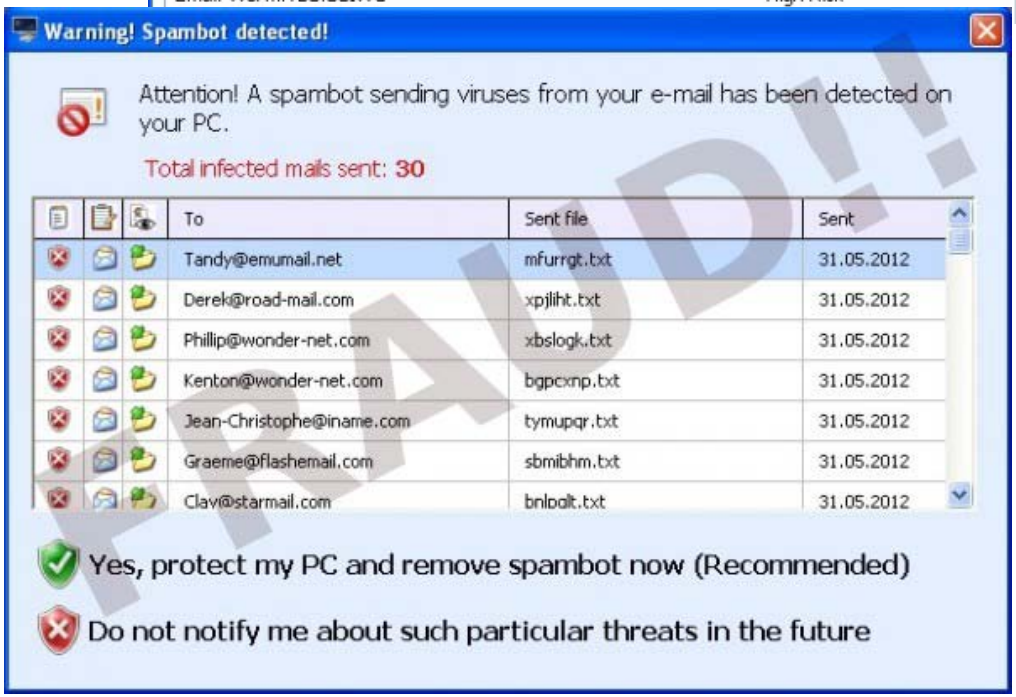
to clean your system.

SCAM!

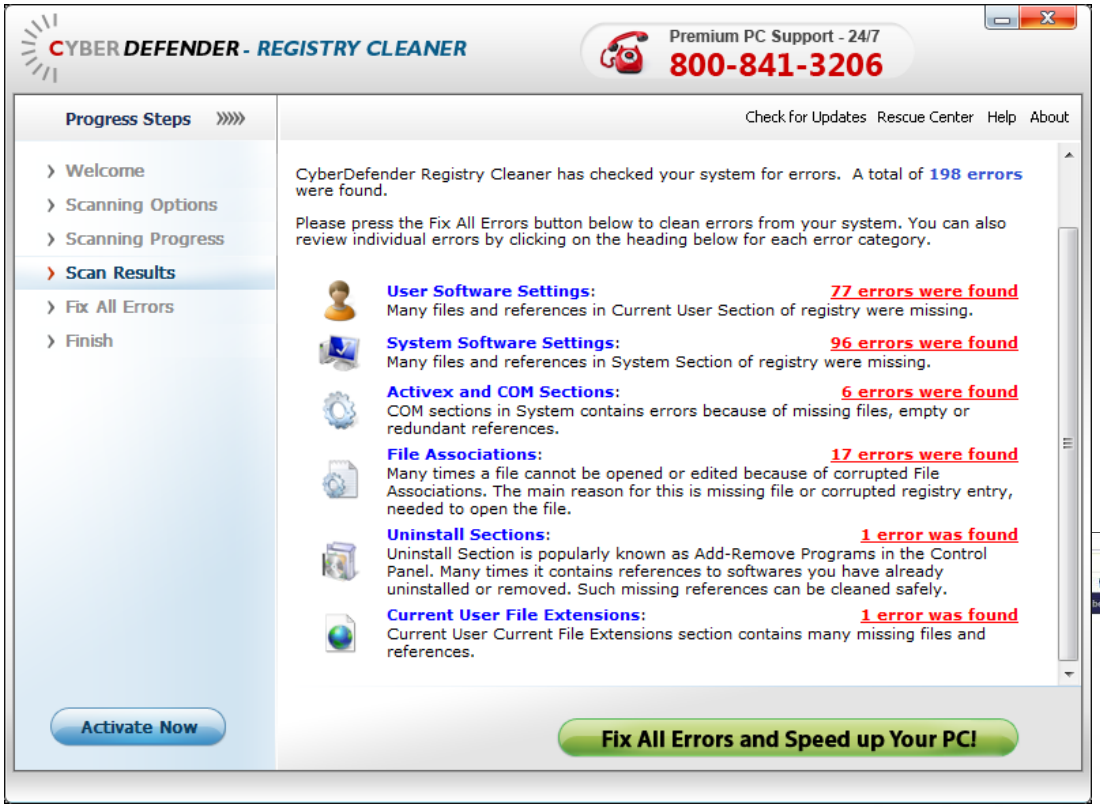
But They Look Authentic…

- That is the SCAM.
- They scare you into thinking you need to take action, when in reality, all you need to do is CLOSE EVERYTHING. Run your cCleaner Run spybot and do a quick scan with ZoneAlarm.

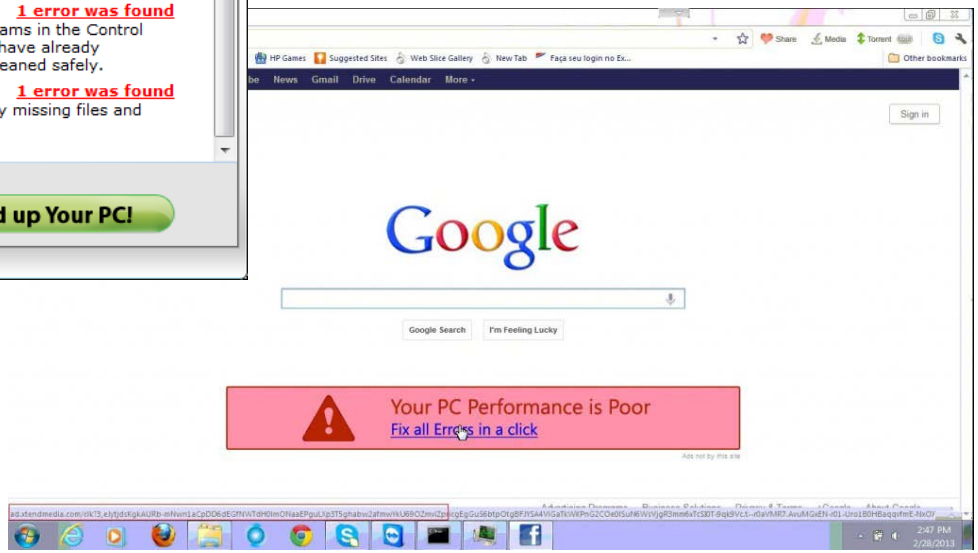
As long as you didn't click their messages or download anything you should be okay.



Some other things to look for:

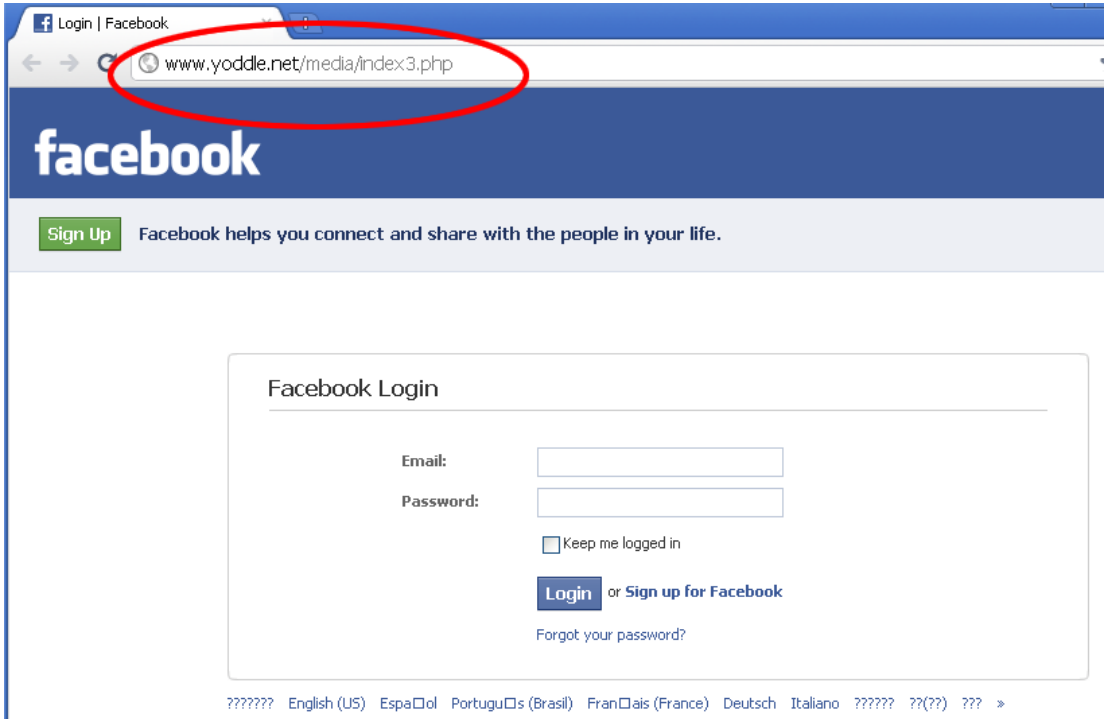


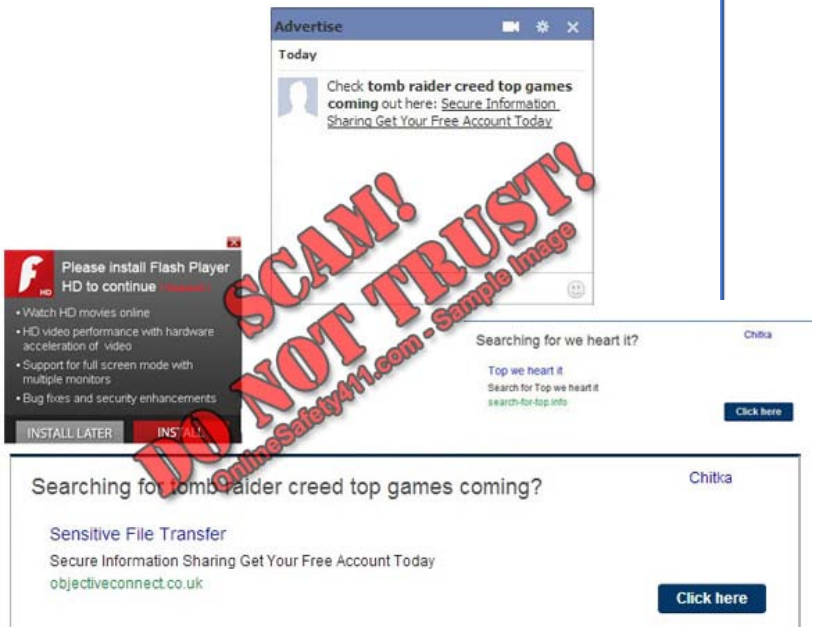
- Your search can pull up ads that look like virus warnings. Don't click them!



Some other things to look for:

• Facebook is not safe either: Their ads sometimes link to corrupt websites, their games can be infected and links from strangers are like candy from strangers – **Don't Click It!**





• ALWAYS take note of the website address of any website before you login! Websites can be designed to look EXACTLY like legit websites – the only difference is the address.

Free Software is NOT Safe.

Never click a link. Just close the internet.

How to Protect Yourself

- Clean your system regularly using Ccleaner and Spybot Search & Destroy.
- Install a Firewall & Antivirus Program (ie: ZoneAlarm)
- Get your windows updates regularly.
- Don't click on unknown or unsolicited links or attachments.
- Don't download unknown files or programs to your computer.
- Change your password regularly and make them strong.

ZONEALARM
by Check Point

Microsoft Windows

Windows Update

CHANGE YOUR PASSWORDS

Ransom Viruses

- A type of malware that restricts access to your computer system and demands a ransom paid to the creator to regain access.
- Some ransom viruses encrypt your documents and pictures.

- The most common ransoms look like they are coming from the FBI, Homeland Security or Police.
- Many take over your webcam and record you.

The following are what some Ransom Viruses Look Like:

Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

- 18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
- 18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
- 18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1. Take your cash to one of this retail locations: Walmart, K-Mart, CVS/pharmacy, Walgreens, 7-Eleven
2. Get a MoneyPak and purchase it with cash at the register
3. Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code: Submit

1 2 3
4 5 6
7 8 9
Delete 0 Enter

THE FBI FEDERAL BUREAU OF INVESTIGATION

ATTENTION !

IP: [redacted]
Location: [redacted]
IPS: [redacted]

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011,

Video Recording ON

MoneyPak

Code: Sum: 100 $

1 2 3 4 5 6 7 8 9 0

Pay MoneyPak

IP: [redacted]
Location: **United States** [redacted]
ISP: [redacted]
Operation system: **Windows XP (32-bit)**
User name: [redacted]

Homeland Security
National Cyber Security Division

THIS COMPUTER HAS BEEN BLOCKED

THE WORK OF YOUR COMPUTER HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.

Article 184. Pornography involving children
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic material)

Article 171. Copyright
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

The first violation may not entail the criminal liability if the payment of the fine would be excecuted in connection with the law of loyalty to the people, on 1 March 2013. If repeated violations occur, the prosecution is inevitable.

To unlock the computer you are obliged to pay a fine of $300.
You must pay the fine through MoneyPak.

You have 48 hours to pay the fine. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer and take You to Court.

green dot MoneyPak Code:

1 2 3 4 5 6 7 8 9 0

Pay MoneyPak

After paying the fine your computer will be unblocked. (In the case of second violation you will become the subject of criminal prosecution without the right to pay the fine)

An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

How to pay the fine using MoneyPak?

1. Take your cash to one of these retail location:
Walmart, Walgreens, CVS/pharmacy

2. Pick up a MoneyPak and purchase it with cash at the register

3. Enter $300 MoneyPak code and press OK.

For identifying cyber-criminals and a better Cyber Law Enforcement, the treaty to develop an anti-virus software was signed on March 1, 2012.

If you get a Ransom Virus…

- This is not good.
- Turn OFF your computer.
- Disconnect it from the internet.
- Call Leprechaun Technical Services.
- Pray your files were not encrypted, your operating system not corrupted or your hard drive damaged.
- Most of the time I can scan the hard drive externally, remove the virus, repair the operating system and save your files. Sometimes I can’t.

Don’t Be Afraid of Your Computer

- An educated computer user is a safe computer user.
- If you know what to look out for, read before you click and practice safe surfing you will be fine.

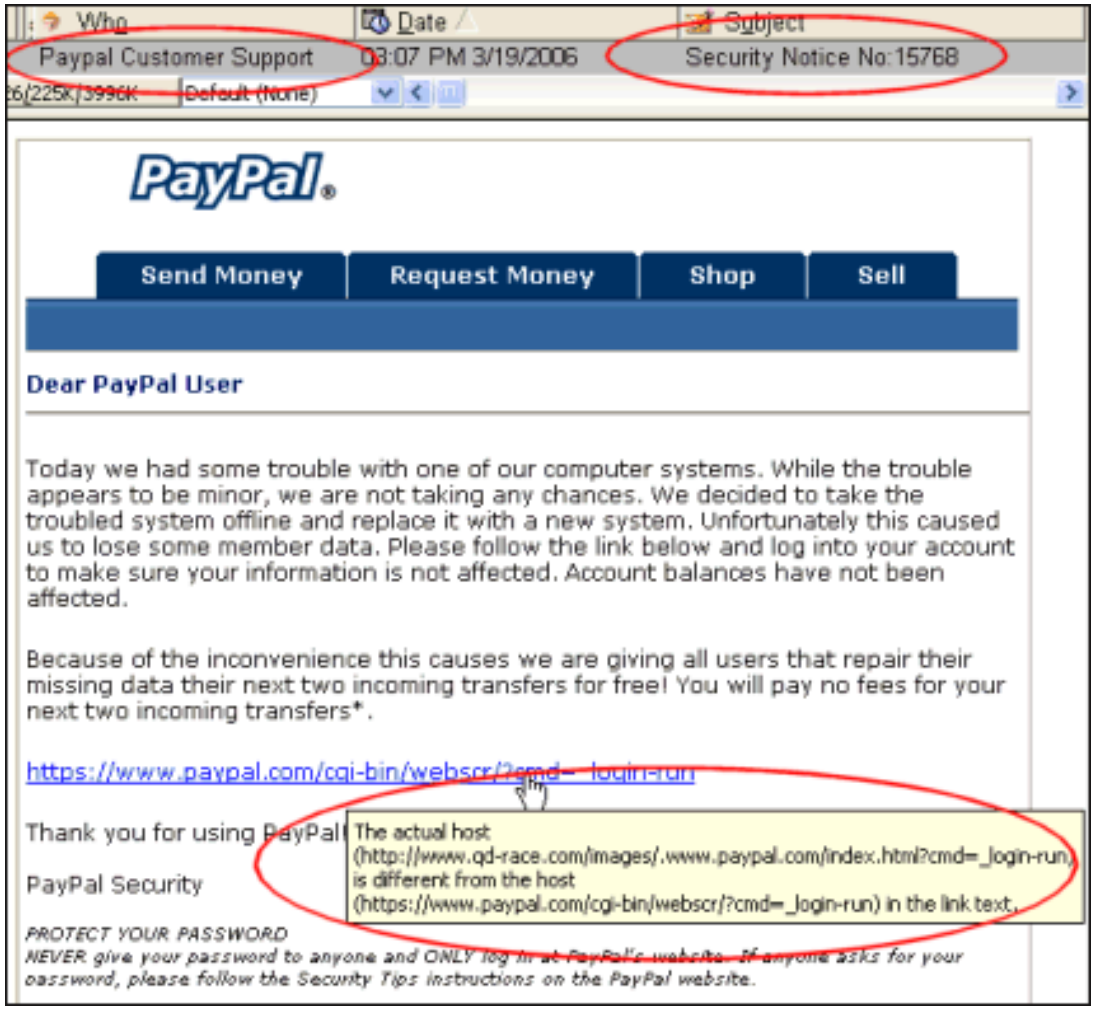
Tips & Tricks

- If you hover over a link with your mouse it will show you the website link it is intending to take you to. If you do not recognize the website, do not click on the link.

This works on websites AND emails.

Tips & Tricks (cont.)

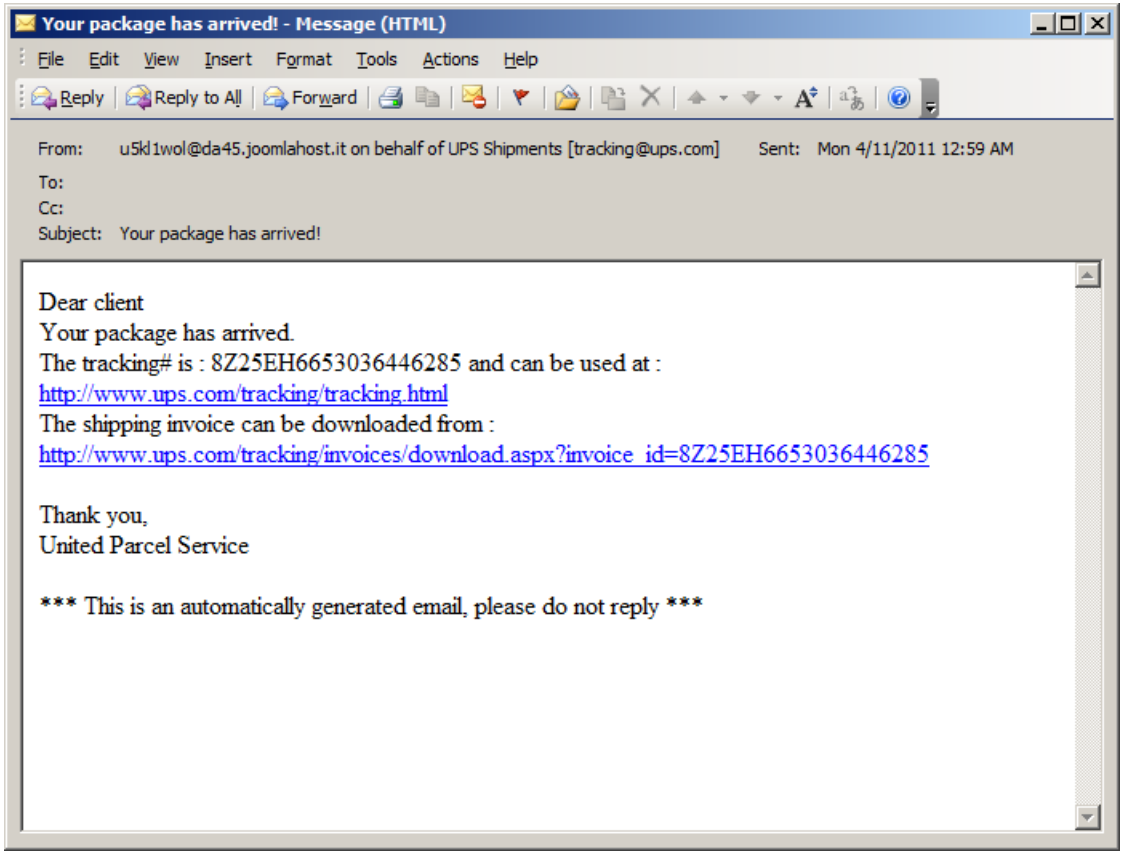
- A reputable company (like your bank or PayPal) will **NEVER** send you a link in an email to click on to change your password.
- If there is a misspelled word or grammatical error in the email – that is a big clue it is a scam.



Tips & Tricks (cont.)

- Emails can look legit, but when in doubt, look at the From email address. Then hover your mouse over the link to see where it wants to take you.

- Emails from friends with notes like "Check this out: and a link" means their email was hacked. They need to log into their email and change their password.



Thank You!

Leprechaun Technical Services

If you would like to schedule a service call:

830-237-1924

For more information visit:

www.LeprechaunTechnicalServices.com