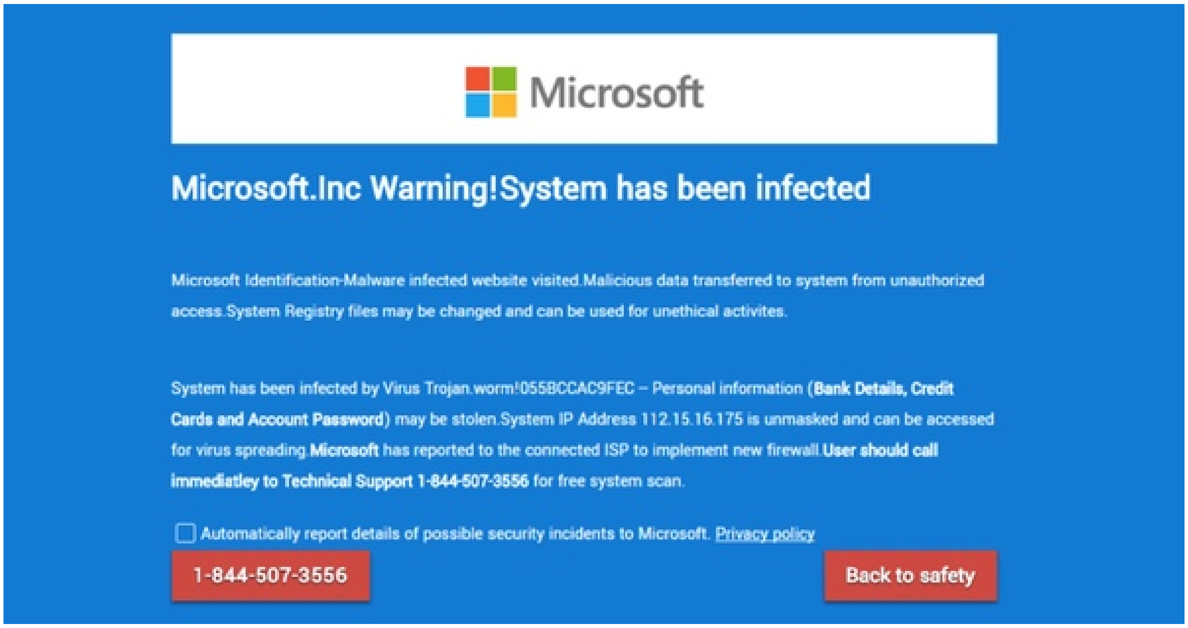
Kerno.biz LLC Newsletter **June 2018**

How to Avoid Fake Security Messages

When you are searching or surfing the Internet there are well known and less well known websites. Well known websites such as amazon.com, google.com, washingtonpost.com, epicurious.com, wikipedia.org are all fine to go to. But what about less well known websites? How do you know if it is safe to click on a link that will take you to a less well known website? *Google* provides a service where you can check the website before you randomly click a link to go to that website.



Microsoft.Inc Warning!System has been infected

Microsoft Identification-Malware infected website visited.Malicious data transferred to system from unauthorized access.System Registry files may be changed and can be used for unethical activites.

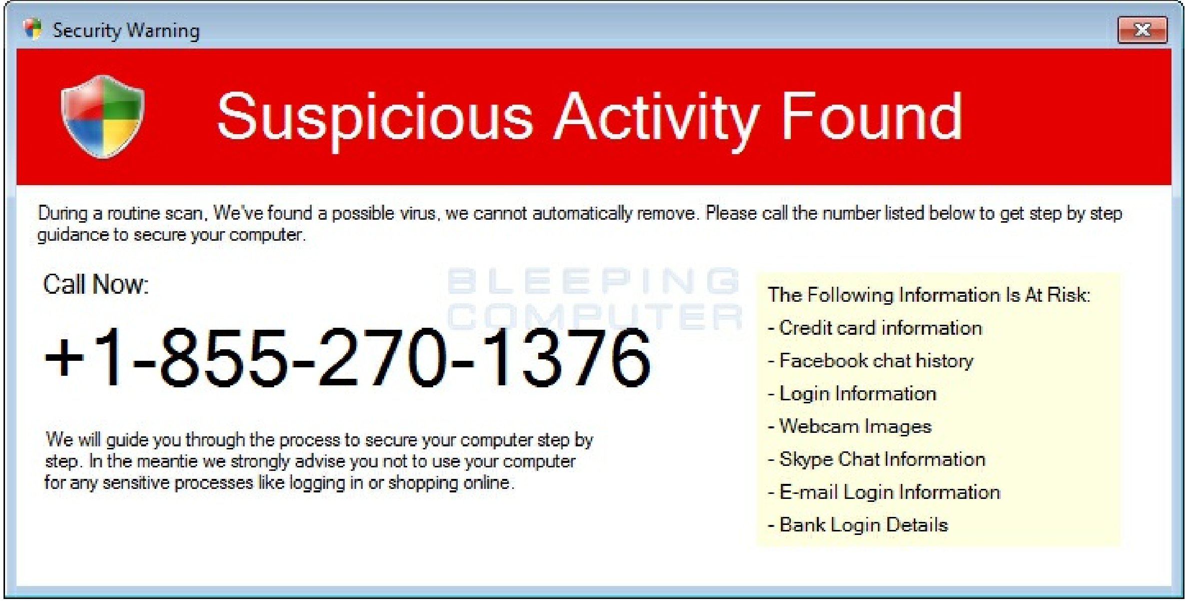
System has been infected by Virus Trojan.worm!055BCCAC9FEC – Personal information (**Bank Details, Credit Cards and Account Password**) may be stolen.System IP Address 112.15.16.175 is unmasked and can be accessed for virus spreading.**Microsoft** has reported to the connected ISP to implement new firewall.**User should call immediatley to Technical Support 1-844-507-3556** for free system scan.

□ Automatically report details of possible security incidents to Microsoft. Privacy policy

Fake Microsoft Message

Copy and paste this URL http://google.com/safebrowsing/diagnostic?site= followed by the site you want to check, such as kerno.biz. *Google* will let you know if the website has hosted malware in the past 90 days. (How to copy and paste)

For example: http://google.com/safebrowsing/diagnostic?site=kerno.biz



Security Warning

Suspicious Activity Found

During a routine scan, We've found a possible virus, we cannot automatically remove. Please call the number listed below to get step by step guidance to secure your computer.

Call Now:

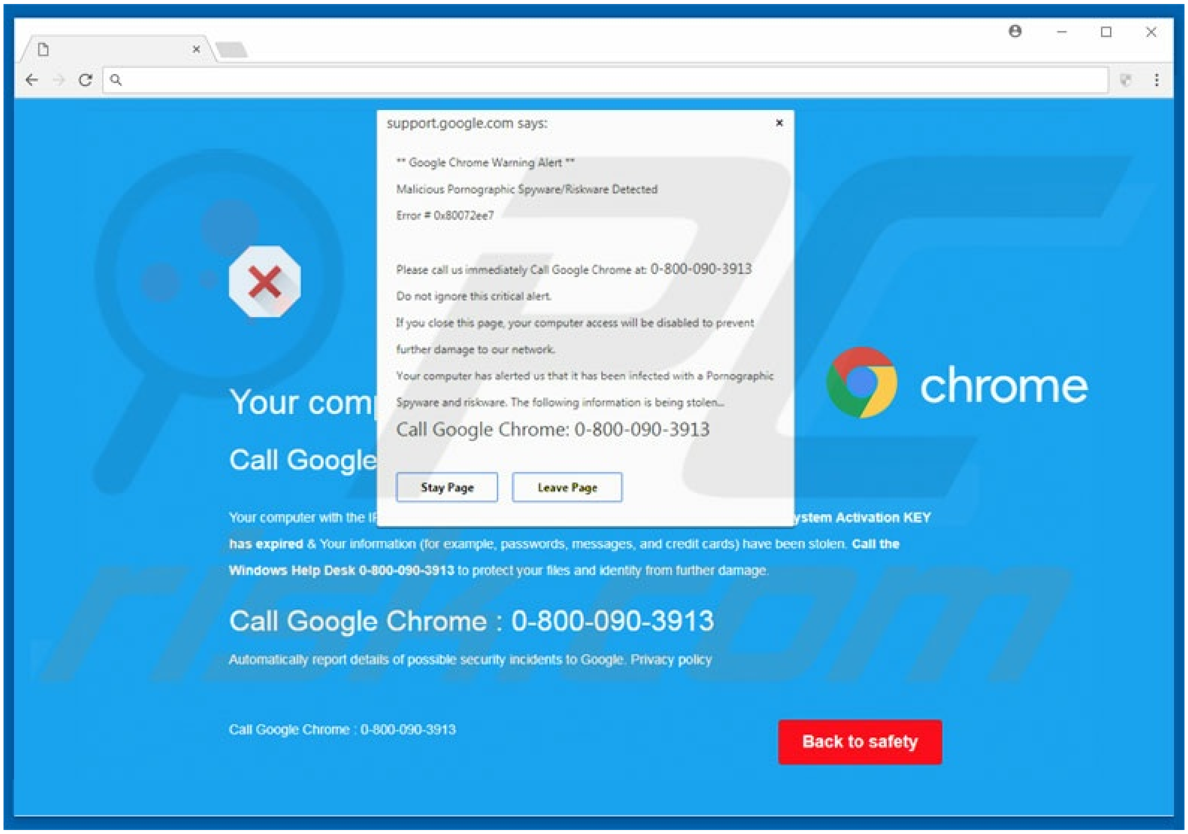
+1-855-270-1376

We will guide you through the process to secure your computer step by step. In the meantie we strongly advise you not to use your computer for any sensitive processes like logging in or shopping online.

The Following Information Is At Risk:
- Credit card information
- Facebook chat history
- Login Information
- Webcam Images
- Skype Chat Information
- E-mail Login Information
- Bank Login Details

Fake Security Warning

So when you are searching for that ultimate apple pie recipe and you come across a link you want to click on, if the part right after http:// or https:// in the URL (website address) is not familiar to you, stop and check the website first.



support.google.com says:

** Google Chrome Warning Alert **

Malicious Pornographic Spyware/Riskware Detected

Error # 0x80072ee7

Please call us immediately Call Google Chrome at: 0-800-090-3913

Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware. The following information is being stolen...

Call Google Chrome: 0-800-090-3913

Your comp

Call Google

Your computer with the I **ystem Activation KEY has expired** & Your information (for example, passwords, messages, and credit cards) have been stolen. **Call the Windows Help Desk 0-800-090-3913** to protect your files and identity from further damage.

Call Google Chrome : 0-800-090-3913

Automatically report details of possible security incidents to Google. Privacy policy

Call Google Chrome : 0-800-090-3913

Fake Google Chrome Message

Avoid getting one of those fake messages saying your computer is infected or has a security problem and call this number immediately. All of these messages are fake and the last website you went to just before you saw the message was the culprit. So after you Google search for something, be careful before randomly clicking on a link you come across. Check it out first.

Also be wary of any come on "news" story links on the right side or at the bottom of any website. These are often the culprit. They will tempt you into clicking on one of their "stories" and the next thing you know you have been hit with a fake security warning. Avoid these solicitations to click on their link. Don't pay any attention to them. They are only there to try and get you to call a fake number so they can get your credit card number. If you want to read the news go to a reputable news website and read the news there.

If You Are Hit By A Fake Security Message

Usually all of these fake messages are harmless. They are designed to get you to call the number to give up your credit card number, which is the real harm. Never, ever call a phone number that pops up on your screen (or one in an email either). They are all fake so don't fall for it. Simply restart your computer and usually the message will be gone. Do not return to the last thing you were doing just before the message appeared. That was the website that did it to you. If you can't restart your computer normally then simply hold the power button for 10 full seconds. That will shut the computer down, let go of the button and then press it normally to turn it back on. In most cases the message will be gone and the computer will be back to normal.

In the rare case that the message returns after a restart let me know and I will login to your computer and remove the message. If you are curious about the website that "gotcha", you can look at your browser history and see the last website you were on before the fake messages appeared. But remember, do not return to that website or you will have to restart your computer again.

More info:

Microsoft Edge: View and delete browser history in Microsoft Edge

Internet Explorer: View and delete browser history in Internet Explorer

Google Chrome: See and Delete your Google Chrome browsing history

Microsoft: Tech Support Scams

Microsoft: Teaming up in the war on tech support scams

FTC to Provide Refunds to Victims of Tech Support Scam

Newsletter Archives

Click here to read some of my past newsletters.

Some of my clients do not realize that my business has expanded to all mobile devices. In fact, any consumer electronic product that you can purchase I can help you with. So if you would like help setting up or syncing your new smartphone or tablet or connecting your new WiFi TV to the Internet, just let me know.

Claude Kerno
Technology Consultant
719.650.9916