Crossing the Digital Divide (v153)
"Yawn"
by Joseph Feigon
for the Observer

If your browser is being redirected to sites that display errors or alerts, asking you to call a tech support number to fix it, then it is possible that you've stumbled upon a Tech Support Scam. Tech support scams are an industry-wide issue where scammers use scare tactics to trick you into paying for unnecessary technical support services that supposedly fix contrived device, platform, or software problems.
These Tech Support pop-up scams are a social engineering attack that puts your browser on full screen and display pop-up messages that won't go away, essentially locking your browser. These fake error messages aim to trick you into calling an indicated technical support hotline. If you call these scammers, they can offer fake solutions for your "problems" and ask for payment in the form of a one-time fee or subscription to a purported support service.

These alerts are nothing more a scam. Microsoft or Apple do not send unsolicited email messages or make unsolicited phone calls to request personal or financial information or fix your computer. Treat all unsolicited phone calls or pop-ups with skepticism. Do not provide any personal information.

Your browser may be redirected to the Tech Support Scam sites either by malicious advertisements on the sites you visit or adware. This guide was written to help Windows users remove malware from their devices, if your just looking for a way to block the redirect to a Tech Support Scam on a specific site, then you can use a free browser extension like Adblock.

When it comes to adware, these malicious programs are bundled with other free software that you download off of the Internet. Unfortunately, some free downloads do not adequately disclose that other software will also be installed and you may find that you have installed adware without your knowledge.

The Tech Support fake error messages is shown in such a way as to trick the user into thinking their computer has crashed or that a virus has been detected on the computer. It does this to try and scare the infected user into calling one of the listed numbers in order to receive support. In reality, though, they will only be greeted with people who are trying to sell them unneeded support contracts and services. If you actually call one of these scammers, they will typically attempt to get you to allow remote access to their computer. After remote access is gained, the scammer relies on confidence tricks typically involving utilities built into Windows and other software in order to gain the victim's trust to pay for the supposed "support" services, when the scammer actually steals the victim's credit card account information.

These bogus tech support pop-ups may display the following message:

> You might be infected with adware / spyware virus
> Call 1-866-928-0684 immediately. Fast assistance with removing viruses.

(Toll-FREE, High Priority Call Line)
What you must do:
More about the virus:
Seeing these pop-ups means that you may have a virus installed on your computer which puts the security of your personal data at a serious risk. It's strongly advised that you call the number above and get your computer fixed before you continue using your internet, especially for shopping.

Possible Privacy Breach if virus not removed immediately:
Data exposed to risk:
1. Your credit card details and banking information
2. Your e-mail passwords and other account passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be accessed remotely by stalkers with a VPN virus

Support.Microsoft.com says:
** Windows Warning Alert **
Malicious Pornographic Spyware/Riskware Detected

Please call us immediately at: 1855-246-8689
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…
> Financial Data
> Facebook Logins
> Credit Card Details
> Email Account Logins
> Photos stored on this computer
You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity. Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

Toll Free: 1855-246-8689

Prevent this page from creating additional dialogues.

You should not purchase anything from numbers listed in these types of alerts. Whatever you do, please do not call the phone number for support because it is not Microsoft's but rather a group of scammers waiting to rob you of hundreds of dollars under false pretenses. **Call your credit card provider to reverse the charges, if you have already paid.**
You should **always pay attention when installing software** because often, a software installer includes optional installs. Be very careful what you agree to install.
Always opt for the custom installation and deselect anything that is not familiar, especially optional

software that you never wanted to download and install in the first place. It goes without saying that you should not install software that you don’t trust.

Control the things you can and keep the surprises to a minimum.