



Mecklenburg County Consumer Fraud Task Force

*"One Less Victim" - The first task force in North Carolina
dedicated to the prevention of consumer fraud.*

Scam Alert Archives/Archivos de Alertos de Fraude

January, 2010

ENGLISH VERSION

POP-UP ADVERTISEMENTS OFFERING ANTI-VIRUS SOFTWARE POSE THREAT TO INTERNET USERS

An ongoing threat exists for computer users who, while browsing the Internet, began receiving pop-up security warnings that state their computers are infected with numerous viruses.

These pop-ups known as scareware, fake, or rogue anti-virus software look authentic and may even display what appears to be real-time anti-virus scanning of the user's hard drive. The scareware will show a list of reputable software icons; however, the user cannot click a link to go to the actual site to review or see recommendations.

The scareware is intimidating to most users and extremely aggressive in its attempt to lure the user into purchasing the rogue software that will allegedly remove the viruses from their computer. It is possible that these threats are received as a result of clicking on advertisements contained on a website. Cyber criminals use botnets to push the software and use advertisements on websites to deliver it. This is known as malicious advertising or malvertising.

Once the pop-up appears it cannot be easily closed by clicking "close" or the "X" button. If the user clicks on the pop-up to purchase the software, a form is provided that collects payment information and the user is charged for the bogus product. In some instances, whether the user clicks on the pop-up or not, the scareware can install malicious code onto the computer. By running your computer with an account that has rights to install software, this issue is more likely to occur.

Downloading the software could result in viruses, Trojans, and/or keyloggers being installed on the user's computer. The repercussions of downloading the malicious software could prove further financial loss to the victim due to computer repair, as well as, cost to the user and/or financial institutions due to identity theft.

The assertive tactics of the scareware has caused significant losses to users. The FBI is aware of an estimated loss to victims in excess of \$150 million.

Be cautious—Cyber criminals use easy to remember names and associate them with known applications. Beware of pop-ups that are offer a variation of recognized security software. It is recommended that the user research the exact name of the software being offered.

Take precautions to ensure operating systems are updated and security software is current.

If a user receives these anti-virus pop-ups, it is recommended to close the browser or shut the system down. It is suggested that the user run a full, anti-virus scan whenever the computer is turned back on.

If you have experienced the anti-virus pop-ups or a similar scam, please notify the IC3 by filing a complaint at www.ic3.gov or www.consumertaskforce.org.

SPANISH VERSION

Mecklenburg County Consumer Fraud Task Force

Jan 2010 - SPANISH

Anuncios englobados sobre el Internet/FBI

Spanish IR

Hola, le habla un agente del FBI de la división de Charlotte en el condado de Mecklenburg. Somos miembros del grupo en contra del fraude al consumidor en el condado de Mecklenburg.

Existe una amenaza para los usuarios de computadoras, en donde anuncios englobados (pop-ups) indican que sus computadoras están infectadas con numerosos virus. Estos anuncios englobados se conocen como “scareware”, o medios diseñados para intimidar al usuario a comprar este paquete anti-virus fraudulento. El scareware hasta produce un menú supuestamente legítimo, pero es imposible de usar el enlace para revisar el programa o ver recomendaciones.

El scareware es muy agresivo en sus intentos de obligar al usuario en comprar. Es posible que el usuario recibió esta amenaza de scareware cuando ha dirigido su computadora a enlaces de anuncios legítimos. Los criminales tienen maneras de usurpar su computadora con scareware y, aunque usted se niegue a comprar, su computadora aun puede ser comprometida con programas maliciosos, así comprometiendo su bienestar económico de una manera u otra, incluyendo el robo de identidad. No permita que su computadora corra programas, sin su escrutinio. Las tácticas subversivas del scareware han causado más de 150 millones de dólares en pérdidas a los consumidores.

Tenga cautela. Los criminales del ciberespacio usan nombres simples para asociarlos a aplicaciones muy conocidas. Cuidado con los anuncios englobados. Para comprar aplicaciones anti-virus, averigüe primero el nombre exacto de la aplicación antes de permitir que un anuncio englobado lo lleve a otro enlace. Utilice programas de seguridad al día.

Si usted recibe uno de estos anuncios, cierre la pagina o apague el sistema completamente. Corra un sistema anti-virus cuando encienda su computadora.

Si ha experimentado con este scareware u otros fraudes similares, llene una querrela al www.ic3.gov. Para más información sobre avisos o información sobre el fraude al consumidor, visite nuestro enlace al www.consumertaskforce.org. Recibirá más información sobre fraudes, recursos disponibles e información para reportar una querrela. ¡Gracias!