The Fake Antivirus Has Evolved

You've likely run across them; often referred to as fake AV or scareware, fake antivirus banner ads and popup windows are designed to trick users into thinking their computer contains viruses, system errors, or spyware. The ads then offer a link to download (and pay for) fake antivirus software that will supposedly remove the virus. In many cases, when you move forward with the offer, malware is then installed on your computer. Even though consumers have become more prudent, millions have still fallen prey to this scam. The good news, thanks in part to crackdowns by the FTC, we are starting to see a decline in this type of scareware. The bad news is it's been replaced with a new generation of the same scam.

This new breed of scam still uses the ads and popups of old, but is now able to combine fake antivirus with basic screen-locking called ransomware. Ransomware is computer malware that holds a computer system hostage against its user by demanding a payment. To remove the ransomware, the bad guys will have you contact a "technician" who pitches you a support plan, putting the onus on you since you called them for help. By doing this, the scammers may try to exonerate themselves with the FTC by using the defense: "We didn't call the consumer, they called us".

But fear not. Fraudulent misrepresentation is a scam, regardless of whether the victim initiated the phone call. If you see a possible scam claiming a virus, spyware, or other false pop-up on your screen, the best course of action is to ignore it—unless the alert is coming from the antivirus software you already have installed.

Protecting Yourself from Ransomware

The experts at 41st parameters, a fraud prevention company, suggest taking these steps to avoid attacks or protect yourself after an attack:

1. **Use reputable antivirus software and a firewall.** Maintaining a strong firewall and keeping your security software up to date is critical. It's important to use antivirus software from a reputable company.
2. **Back up often.** If you back up files to either an external hard drive or to an online backup service every six months, you can restore your computer's system easily in case of attack.
3. **Enable your popup blocker.** Popups are a prime tactic used by the bad guys, so avoid even accidentally clicking on an infected popup. If a popup appears, click on the X in the right-hand corner.
4. **Exercise caution.** Don't click on links inside emails, and avoid suspicious websites. If your computer does come under attack, use another computer to research details about the type of attack. However, be aware, the bad guys are devious enough to create fake sites.
5. **Disconnect from the Internet.** If you receive a ransomware note, disconnect from the internet so your personal data isn't transmitted back to the criminals. If you have backed up your data, you may be able to re-install software. To be extra safe, take your computer to a reputable repair shop.
6. **Alert authorities.** Ransomware is a serious form of extortion. Local police are probably not equipped to deal with this, however, the local FBI may want to know about it.

Using BALANCE for Identity Theft Solutions

You may already know that banking with Bellco gives you access to BALANCE, a financial fitness program that offers financial counseling services to help you avoid bankruptcy, make informed spending choices, increase savings, and reach goals of home ownership, running a business, funding college education, retirement and more. But what you may not know is BALANCE also provides Bellco members with a wide array of Identity Theft Solutions.

These solutions include 5 main sections to help you avoid becoming a victim of identity theft and ways to recover if damage has already been done.

1. **Common Practices** educates you on illegal activities that thieves use to obtain your identity, what thieves will do with your personal information once they've taken it, and an assessment test to see how secure your identity really is.
2. **Prevention** offers ways to protect your private information that include credit reports, personal identity information, credit and debit cards, checking accounts, computers, credit monitoring, and credit protection.
3. **Consumer Rights** provides tips and education on the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Fair Credit Billing Act, the Fair Debt Collection Practices Act, as well as the Electronic Fund Transfer Act.
4. **Recovery Guide** gives identity theft victims helpful information when dealing with creditors and financial institutions, legal and government agencies, and credit reporting bureaus.
5. **Resources** offer phone numbers, addresses, and websites for credit reporting bureaus, government agencies, checking account fraud agencies, and even a contact to opt out of receiving pre-approved credit offers.

If you haven't already checked out the many benefits of working with BALANCE, stop by their website and see how they can help you.

Bellco Credit Union
1-800-BELLCO1 (235-5261)
7600 East Orchard Road, Suite 400N
Greenwood Village, CO 80111

Federally Insured by NCUA