Beware of Scammers Pretending to be Bitdefender Support

As Bitdefender's influence in the cyber-security industry grows, there are more scammers pretending to be Bitdefender tech support. Keep reading to learn how to identify and deal with fake tech support.

1. **SCAM POP-UP**

You're browsing online and suddenly an alarming error message pops up telling you that your device is seriously infected, and you need to call your antivirus company at the number shown on the screen to disinfect it.

2. **UNSOLICITED PHONE CALL**

Someone cold calls you or leaves a voicemail message pretending they are with the support department of your security solution and that they have detected serious issues with your device. They will manipulate you into saying the name of your antivirus and then claim to work for Bitdefender.

3. **FAKE SUPPORT WEBPAGES**

You're searching online for Bitdefender help desk and land on a site that seems legitimate. It has a big Bitdefender logo, and the phone number covers half of the front page. If you dial the number (usually Toll-Free), the person who answers will quickly try to gain remote access to your computer.

HOW FRAUDSTERS OVERCHARGE YOU TO FIX ISSUES THAT DO NOT EXIST

If you try to exit the page or hang up the phone, the frauds may try to convince you that doing this (e.g. waiting until the morning to get a second opinion or shutting down your device) could result in irreversible damage and that you have to instead allow one of their technicians to fix it.

They will usually have you bring up Windows features (Windows Event Viewer, Command Prompt, etc.) that a novice computer user might be unfamiliar with.

Then, they will trick you into looking for error messages that are in fact harmless and should not be considered evidence of a malware infection or system errors. But the scammer will warn you that these error records are dangerous and will completely wreck your data.

Then, they will offer their solution: giving them remote access to your computer to “fix” the issue. In truth, you are installing a remote access Trojan.

At some point during the “investigation”, the scammer will scare you into paying between $200 and $400 to fix the computer. The evillest scammers can even use their remote access to install actual malware or steal your personal documents and bank details. There are even worse cases of scammers that delete system files if the victim refuses to pay.

SOLUTIONS

Do not fall for these scams! Simply hang up the phone or close your browser to avoid getting scammed.

To **avoid** becoming a victim, keep this in mind:

- Bitdefender’s representatives will never call or email you out of the blue to tell you that there’s a security problem with your PC, Mac, or smartphone
- If you get a scam error message while you’re using a browser, remember that real errors & infections never prompt you to call a specific number
- Many of these fake warnings contain spelling and grammatical errors as well as caps and many exclamation points in red
- The best thing to do is contact Bitdefender Support. Here, you can browse our knowledge-based articles to find a solution to your issue, open an e-mail ticket, or you can speak with one of our support technicians by phone or chat.

If you think you have provided your account details to a scammer or if you have already paid for fake support, contact your bank or financial institution immediately and open a chargeback.

You may wish to **file a complaint** with the appropriate authorities or your regional fraud reporting center:

- in the **US**: file a report with the FBI | FTC
- in **Canada**: contact Canadian Anti-Fraud Centre
- in the **UK**: file a report with the National Fraud & Cyber Crime Reporting Centre | Report a cold call
- in **Australia**: contact the ACCC
- **other countries**: report international scams at ECONSUMER.GOV