December 2024

BWN COMPUTER

NEWSLETTER

Do You Really Need Antivirus Software These Days?

Antivirus software has been a standard recommendation for computer users for decades. But in 2024, with advancements in built-in protection, you might wonder if you still need antivirus software. Let's break it down together and see what makes sense for your home computer setup.

The Threat Landscape: What Are We Up Against?

Before diving into specific antivirus programs, let's take a look at the types of threats lurking out there. It's more than just old-fashioned viruses these days:

1. **Viruses and malware**
   These are the classic threats that most people think of. Malware includes everything from traditional viruses that replicate to malicious software that can steal your data or even lock you out of your own files (such as ransomware).

2. **Phishing and scam websites**
   Phishing attacks trick you into giving away personal information such as passwords or credit card numbers by pretending to be trustworthy sites or emails. Antivirus software often helps by blocking these sites.

3. **Spyware and keyloggers**
   Spyware hides in the background, watching what you do. Keyloggers are even sneakier, keeping track of what you type, which can put your passwords and sensitive information at risk.

4. **Zero-day threats and exploits**
   These threats take advantage of security holes in software that the developers haven't yet patched. Good security software can help catch these vulnerabilities before they become a major problem.

Windows Defender vs. Commercial Antivirus: What Should You Choose?

Now that we know what we're up against, the next question is: Is the built-in Windows Defender enough, or should you invest in a commercial antivirus program? Let's compare.

Windows Defender: The Built-In Protector

Windows Defender, which comes free with the Windows operating system, has come a long way but it is no match for a paid, consumer or managed antivirus. It is built right into your Windows computer and runs in the background without much fuss. Here are the benefits:

- **No extra cost.** It comes with Windows, so you don't need to pay extra
- **Simple and minimal**. It's easy to use, with no confusing pop-ups or renewal reminders.
- **Integrated protection**. Because Microsoft makes it, it fits in seamlessly with your system and is regularly updated.

However, Windows Defender isn't without its limits. While it provides basic defense, it falls short when it comes to more advanced threats, such as sophisticated phishing scams or newer forms of malware that commercial packages catch sooner. Therefore, we do not recommend using Windows Defender as your only security.

Do You Really Need Antivirus Software These Days?

>>>Continued from prior page<<<

Commercial Antivirus: Extra Security, Extra Features

Commercial internet security packages often offer more comprehensive protection. Here's what they bring to the table:

- **Advanced threat detection**. These programs usually have more advanced tools for detecting newer threats, including AI-based detection.
- **Additional features**. Many offer extra features, such as password managers, VPNs for privacy, and parental controls, which can be handy for families.
- **Better phishing protection**. They tend to excel in blocking fake websites that try to steal your personal information.

Of course, these extras come at a price. You need to pay for a yearly subscription, and they can sometimes slow your computer down a bit more than Windows Defender.

Managed Antivirus: Managed Security, Maximum Features

- Features real-time monitoring, threat detection and alerting.
- Enables rapid response, including for new threats.
- Provides a more robust and layered defense...with the ability to neutralize potential threats before they can infiltrate your system.

What Protection Do You Really Need?

The right level of protection depends on how you use your computer. Let's look at a few typical situations:

- **Casual browsers and email users** - If you mainly use your computer for Web browsing, emailing, and light activities, we recommend, at minimum, a commercial grade antivirus. They would offer decent security for day-to-day use, especially if you already practice safe habits such as not clicking on suspicious links.
- **Families and shared computers** - If you have kids or multiple people using the same computer, at minimum, a commercial grade antivirus, would be a better choice. Additional protection and parental controls can add peace of mind, particularly if younger family members are clicking on things they shouldn't.
- **Heavy online shoppers and work-from-home users** - If you shop online frequently, handle sensitive work information, or store a lot of important data on your computer, the extra security features of a managed antivirus package are HIGHLY recommended This would give you more sophisticated threat detection and privacy tools that can help protect your information.

Final Thoughts: Do You Still Need Antivirus Software These Days?

Antivirus software is still important and the type of antivirus you need depends mainly on how you use your computer and how much peace of mind you want.

Windows Defender and Mac security have come a long way but is nowhere near as good of protection as using a paid consumer or managed antivirus (and YES...Macs DO get infected).

And if you're unsure or need a little help figuring it out, call us at 940-282-0290.

We're here to help keep you secure.

How Scammers Use Your Friends to Steal Your Facebook Account

Imagine you receive a message from a friend asking for a little help. They say they are trying to get back into their Facebook account, and they need a special login code that Facebook will send to a trusted friend.

It sounds simple, right? You want to help your friend out, but here's the catch: the code they are asking for is actually the key to *your* account, not theirs. Let's dive into how this scam works and how you can protect yourself.

How does this Facebook scam work?

A friend asking for help

The scam usually starts with a message from someone on your friend list. It could look like they need help recovering their Facebook account or logging in on a new device. They tell you that Facebook will send a verification code to their friends, and they need you to share that code with them.

The message comes from someone you know, and they're asking for help. It seems harmless, maybe even urgent, and who wouldn't want to help out a friend in need?

The real danger behind the code

The big problem is that the requested code isn't meant for their account. It's the code to access *your* Facebook account. When Facebook sees someone trying to log in from an unfamiliar location or device, it sends a code to the account owner to confirm that it's really them trying to log in. This code could be sent via text or email, as part of Facebook's two-factor authentication process.

The scammer posing as your friend is actually trying to get into your Facebook account by tricking you into giving them this code.

Where it gets even trickier

This scam can feel especially convincing for a couple of reasons. First, the person reaching out might be using a fake account that looks exactly like your friend's, with the same name and profile picture. However, in many cases, the scammer might actually be using your real friend's account. They managed to compromise your friend's account first, and now they are using it to trick more people – like you. It's a chain reaction, where each hacked account leads to more and more victims.

How to protect yourself from this scam

Verify before you act

If a friend messages you asking for a code to help them recover their account, take a moment to verify things first. Don't feel rushed. Scammers often rely on creating a sense of urgency. Call your friend directly or message them on another platform to confirm that it's really them.

Never share login codes

Remember, any code that Facebook sends to *you* is meant to protect *your* account. It should never be shared with anyone, not even friends. If someone asks for a code sent to you, it's a red flag.

Look out for cloned accounts

If you receive an unusual request from a friend, check their profile. Look at their recent posts, photos, or activity. If anything feels off or incomplete, it could be a fake account designed to look like your friend.

How Scammers User Your Friends to Steal Your Facebook Account

>>>Continued from prior page<<<

What to do if you fall victim to the scam

If you've already shared a code and suspect someone might have accessed your Facebook account, here are the steps you should take immediately:

- **Change your password**. Update your Facebook password as soon as possible. Make it something unique and hard to guess.
- **Enable two-factor authentication.** This adds another layer of security to your account. You can set it up so that login attempts require a code from your phone.
- **Report the incident**. Inform Facebook that your account may have been compromised. They can help secure your account and investigate further.

We're here to help keep you safe online

Navigating the internet can be tricky, and scams like this are getting more sophisticated every day. If you need help securing your devices, give us a call. We're here to look after you and make sure your online experience stays as trouble-free as possible.

Stay alert, stay safe

Remember, a little bit of caution can go a long way towards keeping your accounts and personal information safe. If you're ever in doubt about a message or request, it's always better to double-check. Scammers count on us to act quickly without thinking things through. Let's not give them the chance.

We're always just a phone call away if you need help or advice. Stay safe out there!

You can call us at 940-282-0290.