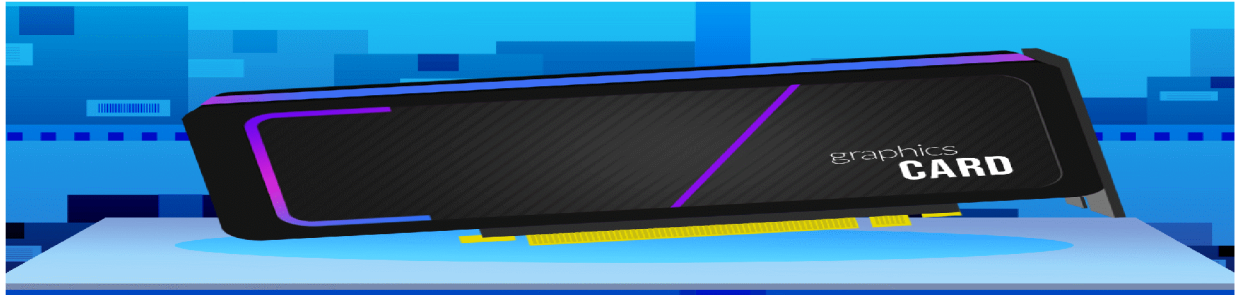




BWN
COMPUTER

NEWSLETTER

January 2023



GPU Shortage Ends: The Benefits

You may not think about it much, but your computer needs a graphics processing unit (GPU). The GPU allows you to see multimedia content and renders the graphics of your video games. It can also accelerate high-performance computing. The good news? It's no longer as difficult to get a new graphics card at a reasonable price.

A global shortage of GPUs in 2021 made it challenging to obtain new graphics cards. That could stall repairs and upgrades. Plus, people who wanted to build their own computers struggled to do so. If you did find a GPU available, you could expect to pay much more than usual. Scalpers were also buying the chips up and charging exorbitant prices.

One problem was that major chip manufacturers were struggling to source silicon. It's needed for the semiconductor functionality of GPUs. The pandemic slowed and even stopped production at some of the largest silicon manufacturers.

It didn't help any that cryptocurrency miners were buying up GPUs, too. They

needed the processing power to mine efficiently.

Why the shortage is over

Fortunately, the GPU shortage is ending. GPU manufacturers continued developing chips while waiting for the silicon semiconductors they needed. Now that those are back online, the graphics card companies can quickly make up for lost time.

At the same time, GPUs are no longer the best option for cryptomining. Instead, they have been replaced by more efficient application-specific integrated circuits (ASICs).

What happens next?

Actually, a surplus of older GPUs is expected, as a new generation of GPUs has arrived.

A new GPU series means manufacturers and computer parts stores will look to clear inventory. They'll want to sell off older GPUs to make room for the new product.

This can be good news. You can expect prices of the previous generation of technology to come down. Plus, you

can take advantage of the GPU surplus to replace a failing GPU. Or you can now upgrade your graphics card more affordably.

Get in the GPU Game

Want help upgrading your GPU or evaluating if your computer can handle the new GPUs coming in a few months? Our experts can help.

Contact us today at 940-282-0290.



What is SIM Jacking, and Why Should You Care?

If you play the popular SIMS life-simulation video game, you could think SIM jacking means someone takes over your characters, but the reality is even worse. SIM jacking is a type of identity theft targeting your real-life identity via your phone.

In SIM jacking a bad actor uses the subscriber identity module (SIM) card associated with your cellphone number to make calls, send texts, and use data. This has several potential negative outcomes:

- Your phone bill goes off the charts with international calling and data usage fees.
- They might impersonate you by sending texts to scam your friends and family.
- They can sign up for new email and social media accounts using your phone number.

Most importantly? They can use your phone number and SIM card to sign into your personal accounts. Many of us use text messaging for authentication. That's when a site, say your bank, sends a code to your phone to confirm it's you.

Now, imagine the criminal has access to your bank account through a leaked password. Whereas they couldn't get in before because of two-factor

authentication, they now have your SIM card, too. That means the SMS to authenticate your account also goes to them. They're in, and you're out.

How Does SIM Jacking Work?

Typically it starts, as so many cyberattacks do, with phishing. You might get a text or email that looks like it is from the cellphone carrier that asks you to click on a link. It might tell you there's been suspicious activity on your account or that your bill is past due. It's usually something that will make you anxious and feel the need to act urgently.

You're taken to a fake website where you provide your name, address, cell phone number, and date of birth. With the right information, the scammer contacts your phone carrier and asks for a new SIM card. Once they have that in hand, they access your account and take over your cellphone. If they pair that with leaked credentials, they can really do damage.

If you've been SIM jacked, you'll find out after the fact. You will no longer have a signal connection, so you won't be able to send texts or make or receive calls. You may also have difficulty signing into hacked accounts.

If you do think you've been SIM jacked, contact your carrier ASAP. Also, change your passwords and let your friends and family know. Otherwise, they might fall victim to a malware attack that appears to come from you.

Protect Yourself from SIM Jacking

Be careful with your personal information. Be wary of any requests to share your sensitive information online. Avoid taking action based on text messages or emails from people you don't know and trust.

Protect yourself by using an authentication app such as Google Authenticator or Authy. Do this instead of using text messages to authenticate yourself online.

Always update the applications on your smartphone. Yes, it seems like there are constantly new updates, but they can be protecting you from vulnerabilities.

Want to protect your online activity? Our IT experts can help update your applications and identify any vulnerabilities.

Contact us today at 940-282-0290.