



BWN COMPUTER
Repair/Service/Upgrade
940-282-0290

NEWSLETTER



6 Uses for Your Old, Extra Computers

When you have upgraded to a new computer, the old one is a bit of an albatross. You paid good money for that desktop or laptop, and you want to continue to see return on investment. Plus, disposing of that technology feels wasteful. It is not as if a computer is going to compost itself! To help, we have provided seven solid ideas for how to repurpose your old, extra computers.

#1 Turn it into a Kids' PC

Make the computer available exclusively to your young ones. You can set the device up with parental controls software to:

- limit the sites they can access;
- control when and for how long they can use the computer;
- restrict them from downloading without your approval;
- monitor their activity.

You can also isolate the device from the family's home network to further restrict their access and cut the risk of malware infection.

#2 Make a PC for Seniors

Or accommodate those at the other end of the seven stages of man. Turn the computer into one geared for older family members. Optimize screen

display color contrast for those with poor vision. Make the text size bigger. Set up the use of voice commands. You might even use puffy paint on the keyboard to make common keys easier to find.

#3 Convert to Storage

Storing documents, videos, photos, and music on your computer takes up a lot of room. So, turn that extra computer into a media storage device to keep your new computer in top shape. Think of it as an external storage device with much more capacity than a thumb drive.

Backing up your documents and media to the cloud is always an option. Yet, you may have more that you want to store than you want to pay the fee for storing.

#4 Share a Printer on the Network

If you have a printer that connects via a USB cable, you can generally print from that computer only. You can turn your old computer into a print server that shares the printer over the network. This way, any computer on the same network can make use of the printer.

#5 Donate

If the computer is in decent condition, donate it to a school, library, charity or

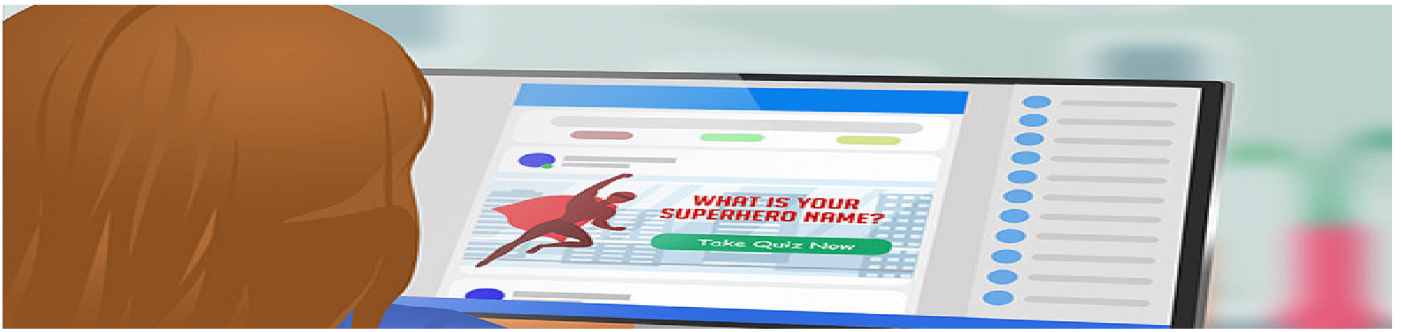
other non-profit. Of course, before doing so, you will want to clean it up:

- Back up and then delete all your files.
- Consider "zero filling" your hard drive so data cannot be recovered.
- Reinstall the operating system so it is usable by the recipient.

#6 Sell Parts

You could continue to see value from that extra computer by parting it out. This is a good idea especially when the computer is no longer working and cannot be held onto as a backup (just in case). In some cases, parts sell for more than complete computers.

When you are looking for that new computer (or for ways to repurpose your old one) our IT experts can help. Contact us today at 940-282-0290!



Beware These Social Media Scams

Huntington Volvo? Rowe Subaru? What will your hilarious quiz results be when you enter your fourth-grade teacher's name and first model of car? You may think it is silly entertainment ... until it is not. Many fun social media questionnaires are set up by hackers to steal your identity.

It seems like a harmless collection of random facts from your past. These quizzes might ask for details such as:

- What was your first job?
- What was the name of your first-grade teacher?
- What car did you learn to drive in?
- What was your first concert?

These popular quizzes promise to tell your "rock star" name or your "superhero" name. You know it is as reliable as the Magic Eight ball, but you play along anyway. We all need a laugh, right?

Except that the people really laughing are hackers. Many of the questions posed are also security prompts used to verify your identity online.

Cybersecurity experts agree, do not take these quizzes. It is not as if there is any real value in filling out the social questionnaire. You are simply taking the bait and risking having your personal data stolen.

Avoiding Social Media Scams

Here are some tips to help keep you safe from social media hackers:

- Do not get hooked by clicking on that post that seems too good to be true, especially shocking, or scandalous.
- Be wary of any quiz that asks for information that could be relevant to your online password.
- If you must quiz, fill out questionnaires on reputable websites only.
- Avoid quizzes that ask you to provide your email address.
- Contact companies through trusted channels only.
- Make sure that you are dealing with the proper entity's real website and not a look-alike site created by a scammer.

Also, think twice about apps that change your face into a cartoon character or a painting. Facial recognition is a more common security tool. Be cautious about letting unknown apps collect your photos and facial details.

What to Do If Your Online Accounts Are Hacked

#1 Have your devices inspected by trusted IT experts. This is one more area to be wary. Scam artists will set up

sites that appear to be affiliated to the manufacturer or phone numbers that appear to go to technical support specialists. It is best to take your devices to a physical repair shop with a real human doing the work.

#2 Change your passwords. When your account is hacked, you will want to change that password immediately. Plus, as annoying as it is, change passwords for all accounts accessed on the compromised device. The hackers may have installed a malware that tracked all data transmitted on the device.

#3 Set up credit monitoring. Notify any financial institutions or credit card companies if those accounts are hacked. You will likely need to have them issue you new cards with fresh account numbers. You can also ask them to monitor your accounts for fraudulent transactions. You might also set up credit monitoring with your region's credit reporting agencies.

Keep in mind that criminals can be patient and may not use your information right away. So, do not think you are in the clear because nothing happens in the first month.

Need help protecting your devices and online accounts? Contact us today at 940-282-0290!

We can also review your security setup at home to help keep you from becoming a victim of a cyberattack.