BWN COMPUTER

February 2023

NEWSLETTER

Is Your Data Breached? What to Do?

News of data breaches is all too common. This company apologizes for six million accounts breached. That company acknowledges hackers accessed 35,000 users' personal identifiable information. But the question that probably matters most: Is your data breached, too?

The company should contact you if your information is in a data leak, but you can't rely on that. You can also find out if your phone number or email address has been leaked by visiting https://haveibeenpwned.com/.

HaveIBeenPwned has uploaded various breaches and consolidated the information to make searching easy. Enter your address and get a list of breaches that compromised that email. You'll get a summary paragraph as well as a description of data compromised in each breach.

It is not uplifting reading! Next, the question is what to do about your breached information.

Steps to Better Security

First, change your passwords for those breached accounts. If you use that same password to access other accounts, change those passwords, as well, even if they are not listed as leaked. ***Always avoid reusing passwords. Yes, it can be a hassle to remember many different access credentials, but you risk exposing many accounts if you keep reusing one email address and password combo over and again.

Make using unique passwords for all accounts easier by using a password manager. A manager can store your many passwords in one place and generate strong ones to use. You can often download an app to your mobile device, which gives you the convenience of filling in your credentials when you're on the go, too.

The next step is to use two-factor authentication (2FA).

Understanding 2FA

This adds a layer of difficulty for hackers trying to access your accounts. Even if they had your username and password, they would need a second way to verify your identity.

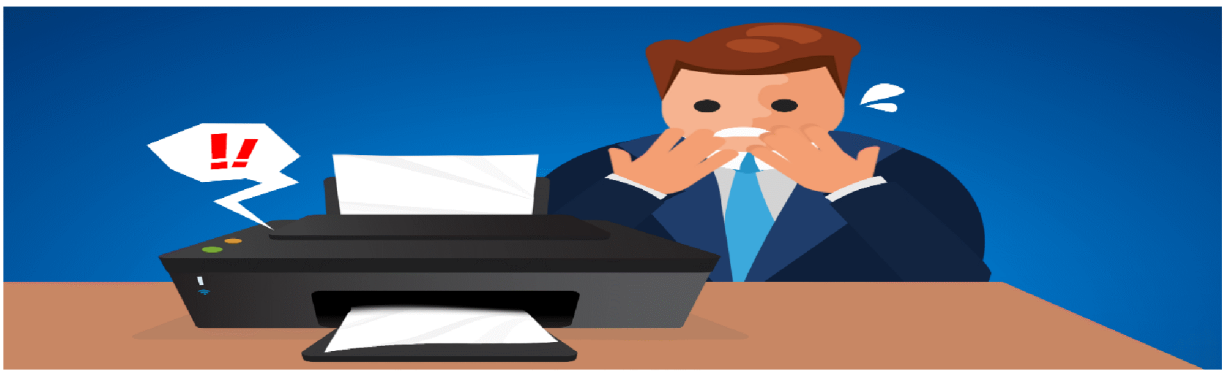
Using 2FA requires you to provide one of the following before you can gain access:

- something you know (e.g. the answer to a secret question);
- something you have (e.g. your smartphone);
- something you are (e.g. your fingerprint).

A bad actor would need to have not only your leaked credentials but also your other "something."

A common approach to FA is an SMS text message or voice-based authentication. You enter your credentials, then the site follows up with a text or phone call providing a separate code you must then enter. This is not the best method, however. Scammers can hack the SIM card associated with your device, and then use your number to make and receive calls and texts. Software tokens for 2FA are a safer solution. You'll download and install an application on your phone (e.g. Authy or Okta Verify). It can generate a unique verification code that is valid only for 30-60 seconds.

Want to learn more about password management and 2FA? We are here to help. Call us today at 940-282-0290.



Why Are Printers Still So Terrible?

Our phones can recognize our faces. Digital watches can detect that we've been in an accident. We can put on a virtual reality headset and feel as if we're swimming with dolphins. With all this technological innovation, why are home printers still so frustrating? This article explains why and how to make the most of the situation.

Hewlett-Packard released its home DeskJet inkjet printer in 1988. These printers spray liquid ink onto the page through printheads. Home laserjet printers followed shortly after. They use lasers to create static electricity to attract and melt toner onto the paper.

And here we are, thirty-five years later, with pretty much the same printer technology. Although now, you might also consider a multifunction (all-in-one) printer. These print documents and can often also scan, copy, fax, and email documents.

But we're still saddled with clogged inkjets and leaking ink cartridges, plus paper jams, or a printer that can't recognize the paper that you've now taken in and out of the tray 16 times in a row. Why?

Manufacturer priorities for printers

Printer manufacturers often lose money selling you the printer. Printer technology is quite complicated, but you're getting the device for the price of parts. That's because the manufacturer banks on making their money back on the sale of the ink.

Because they're looking to make money off ink sales, printer users now endure:

- ink cartridges that run out quickly – yes, they're putting less ink in their cartridges these days;
- printers designed not to work as well if you use off-brand cartridges;
- having to perform printer maintenance that uses up more ink.

Even if you do invest in top-quality, on-brand ink, you could still encounter problems. Connectivity issues or error messages when you change paper are common.

That's because the internal workings of the printer can be outsourced to the lowest bidder. Printer longevity is not the goal, so there's less incentive to develop robust networking components or print drivers.

Plus, printing is hard

It's not all down to printer manufacturer choices. Printing is a complicated process. Many moving parts need fine-tuning to apply the right pressure and position the ink. Plus, people could be using glossy photo paper one minute and recycled paper the next. At the same time, humidity or air that is too dry can also impact the paper and how the printer can move it around.

So, what can you do? Prefer a laser printer, which uses dry powder, if you're going to print mostly in black and white. You'll pay more upfront, but you're no longer hostage to the ink-cartridge dilemma. If you need to do color prints, you might find it's cheaper to actually go to your local print shop or big-box store.

If your Wi-Fi connectivity conks out, install the printer as a USB printer. It may not be as pretty, but it will get the job done.

Want to save hours of your life troubleshooting your printer woes? We can help. Contact our experts today at 940-282-0290.