Komputer Korner 6 - 26

By Stan Palen

stanpalen@breezeline.net

540.538.1200

Hints, Helps, Suggestions and News for IBM Compatible Computers

If you use Wi-Fi at home or in the office, make sure your router is current. Older routers are more vulnerable to hacking. If you are still using the default password printed on the router, change it.

World Password Day is observed on the first Thursday in May, which is May 7 in 2026. It aims to raise awareness about the importance of creating strong and unique passwords to protect personal information online. The cyber community recommends that you change your passwords yearly.

Changing passwords is fairly easy with a password manager. If your password manger already has your current password, you can start the change with forgot password or just request update password under your account. The password manager will suggest the password and insert it in both the password boxes and store the new password. You can insert your password, but people tend to make their passwords too similar. If someone figures out one of your passwords, it makes it much easier to guess the rest of them.

I do not trust the save password option on any of the popular browsers except maybe DuckDuckGo. They are too big a target. I use 1Password. It can be installed on all your devices. I do not have passwords saved on my phone by my phone company or browser. 1Password can be opened with my fingerprint on my phone.

The FBI and the Cybersecurity Alliance strongly recommend rebooting your router. Unplug it, wait one minute, and plug it back in. In many cases, this helps the router install the latest security updates, along with other fixes. They also recommend changing your Wi-Fi password. Some brands still use admin as the default username, so change that as well. Be aware that your internet provider may not be able to help you sign in, so write down your new router username and password.

For more information, see Cybersecurity Alliance guidance.

The FBI has remotely rebooted many routers, but there is no way to know whether yours was included.

Many scam messages claim you paid $399, or another amount, to a well-known company. If you try to investigate the charge through the message, you may be putting yourself at risk. Simply opening the message can cause problems, and clicking any link is even riskier. Some messages include hidden links, and scammers now use AI to create fake websites that closely mimic real ones. Treat any message you cannot fully verify as a possible scam.

I receive about three messages a day that appear to be from my internet provider, warning that my email will be shut down within 24 hours unless I click a link. You would think the provider could block these messages from getting through.

I recently received a fraud alert from my bank describing a customer who got a call showing Chase on the caller ID. The caller claimed he needed to move his money immediately into a "safe" account in his own name. She told him to use Zelle, a wire transfer, or an account-to-account transfer or risk losing everything. He hung up, called the number on the back of his card, and learned that nothing was wrong with his account.

Stay safe out there,

Always pause before responding.

Don't forget to send!