You're Gonna be a Hacker, Kid!

You've seen it everywhere: at your local hospital, government, maybe even a business you know. What is it? Ransomware! It's the digital version of a hostage situation, but the hostage is your information.

These fraudsters, although sounding like specialized hackers from a world-renowned spy group, might be like your friend Gary down the street...

Gary is a janitor that's in a bit of a pinch; he needs some quick cash to pay his mortgage, but he doesn't have time for a second job. Gary knows how to use basic programs, like Word and Adobe, but he doesn't know how to create Ransomware itself, so he bought it from an online vendor for $50. All Gary has to do is type in his friend's (or foe's) email addresses into an email, and he can start his misadventures right there. If he's lucky, this scam will pay off his debts this month and might even drain your bank account. If you were to fall for this trap, would you trust that Gary knows how to unencrypt your information? By following the suggestions below, you can protect yourself, your clients, and your family from becoming another victim of Ransomware.

Ways to protect yourself:

Report any suspicious emails immediately.
If your company has a team that assists employees with suspicious emails, alert them immediately. If not, report it to your manager(s) or local IT team for help to determine if it's safe. Lastly, delete the email if it's just you and your family. You may have just saved yourself from becoming a victim.

Do not open attachments that you were not expecting.
A common way fraudsters like to deliver Ransomware is with attachments like a fake invoice or other documents commonly used in your industry. They are often in the form of a PDF but can be in any document type, so don't let your guard down just because it's a picture file.

Do not download documents/files from the internet.
Fraudsters will put fake documents on file-sharing websites and wait for you to download them, but this can be easily thwarted. If your career requires you to have certain documents, the company will usually provide them or have a group/person you can ask to procure the documents for you.

Back up your information.
You can do this by using the cloud or a physical device - like an external hard drive - to store a copy of all your documents. That way, if a fraudster deletes or encrypts your original files, you still have a copy. Remember, don't use an easily-guessable password, and don't leave your backup "hooked up" to your computer when not in use.

Do not reuse passwords.
It's hard to remember all your passwords, but that's where a password manager can help. It can securely store all your passwords then provide them back to you when logging in to a website or a service account you use. This will make it much easier to have unique, strong passwords for every website and account you have. No extra brainpower needed!