COMPUTER GURU

by Don Benjamin

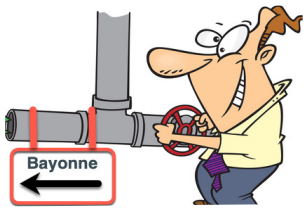
Technology Lab Programs sponsored by: NightingaleNJ Eldercare Navigators

The Colonial Pipeline Hack

Reusing passwords for different accounts is risky. Not only should you employ unique passwords, you should also opt for double authentication when you sign in to your most critical online accounts.

On May 7, 2021, Colonial Pipeline, which delivers refined petroleum products from the Texas Gulf Coast to New York, shut down its operations when operators discovered a cyber intrusion had corrupted the company's computer files.

When the dust cleared, it appeared that hackers obtained one of the company's passwords from another source, which let them log into Colonial's file system to wreak havoc.



Harold is closing the oil valve that serves Bayonne in this actual re-enactment.

But how? And could this happen to you? Let's see…

Hacker groups routinely sell IDs and passwords they steal from corporate servers. For example, between 2014 and 2018, hackers stole some 500 million IDs and passwords belonging to customers who signed up for the Marriott Miles program. The hackers then sell these stolen credentials on the internet.

Suppose you're a Marriott customer whose ID and password were stolen, and also suppose you use the same ID and password for your PNC online bank account. If someone steals your Marriott credentials, they could attempt to log into your PNC account with the same ID and password, and if they're successful, they'll have access to your bank accounts.

Sheldon takes computer security very seriously.

Apparently, Colonial Pipeline reused a password for its corporate file system that had been stolen from another database of ID's and passwords. That enabled the hacker to log into the Colonial Pipeline data files, encrypt the information, and demand a ransom from Colonial for the decryption key.

That's why you must use a different password for every online account—especially your most important accounts, like your bank, Social Security, Amazon, and so on—anything that involves your money, identity, or other information you want to keep private.

Double Authentication

Many online accounts offer an additional security check called double authentication. I started using double authentication two years ago after my bank notified me that someone was trying to log in to my account with the wrong password. Now, when I log into my bank account, the bank sends a six-digit code to my smartphone that I must enter on my computer. That code is different every time I log in, and it helps confirm that I am the legitimate owner of the account.

With double authentication in place, even if hackers have my password, they still can't log in because they don't have a way to receive the code. And if they tried, I would receive the code, which would warn me that someone was trying to log in, and I would change my password immediately.

Trusted Devices

Some online accounts require that you register the device (computer, tablet, smartphone) on which you'll log in to your account. When adding device registration to double authentication and a unique password, you will be authenticated based on something you know (your password) and something you own (your registered devices).

If you have questions about computer security, just mosey on over to the PSRC website, click the Tech Resources webpage and fill out the Tech Request Form at **princetonsenior.org/psrc-tech-resources/**.