It is very well-known what vulnerabilities arise when not having a strong password. Now-a-days, most sites are using the two-step verification method, which while an extra security measure, does not keep the user completely safe from having their password exposed. With offline hackers, when they gain access to the sites database, “the attacker has complete access to the database comprising passwords of all registered users of a website. The attacker in possession of the password database can generate and verify potentially unlimited guesses against hashed passwords. And, if passwords are simple, such as dictionary words or small enough for brute-force search, then the attacker can recover them in no time (Tupsamudre, H., & Lodha, S.).” With the attacker being in the database, they bypass the need for two-step verification and scan the database for well-known passwords.

References:

Tupsamudre, H., & Lodha, S. (n.d.). Passwords: Divided they Stand, United they Fall [PDF].

Response:

Hello Jared,

Being that you are a Penetration Tester, your mind would one that I could pick for hours! I’m sure discussion topics like this are second nature for you lol. I was also reading somewhere how hackers use common replacements like 3 for e, or 0 for o. Is it a common practice to try and crack passwords with missing letters? It’s how I have been creating my password for a long time. It might look something like if my password were to be “thisismypassword”, I would remove all the S’s to make “thiimypaword.” Unlike this example, the letters I typically remove, make my passwords easy for me to remember.

-Dan

Hello Camren,

It does seem that many facilities have forgotten the importance of their physical database security. I used to perform service on Audio/Video systems that were housed in the same room as their databases. I would say that about 30% of the time, I would get to the IT closet that was unlocked and not in eyesight of anyone in the facility. I’m guessing they’ve never experience a physical hack but they sure seem to be leaving themselves vulnerable to one.

-Dan