



cloudnexus

The Secret to Good Passwords

CloudNexus provides cyber security services for companies throughout the USA. Consider this a PSA. Often times we need to pretend to be like the bad guys to help our customers stay secure.

Everyone jokes about the questions you answer on these social media quizzes and the latest, senior high school yearbook pictures.

As a rule: If you post something, then never use any part of it in a password or security question. There are certain things that can be derived from too many places that people put in passwords and we are preaching caution.

Almost everyone posts something that can point a bad actor to anything about high school. We can tell what high school you graduated from and when from the following:

1. Any reference to your age or birthday
2. 2. Hometown
3. 3. Your friends

There are too many points where we can figure out your password from your high school, favorite sports teams, pet names and kids' birthdates. Usually within an hour or so, we can determine your password if you are like 70% of online users.

Creating passwords needs to be derived from something only you know. Think of things only you have control over. What is NOT something only you know:

1. Dates: anniversaries, birthdates, etc. your spouse, kids or friends know these dates. They can post Happy birthday or happy anniversary messages on your wall. Your kids can post their birthdays in one of their social media accounts or post pictures from a birthday party, senior prom, etc.
2. Sports team favorites.
3. Cars you have owned
4. Pets and their names
5. Previous addresses

You get the idea... these are all things that other people know and can inadvertently expose and with little effort, can be linked back to you.

There are challenges here though. Many financial institutions use auto loan details or mortgage details to verify that you are who you claim to be.

So what should you do?

The best passwords are 18 to 24 characters (64 is ideal). Mix upper case, lower case, numbers and special characters. Make the password very obscure but at the same time very familiar and easy to remember for you and only you.

Example: maybe your fondest memory is of Kermit the Frog so look for a song by Kermit and take the first letter of each word in the lyric with a few random characters.





cloudnexus

The Secret to Good Passwords Cont.

"It's not that easy being Green having to spend each day the color of leaves when I think it can be nicer"

!^t3BGh2s3Dtc0Lw1ticB^

! Used as "l" upper i
1 used as "l" lower L
^ used as "n"
3 used as "e"
2 used as "to"
0 used as "o"

Basically you are creating a secret code but you will find that as you recite the lyrics, you will more easily remember your password as you type it.

Never use the same password twice. Come up with a phrase that you can use that will be easy to remember but still be cryptic.

Phrase: Mom likes to get her (***) at Walmart so your online Walmart password can be:
Ml2gh(G)@WLMrt

For Kroger:
Ml2gh(G)@K

For Walgreens:
Ml2gh(G)@WlGrns

Try not to be too patterned but basically reciting common phrases while typing the first letter of each word with a symbol or number that looks like the letter gives you a nice cryptic password and it is a lot easier than it looks. After the first few times you will get used to it.

Be aware of what financial institutions ask you for security questions. Do not provide a security question that you might have posted about or that somebody else knows.

Don't be afraid of posting high school class year or what high school you went to as long as you don't make it a habit of including that information in any passwords.

We all have to be more diligent. A lot of these password guesses are now built into dictionary files that are brute force attacks hackers use with what's called a Dictionary Crack. It's not some individual trying to get your information now. It is now automated with the use of bots on the Internet that is automatically probing banks and other websites that you might have an account on to get your info.

Things are very different now. We have to be aware of what information we have shared and what we need to be careful about sharing. We have more control than you think. Make sure the information is something only you control. A lot of bad guys and gals are out there trying to get your money. Be safe out there.

