Online Safety

Password and Account Best Practices

CloudNexus does cybersecurity 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.

The biggest threat to you and your employer is using simple to derive passwords. Today, we use social media to stay in touch with friends, relatives, classmates and acquaintances. Unfortunately, every interaction online with these friends can be data that feeds social engineered attacks of your accounts. Quizes you take online, tagging your self on someone else's timeline are all small pieces of a puzzle as to who you are and what you like.

From your Facebook account, can we glean what professional sports team you follow? What year you graduated? Your anniversary date? Child's name or birthday? 70% of individuals use these bits of information, usually compbined, to create easy to remember passwords. The bad guys know this and can quickly put together a list of passwords to try.

We professionally recommend using a password manager such as Lastpass. The tool is inexpensive and very secure. It has a random password generator and the license you get can be used on mobile devices as well as a computer. When you come to a webpage you know, the LastPass plugin will populate the username and password fields with a click of your mouse. That way you never have to remember a password. (except the one to get into LastPass).

In additions, we highly recommend enabling MFA or 2FA (Multifactor Authentication) Such as Authy or Google Authenticator to better secure your accounts. These are randomly generated 6-digit codes you get from your app or in a text message that you enter after you login.

The latest version of LastPass has this capability as well, but we recommend separate applications as an added layer of safety.

But, if you must….

If you do have to create a password from scratch that is not from a password generator, here are some tips.

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.
2. Sports team favorites.
3. Cars you have owned
4. Pets and their names
5. Previous addresses

These are all things that can be shared or derived from social media. Trying to come up with something unique is difficult for the human brain to do as we always need a reference. But there are ways to generate passwords yourself that are complex and easy to remember.

Online Safety

Password and Account Best Practices

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. Kermit the frog song lyric:

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

Password result: !^t3BGh2s3Dtc0Lw1ticB^

! Used as “I” 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

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 select 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.