# TIPS to create unbreakable password

You can lock every door and window of your house, but if you use a skeleton key the odds are pretty good someone is probably going to end up robbing you blind. The same is true of your passwords. If your passwords are not unique and unbreakable, you might as well open the front door and invite the robbers in for lunch. The following are a few tips that might help you develop passwords that are especially complex, nearly unbreakable, but also memorable.

## Nursery Rhymes

One preferred method of coming up with complex passwords that pass every IT security policy out there – even those that require 15 character passwords – is the nursery rhyme technique.

Choose one of your favourite nursery rhymes, capitalize the first letter of each sentence, replace certain letters with numbers, and follow that up with an exclamation point or some other symbol at the end. For example, take the nursery rhyme Little Boy Blue, which goes like this:

"Little boy blue, come blow your horn. The sheep's in the meadow. The cow's in the corn."

Now you transform that replacing any "s" with "5" and any "L" with a 1 or a 7. Here's the new password.

"7bbcbyhT5itmTcinc!"

That's an 18 character password that includes numbers, letters, uppercase, lowercase and at least one special character.

## Use Industry Lingo

One alternative of this is using very specialized industry lingo to come up with the phrase. Nursery rhymes or even movie quotes could be guessed with a computer algorithm running through as many possibilities as a computer can manage. However, industry-specific lingo is much harder to guess.

For example, if you're a nurse, your phrase might be:

"The aortic coarctation led to an agonal response, BLS and finally intracerebral infarction."

Replacing "a" with 0 results in the following password:

"T0clt00rb0fii!"

This is only 14 characters rather than 18, but much harder to guess.

## Use a Keyboard Pattern

Here's a fun password approach that uses the same technique as the smartphone login pattern. In this case, what you're going to use is your keyboard. Draw some kind of recognizable pattern on your keyboard, and then use the letters and numbers as the password. For example, let's say you create a pattern on your keyboard as shown below.

If you start this pattern at the number 3, it should be pretty easy for you to draw out the pattern each time. If it helps, you might even draw recognizable images or letters on top of the keyboard. In the case above, the password ends up as follows:

"3waxcvgy7890-="

Using this approach, you can alter the complexity of the pattern to lengthen the password. A hacker could potentially run an algorithm through that would attempt every password possible on a keyboard by connecting every key to one another, so making the pattern as complicated as possible – such as going back and forth or making complex, diagonal lines – should make that kind of hacking much more difficult.

*(makeuseof.com)*

# Google suspends fact-check

**San Francisco**

Google has suspended its fact-check feature in its Search and news results after its algorithm wrongly linked a Washington Post fact check to a Daily Caller article about US Special Counsel Robert Mueller's investigation team, the media reported.

Noting that the feature proved to be too faulty for public use, Google attributed the decision to an investigation by The Daily Caller News Foundation after it published a story lambasting the tech giant for wrongly appending a Washington Post Fact Checker debunk to one of its stories.

"We launched the reviewed claims feature at the end of last year as an experiment with the aim of helping people quickly learn more about news publications," *The Daily Signal* quoted a Google spokeswoman as saying.

"We said previously that we encountered challenges in our systems that maps fact checks to publishers and on further examination it's clear that we are unable to deliver the quality we'd like for users," she added. *(IANS)*

# GFH shares begin Nasdaq Dubai trading

**Manama**

GFH Financial Group announced the inclusion of Single Stock Futures Contracts on the Group's shares available for trading on Nasdaq Dubai's equity futures market with effect from 16 January.

GFH joins 16 other leading UAE-listed companies whose futures already trade on the Nasdaq Dubai market. These include leading companies listed on the Abu Dhabi Securities Exchange (ADX), Dubai Financial Market (DFM) and Nasdaq Dubai. Among them are Abu Dhabi Commercial Bank, Aldar Properties, Arabtec Holding, DP World, Dubai Islamic Bank, DXB Entertainments, Emaar Properties, Etisalat and Union Properties, among others.

The addition of contracts on GFH's shares were added to the futures market, which was established in September 2016, as a result of Nasdaq Dubai's development strategy, which aims to add

*Hisham Alrayes, CEO of GFH*

further depth and breadth to the futures market as it works to provide derivatives trading opportunities in regional assets.

Hisham Alrayes, CEO of GFH, said, "We're pleased to see GFH's shares included alongside the UAE's leading listed companies on Nasdaq Dubai's equity futures market. GFH's shares continue to be among the most actively traded on the DFM and GFH is the first non-UAE based company to be listed on Nasdaq Dubai futures market. The continued development of the region's capital markets is a win-win for companies and for our investors who are now being given greater freedom and options to better manage and hedge their exposures".

# Twitter finds 1,062 more Russia-backed accounts

**San Francisco**

Twitter has identified an additional 1,062 accounts associated with the Russia-backed Internet Research Agency (IRA) accused of interfering with the 2016 US presidential election.

This brings IRA-linked accounts to a total of 3,814 that posted 175,993 tweets, approximately 8.4 per cent of which were election-related, the micro-blogging platform said in a blog post on Saturday.

"We are emailing notifications to 677,775 people in the US who followed one of these accounts or retweeted or liked a Tweet from these accounts during the election period," Twitter said, adding that it has already suspended these accounts.

Twitter has told a US Senate committee that the micro-blogging platform is working towards alerting its users who may have seen Kremlin-linked advertisements during the 2016 election.

Appearing before the US Commerce, Science and Technology Committee this week, Carlos Monje, Twitter's Director of US Public Policy, said Twitter would 'inform individually' everyone who saw tweets from accounts linked to IRA. *(IANS)*