'Password fatigue' haunts Internet masses

June 25 2013, by Robert Macpherson

People group around laptop computers at a cafe in Beijing on May 29, 2013. Passwords have proliferated so much that it's a daily struggle for users to cope with dozens of them—often across several devices.

Looking for a safe password? You can give HQbgbiZVu9AWcqoSZ mChwgtMYTrM7HE3ObVWGepMe OsJf4iHMyNXMT1BrySA4d7 a try. Good luck memorizing it.

Sixty-three random alpha-numeric characters—in this case, generated by an online password generator—are as good as it gets when it comes to

securing your virtual life.

But as millions of Internet users have learned the hard way, no password is safe when hackers can, and do, pilfer them en masse from banks, email services, retailers or social media websites that fail to fully protect their servers.

And besides, with technology growing by leaps and bounds, why does the username-and-password formula—a relic of computing's Jurassic era—remain the norm?

"The incredibly short answer is, it's cheap," said Per Thorsheim, a Norwegian online security expert and organizer of PasswordsCon, the world's only conference dedicated to passwords, taking place in Las Vegas in July.

"If you want anything else—if you want some kind of two-factor authentication that involves using a software-based token, a hardware-based token or biometric authentication—you need something extra," he told AFP.

"And that will cost you extra money."

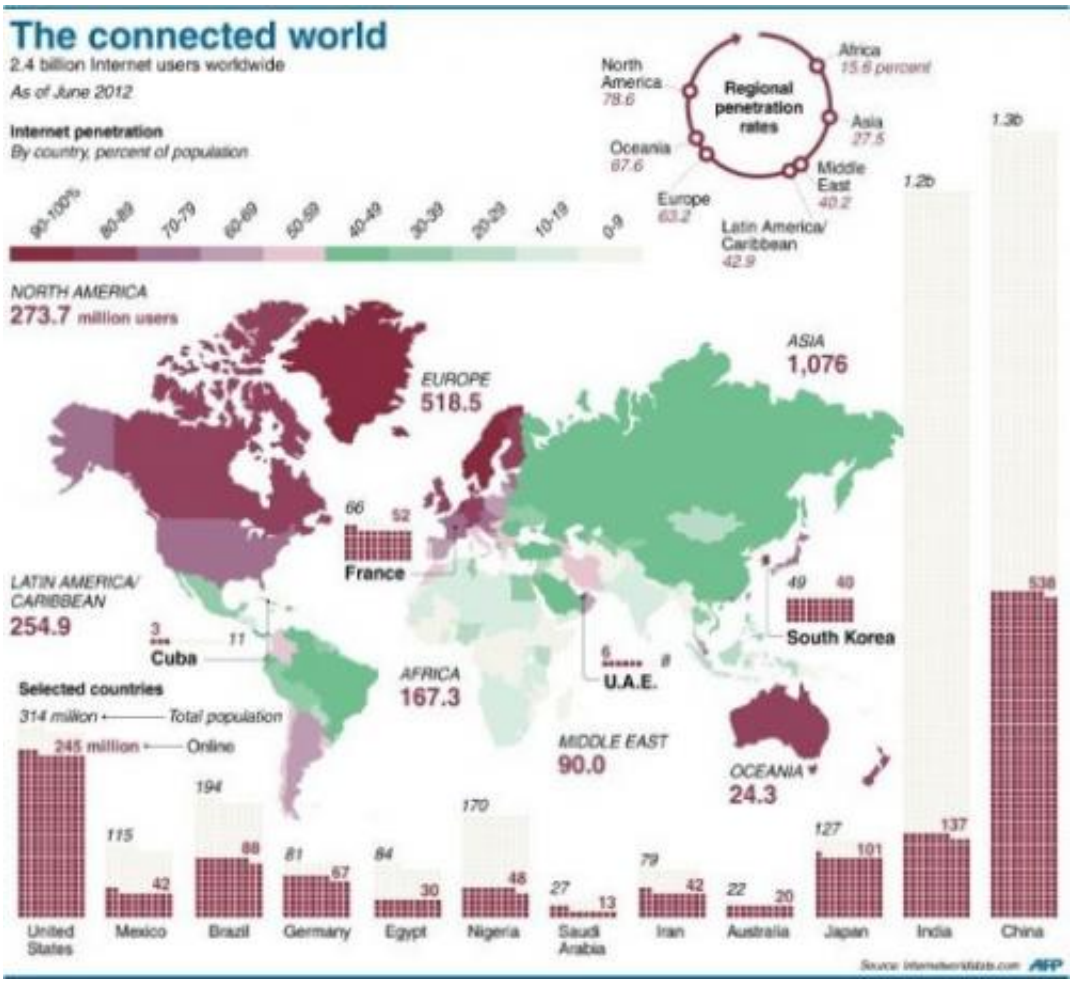
Back in the beginning, it was all so easy.

The very first computers were not only room-sized mainframes, but also stand-alone devices. They didn't connect to each other, so passwords were needed only by a handful of operators who likely knew each other anyway.

Then along came the Internet, binding a burgeoning number of computers, smartphones and tablets into a globe-girdling web that required some virtual means for strangers to identify each other.

Passwords have thus proliferated so much that it's a daily struggle for users to cope with dozens of them—and not just on one personal computer, but across several devices.

There's even a name for the syndrome: password fatigue.



Graphic showing the percentage of national populations connected to the Internet.

"People never took passwords very seriously, and then we had a number of really big password breaches," said Marian Merritt, Internet security

advocate for software provider Norton.

"As people are increasingly accessing websites from smartphones and tablets, typing passwords is becoming an ever bigger pain," added Sarah Needham of Confident Technologies, developers of a picture-based password alternative.

In a 24-nation survey last year, Norton found that 40 percent of users don't bother with complex passwords or fail to change their passwords on a regular basis.

Rival security app firm McAfee says its research indicates that more than 60 percent of users regularly visit five to 20 websites that require passwords, and that a like-sized proportion preferred easy-to-use passwords.

The most popular passwords, infamously, are "password" and "123456," according to Mark Burnett, whose 2005 book "Perfect Password: Selection, Protection, Authentication" was among the first on the topic.

People use their laptop computers at a Starbucks in Washington, DC, on May 9, 2012. Norton found that 40 percent of users don't bother with complex passwords or fail to change their passwords on a regular basis.

Biometrics are coming

Carl Windsor, director of product management at California-based network security firm Fortinet, said he once ran John the Ripper, a free program to crack passwords, through an employer's Unix system with its consent.

Within seconds, Windsor had one-third of its passwords. Within minutes, he had another third. "I also won a bet by finding the 'super secure' password of a colleague in less than five minutes," he told AFP by email.

Password alternatives are in the pipeline.

Google is toying with the idea of users tapping their devices with personalized coded finger rings or inserting unique ID cards called Yubikeys into the USB ports of their computers.

The FIDO Alliance, a consortium that includes PayPal, is pushing an open-source system in which, for instance, websites would ask smartphone users to identify themselves by placing their fingertips on their touchscreens.

"These (biometric) technologies are coming to a place where they are highly mature, cost effective and in a position to roll out into the consumer market today," FIDO's vice president Ramesh Kesanupalli told AFP.

Kesanupalli said FIDO technology could be available as early as this year, bettering IBM fellow David Nahamoo's prediction in 2011 that biometrics would replace passwords within five years.

In Washington, the US Patent and Trademark Office has recently published several patent applications from Apple that envision facial recognition and fingerprint scanning.

Motorola's head of research Regina Dugan has gone further, proposing a "password pill" with a microchip and a battery that would be activated by stomach acid. The resulting signal would emit an unique ID radio signal.

"I take a vitamin every morning. What if I take vitamin authentication?" said Dugan at the D11 tech conference in California last month, quoted by TechWeekEurope.co.uk.

For now, many Internet services are embracing two-factor authentication, that challenges users with a bonus security question—like "What is your dog's name?"—or emits a one-use-only numeric code via SMS messaging.

Online password managers with names like Lastpass, KeePass, 1Password, Dashlane and Apple's just-announced iCloud Keychain have also been popping up like mushrooms.

They pledge to securely stash an individual's entire password collection, accessible via one master password. Some experts, however, consider the idea a Band-Aid solution pending the definitive password replacement.

Until then, security experts widely agree on two core principles: make your passwords as long as possible, mixing up words with some numbers and symbols, and never ever use the same password for more than one website.

Beyond that, just cross your fingers and pray that the website you're using is doing all it can at its end to protect the mental keys to your virtual world.