Passwords That Won't Make You Ill

cyber security risk management

Summary: Now that hackers use sophisticated tools to detect versions of commonly used passwords, the National Institute of Standards and Technology (NIST) issued revised password guidelines. We have the update for you.

You have probably seen people sitting on planes wearing masks to protect others or themselves from illness. Pollution in some cities worldwide is also a problem. That is why we were intrigued by a new invention known as breaze. You charge it up each night so its fans and filters can work all day as you go about your business. Who knows if this will take off, but it might help people stay healthier perhaps.

On the banking front, the focus is always on keeping healthy, particularly when it comes to cybersecurity. Given October is National Cybersecurity Month, we wanted to bring you some information on passwords and cyber risk.

Now that hackers use sophisticated tools to detect versions of commonly used passwords, the National Institute of Standards and Technology (NIST) issued revised password guidelines to help people create passwords only they would know (and that would be difficult for thieves to crack).

"If you can picture it in your head and no one else could, that's a good password," says Paul Grassi, the institute's senior standards and technology advisor, who oversaw the revision of Special Publication 800-63B on Digital Identity Guidelines.

Gone are recommendations to make passwords overly complex. Now, the important thing is for them to be personal and unique. Anything that you could easily think of might be a good password (a unique experience or diverse interest perhaps). Moreover, with these uniquely crafted passwords, you may not need to change them as often either. Let's face it; passwords are usually only changed minimally when they must be changed so often. As Grassi notes, these changes aren't really effective.

Some things still hold true when it comes to passwords though. NIST's guidelines continue to call for restricting sequential and repetitive characters (such as 12345), along with words that pertain to the particular site that the person is using.

Also, commonly used passwords (such as p@ssw0rd), are still big no-nos. Be sure to warn both employees and customers not to use passwords they may have had at other institutions or websites that subsequently suffered breaches. NIST says hackers often search for those first.

While the recommendations are intended to make passwords harder for hackers to crack, NIST stresses that banks and other companies should still employ multi-factor authentication measures to lessen the chance of successful breaches.

Indeed, more organized crime rings are successfully performing account takeover attacks on web and mobile applications. So, thwarting them with both unique passwords and additional authentication puts up two walls of defense.

Know that criminals typically buy lists of commonly used user name and password combinations on the black market, and input the pairs into password cracking software called automated credential stuffing tools. Cybercriminals then use botnets to infect websites and mobile apps, enabling them to then use these credential stuffing tools to crack user names and passwords.

This all sounds a bit scary, we know. But, with cyber risk a top concern and priority for banks, we want to keep you aware of the latest happenings on cyber risk.

LOAN SERVICES FOR COMMUNITY BANKS

PCBB is almost entirely owned by community banks and it does not compete for your business. Contact us to do loan participations as you protect your customer relationships.