Password Management Reminders In A WFH World

cyber security employees

Summary: Password protection is especially important these days. We share three key password management reminders.

The computer password was created in 1960 by Fernando Corbato of MIT. Its original intent was to keep individual files private, while users worked on them. Fast forward 60Ys and the idea of private information has expanded exponentially.

Despite decades of advancement, the primary form of security for many bank employees is still the password. Furthermore, with many bank employees working from home in recent months, the potential risks of basic password security are becoming more evident. With so many personal and professional sites and networks requiring passwords, most folks on average have to remember at least 90 passwords. Because of that, nearly two-thirds of people admit to using the same password for many or even all of their accounts, according to Harris Poll and Google's Online Security Survey.

Another study by cybersecurity provider Security.org surveyed 1,012 Americans to look at how they managed password hygiene differently. Across all of the demographics, 72% said that they "recycle" old passwords at least 4x across multiple uses and accounts. Moreover, 76% of millennial respondents admitted to frequent password reuse, as compared to just 56% of boomers.

With far more bank employees and contractors working from home lately and possibly for some time to come, here are some suggestions to keep your staff and customers more secure and compliant in their password management:

Encourage password complexity. Make sure that passwords include at least 12 characters with a mix of numbers, symbols, upper and lowercase letters. This can result in hundreds of millions of password options that take up to 200Ys to crack, according to security experts. Encourage employees to keep their passwords random and complex by making use of password generators or coming up with a sentence or phrase that is easy to remember but hard to crack -- and issue reminders by newsletter, emails, updates, and via cybersecurity compliance training.

Be wary of password managers. Password managers have been touted as helpful to store a large number of passwords. However, be wary of these mechanisms. As anything else online, they can be breached and so they should be thoroughly reviewed for any weak spots for cybercriminals before using.

Remind users of important security practices. All of this will not do much good if employees are sharing their passwords, reusing them frequently across personal and business accounts, and writing them down on sticky notes. (Luckily, at least 24% of Security.org study respondents of all ages said that they were "more likely" to use a password management app than use the still alarmingly popular sticky note route.) Send reminders to employees to change passwords on the first day of the month, or at some other regularly appointed time. Encourage them to see changing their password like paying their mortgage or changing the batteries on their smoke detector: A regular practice that they must adhere to for their sake and yours.

TWO APPROACHES TO STRESS TEST YOUR LOANS

Now more than ever, it is important to stress test loans of all types from multiple perspectives. Choose your approach and get expert help, as needed. Learn more about credit stress testing today.