Issued 6/10/18

25% of Employees Use the Same Password for Every Account

Employees may be a company's greatest asset, but they also remain the greatest cybersecurity risk, according to a Monday report from OpenVPN. Despite an increased focus on security training, 25% of the 500 US employees surveyed report that they use the same password for every account, the report found. Another 23% of employees said they frequently click on links before verifying that they lead to a legitimate, safe website. Of the employees that use the same password for everything, a whopping 81% said they do not password protect their computer or phone at all, according to the report. It should go without saying that reusing passwords is a risky behavior that can put an entire company at risk, as weak passwords can be more easily bypassed with brute force attacks. It can also cause damage to the individual, as using the same password to protect bank accounts, email, and social media can risk compromising both personal and work information, the post noted. Traditional password best practices have recently changed: For example, the requirement of using a letter, a number, an uppercase, and a special character isn't useful, and neither is the recommendation of changing your password every 90 days, according to Bill Burr, who published past password standards. Instead, long, easy-to-remember phrases make the best passwords, Burr said. It is also recommended that users only be required to change their password if a breach has been suspected or confirmed. Some employers are turning to biometric passwords such as fingerprints to enhance cybersecurity, the report found. These have generally been welcomed by employees: 77% said they trust biometric passwords, and 62% said they believe they are stronger than traditional alphanumeric codes, according to

the survey. However, at this point, only about half of employees (55%) use biometric passwords.