ARTISANS' BANK
SAFETY + SECURITY
SHARED MONTHLY NEWSLETTER

HARD PASS ON WEAK PASSWORDS

MAY 2024

A strong password or passphrase is the first line of defense to protect your data. When you create a strong, unique password, you keep your information secure. With this month's newsletter, take time to educate and remind yourself of the importance of creating and keeping a secure password for your accounts.

Poorly chosen and badly protected passwords are still one the most common reasons for data breaches. And these days, hackers don't have to guess your weak password: they can purchase it from password stealers, who get the passwords from other social engineering attacks.(1)

28% of people reuse passwords for multiple work-related devices(2)

If important accounts are protected with the same password, a data breach that leaks that password damages them all. Using a unique password for each account reduces this risk.

51% of individuals share business account passwords with colleagues (2)

Sharing passwords is never good practice, even if you trust someone. It opens the door for many different forms of attack. Sharing passwords can be very damaging to your personal and organizational data.

103+ million people used "123456" as a password (3)

Common passwords are easy to break. Also avoid using personal information in your password. It's easier than ever to find details about you online, and those bits of information could be put together to guess your password.

1 second is all it takes to crack the most common password (3)

Your password is the first line of defense against an unauthorized user accessing your account. Creating a strong password is essential. You want to create something that is easy for you to remember but difficult for someone else to guess. Use a variety of letters, numbers and characters. Consider creating a passphrase, such as ie@tic3cream4br3akfas!

How passwords get hacked: Hackers use a variety of different ways to hack passwords. As technology improves, hackers have found different methods of breaking and entering.

Dictionary attack: The computer generates every word possible as a password until it finds the right word. Using a solid passphrase can stop this type of attack

Brute-force attack: This attack finds all possible password combinations possible. Having an account that blocks multiple missed password attempts can stop this type of attack.

Credential stuffing: Once a hacker has access to someone's password, they try that password with other accounts. Having a different password for each account is key to stopping this type of attack.

1 2023 Verizon Data Breach Investigation, 2 2023 Proofpoint State of the Phish, 3 NordPass Most Common Password List 2021