BANC OF CALIFORNIA | TOGETHER WE WIN®

YOU CAN BANC ON IT

QUESTIONS WE NEVER ASK

STRONG PASSWORDS ARE CRITICAL TO YOUR BUSINESS'S SECURITY

Weak passwords and bad habits invite hackers and scammers to come in and browse around your business.

You might think that cybersecurity starts with the latest technology to identify malware threats and find weaknesses in your enterprise network. While that might be a component of your strategy, most businesses would be wise to start with perhaps the simplest, yet most important, part of scam prevention strategy: creating stronger passwords company-wide.

Protect your business by strengthening all employee passwords (even your own).

Improving your password policy to create better passwords isn't just a good idea–it's an absolute and immediate necessity. Businesses need to help their employees create stronger passwords, change them often, remember them and break old habits.

How to create better a password.

- Make every password at least 15 characters. Experts say this is the best thing you can do. Hackers prefer simple and easy, so make your password longer and more difficult to hack.
- Mix up the characters. Password prompts ask you to use at least one uppercase and one lowercase letter, a number, etc. Do more of that with your 15 characters and don't repeat a pattern.
- Be creative. A password doesn't have to be boring and look like a password. It can be the name of the kid who sat next to you in third grade. Or take a favorite quote from a book, movie or song and use only the first letter of each word, and the year it came out. (Important: Just don't use anything you've shared online.)
- Make it memorable. Create a long, goofy sentence that means something to you and mix in numbers and symbols.
- Change your password every three months. Most people don't want to go to the trouble of changing passwords. They're the kinds of people hackers love most.
- Keep passwords in a safe place. Yes, complex passwords are harder to remember, so you need to store them in a safe place, memorize them or use a password manager (more on that below).

It's time to break old password habits.

- Don't use the same password on different accounts. Yes, it makes it easy to remember, but it also makes it easy for a hacker to break into multiple accounts.
- Don't make a simple tweak to update your password. Changing "HotDogs2021" to "HotDogs2022" isn't much of an update.

Passwords don't have to be boring to be strong. The secret is to make them memorable to you, while also making them hard to guess by anyone. By following tips that experts suggest, you can boost your password security quickly.

SPOT THE RED FLAGS. AVOID A SCAM.

- Don't be obvious. Including your pet's name, your anniversary or your favorite team in your password makes it much more guessable.
- Never use obvious sequences. Do not include "1234" or "abcd" or "qwerty" in a password. That gives a hacker a running start because they try those first.
- Don't substitute letters for numbers. It may seem creative to use a zero (0) instead of an "O," but you're not going to a fool a hacker who uses programs and tools to break codes all day long. "P#ssW0rd3" isn't that complex for a hacker to guess.

Weak passwords can cause serious problems.

It's a fact that millions of stolen passwords are available in databases for criminals to leverage in cyberattacks. If those passwords haven't been changed in the past few months (or even years), it could be only a matter of time before a hacker uses one of them to breach another network.

The story of the SolarWinds security breach is the best example of that. It has been described as the largest and most sophisticated attack the world has even seen. In the end, after the breach was finally discovered, more than one hundred U.S. businesses and government agencies had been hacked.

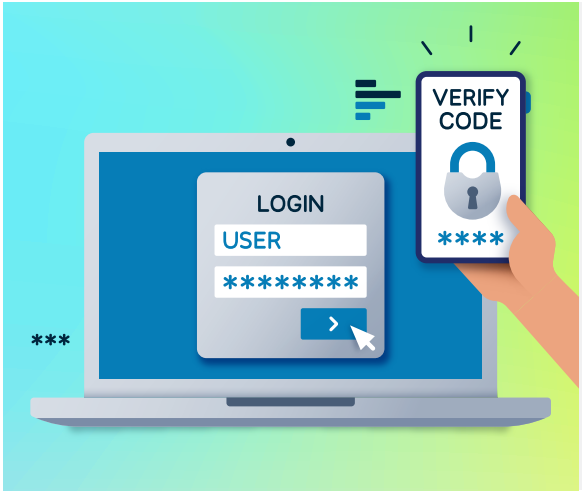
There's strong indication that the hackers gained their initial entry through a simple password that a SolarWinds intern had used—"solarwinds123." That should be enough to keep any business owner awake at night.

When was the last time you reviewed your password policy?

All businesses should revisit their password policy to see where it might need improvement. Even a simple reminder of "common sense" practices could help prevent a problem. Employees should be aware of the following rules:

1. Never share a company password with another employee.
2. Never divulge a company password to someone outside the company.
3. Work-related passwords should not be identical or similar to another password used online.
4. Never post a password online.
5. Never post your network password on a sticky note.

Additionally, businesses should explore the available software programs that require employees to change their passwords at least quarterly. There are also password manager programs for businesses as well as individuals. These programs could be an all-in-one solution for a company. Not only do they help to create unique passwords, but they also encrypt and store all passwords in a secure location.



The hack stops here.

The good news is that a plan to improve passwords company-wide can be put into place quickly. An email to employees and/or a staff meeting on password safety can get this important news out quickly.

Regular employees as well as busy executives can easily fall into bad password habits. That's probably what happened to Mark Zuckerberg, Facebook/Meta founder. His social media accounts were breached a few years ago when a hacker discovered his simple password: "Dadada." Fortunately, the hacker had a sense of humor and simply reported his discovery on social media.

Most of the time, however, a stolen password doesn't end up being a funny story.

To read more Business Insights articles, please visit: **bancofcal.com/business-insights**

BANC OF CALIFORNIA | TOGETHER WE WIN®