BANC OF CALIFORNIA | TOGETHER WE WIN®

YOU CAN BANC ON IT

QUESTIONS WE NEVER ASK

TWO-FACTOR AUTHENTICATION PREVENTS HACKERS FROM LOGGING IN TO YOUR NETWORK

Even if a hacker knows a username and password, “2FA” will help to block them out.

Sometimes, a technical-sounding term like “two-factor authentication” can put you off, making you not want to take the time to learn about it. This, however, is too important to be one of those times. **What two-factor authentication (“2FA”) means is this:**

1. It slows down the login process to make sure the person logging in is who they claim to be.
2. The process essentially says, “Your login credentials (one factor) aren’t enough. You need to provide another piece of information (a second factor) before you’re allowed in.”

Often also referred to as two-step verification or multifactor authorization, this simple process helps reduce unauthorized access and outside cyberattacks from infiltrating your network. It is an **extra layer of protection** for you, your employees and your business for logging in to your network, email or bank accounts… because by implementing 2FA, a hacker can’t get into your network even if they know the username AND password! The extra step required to log in will block them out.

The obvious question is why are so many businesses still not using a form of two-factor authentication? Does your business?

A digital bouncer.

Think of 2FA as a digital “bouncer” for your business network that won’t let someone in until they present a second piece of information that validates their right to enter. If they can’t, they don’t get in.

This is extra protection every business should have because cyberattacks take place every day and aren’t going away anytime soon:

- It’s estimated that 81% of data breaches involve weak passwords
- Statistics indicate that 90% of phishing attacks involve the theft of login credentials: usernames and passwords
- Even with the best encouragement and information, employees continue to use weak passwords or repeat passwords they use on other accounts

Virtually all financial institutions, credit card providers and social media apps offer this extra layer of protection.

2FA to the rescue.

Here’s how two-factor authentication works, in its simplest form, once you’ve set it up (“enabled it”) on an account:

- You go to an account to log in, entering your username and password

Two-factor authentication virtually eliminates the risks associated with compromised passwords. Even if someone knows or hacks your password, the extra step needed to verify the user for login, which is sent to you only, will block them.

SPOT THE RED FLAGS. AVOID A SCAM.

- The website says you need a second code to complete the login and asks how you want to receive it–it's often via text message (SMS) sent to the phone number already linked to the account
- When you click to receive the secret code, it's sent immediately to your phone
- You enter the code you receive and complete the login process

In technical jargon, that second number you need is called a "token code." Since it comes to you just one time, it's also referred to as an OTP, for "one-time passcode."

There are other forms of two-factor authentication, such as a fingerprint or a digital "face ID" check before a user can log in, which is what Apple Pay requires to complete a transaction. That extra step takes just a second and helps prevent fraud.

The biggest decision isn't necessarily which method of verification to choose, but when to do it.

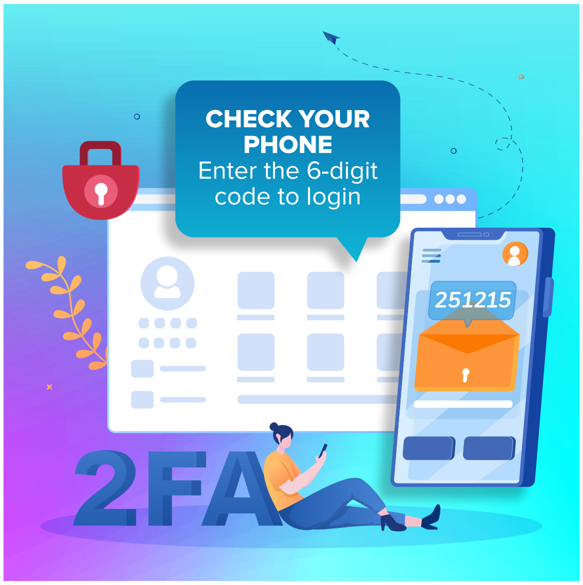
Two-factor authentication is a must!

Virtually every security expert suggests that businesses use a form of multifactor authentication to bolster their company's login procedures. Putting up that extra-secure digital fence around your network prevents the easy access that could happen otherwise.

Banc of California covered this topic in an article titled Building a Culture of Cyber Readiness, where it stressed the importance of knowing who has access to your networks and implementing multifactor authentication for all users.

If your business is not currently using this tool, it's important to correct that situation as soon as possible. The time to start putting that extra layer of protection around your accounts and your networks is now.

You can explore the various options, and it might help to get some advice from your IT department or a trustworthy technical advisor, if you have one. The good news? As identity verification becomes more complex, it also provides a greater measure of security.



Easy for employees and difficult for attackers.

By using a 2FA solution, businesses can move beyond the worries of password strength and management and instead concentrate on growth and success. Requiring that extra step to complete the login process might be a minor inconvenience for you and your employees, but it will help to stop attackers from getting into your network with hacked or stolen passwords.

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

BANC OF CALIFORNIA | **TOGETHER WE WIN®**