WHY YOU NEED Two-Factor Authentication

Your Business Really, Really, Really Needs Two-Factor Authentication

When is the last time you saw a jewelry shop protect their diamonds with a simple lock and key? Even before extra layers of security like alarms, motion detectors, and biometrics were invented, jewelers hid their diamonds and even put out fakes to deter criminals.

In your company, data is as valuable as those diamonds — so why are you protecting it with a simple username and password?

Adding Two-Factor Authentication (2FA), or Multi-Factor Authentication (MFA), increases additional security and gives more assurance to prevent hackers entering your account. All made possible through your mobile phone.

Most breaches happen not because of sophisticated cybercriminals burrowing into companies in complex ways, but rather because of lost or stolen employee credentials.

How does it work?

Two-factor authentication stops easy access with stolen credentials by requiring a second level of authentication after the user enters their username and password. Since a password is something that a user knows, ensuring that the user also needs to have something else to log in thwarts attackers.

There are a variety of ways this second factor of authentication can be delivered, including texts to your phone, biometrics like your fingerprint, or random codes generated by an app.

In effect, two-factor means you will be notified any time hackers try to log in no matter how they stole your credentials so you can take immediate steps to protect yourself from any further damage.

But why does my business need 2FA?

Breaches are no longer a technology issue. They're a core business issue. According to a survey of 200 corporate directors, more than two in five respondents said that CEOs should face the brunt of any breach-related backlash.

Simply by requiring a second form of identification, there is a low probability that a hacker can successfully impersonate an employee and gain access to your systems. If an employee loses a mobile device or a password is stolen, 2FA provides enough time for your company to remedy the issue before too much damage is done.

At least 35-40% of help desk calls are related to password resets, which require an average of 20 minutes of the help desk technician's time to complete.

Key benefits

- Improved business security
- Increased productivity
- Lower security management costs
- Reduced fraud
- Simplified password policies
- No IT training required
- Seamless integration
- Prevent security breaches

Depending on the vulnerability of the data stored in the profile you're trying to access, the 2FA may trust your device for 30 days or a year. Some services give users an opportunity to manage settings of a secret code: you can allow a service to trust your current device or not.

In 2018 the number of identity fraud victims increased by 8% (rising to 16.7 million U.S. consumers).

Today's employees and consumers are used to having the information and resources they need at their fingertips. This level of digital convenience offers huge potential for businesses, while introducing new security risks and vulnerabilities. Two-Factor Authentication provides the stronger user validation that today's enterprises require.