WE DEFINE IT

MULTI-FACTOR AUTHENTICATION FREQUENTLY ASKED QUESTIONS

Data security has to be a core consideration of the modern business, so every small effort you can take to protect your business is important. One such effort is the implementation of two-factor authentication. However, your employees may not initially feel entirely comfortable with some facets of two-factor authentication.

The two-factor authentication platform, adds a valuable layer of security to your existing solutions by requiring an additional credential beyond just your typical username and password. This can be a PIN that is generated by an application or even a physical token like a key fob that provides access.

To make a long story short, your employees may not feel entirely comfortable with your organization requiring them to keep an application on their phone as they may value the autonomy they have over what they do and don't keep on their personal device. As a result, they are bound to have questions that you will need to answer.

To assist you with this, we've compiled a few questions you may have to field, and how to answer them truthfully and diplomatically if you choose to implement two-factor authentication for your business.

WHAT IS IT?

Multi-factor authentication is another way to improve data security and prevent threats from infiltrating business network's access points. Picture your network as a house that your data lives in, with the front door being the access point. The lock that you find in the doorknob is your usual access credentials, username and password. Multi-Factor (or 2FA) adds a deadbolt to that door.

In other words, multi-factor authentication is the added security that can keep many threats out, at the cost of a tiny bit of convenience.

WHY DO I HAVE TO DO THIS?

This line of questioning is indicative that an employee is resistant to change--unfortunately, information technology is built on change. Threats to a business' security are always improving so they have the best chance of creating the most impact. To counter this, a business must acknowledge the risks inherent in powerful technology platforms and do everything they can to control access to their network. Multi-factor authentication is just one of many ways to do that.

It is also important to remember that a chain is only as strong as its weakest link, so the entire business could be made vulnerable if one person doesn't have the same dedication to organizational network security as the rest of the team. By implementing multi-factor authentication as a team, the business is better protected by the team.

WHY DO I HAVE TO DO IT ON MY PERSONAL PHONE?

This answer has two parts to it, one being of best interest to the business, the other being for the employee's benefit. First off, economics. Does your business have the capital to spare to distribute mobile devices for the singular purpose of enacting multi-factor authentication?

Typically, this isn't the case.

Which device is an employee more likely to favor? Their personal device that they have conditioned themselves into bringing everywhere, or the new, unfamiliar device they were just given for work?

WHAT HAPPENS IF I LOSE OR FORGET MY PHONE?

There are ways to get around a forgotten or misplaced device. In many cases, an organization can adjust an employee's multi-factor authentication settings to allow them access via a new 2FA code, but this will require the employee to change their credentials. If the phone is lost, the company is still safe, as the Mobile Device Management platform that the 2FA implementation was likely part of will allow network administrators the requisite authority to handle the situation.

CAN YOU SEE MY PERSONAL STUFF?

This question will likely come up. You should ensure your employees that the privacy of their personal data will not be betrayed, and that the authenticator will only be used to access their company materials.

Information can be a touchy subject, and its security is of paramount importance. Reach out to us at 888-234-WDIT (9348) for more help with your company's data security.

WE DEFINE IT

Don't wait any longer.

Get started today!

wedefineit.com
getproactive@wedefineit.com
888-234-WDIT (9348)