Two-Factor Authentication: What is it and why does my business need it?

What is Two Factor Authentication?

Two factor authentication is a multi factor authentication verification process to verify that the identity of the user is authentic. It is generally achieved by receiving a secondary randomly generated code after inputting the password, generally through an app or a text message. Two factor authentication is far more secure than only using a password. Because the code is randomly generated for each login attempt, there is no way for the fraudster to gain access without the code generated on the device.

Why do businesses need it?

With companies becoming more and more connected to the internet, the threat of data breaches and hacking is becoming a much more prominent threat. With the rapid expansion in technology, and the growing cyber security threats that exist for **firms/**companies, there is a way to protect yourself against unwanted external access to accounts. One of the main areas in technology that enables the unwanted access by third parties to data is passwords. Passwords are meant to be strong enough for others to not be able to guess them, but also easy enough to remember that the user is still able to access the account. Companies have the ability to spend tens if not hundreds of thousands of dollars on complex firewalls and data protection, but the reality is once hackers get access to passwords, the systems become virtually meaningless.

The typical validation method when logging into an account is by single factor authentication in the form of a password. According to Microsoft, on any given day an enterprise worker may have to remember up to 6 different passwords; to simplify their work and personal life, these users often reuse passwords across different platforms. The issue with this is that once a hacker has access to one of these passwords, they have the ability to access all of the other accounts that share the same password and credentials.

According to *Identity Theft Resource Center,* in 2018 alone there was 2.7 billion records stolen or exposed globally. This included the passwords and usernames of millions of users.

The Benefits of Two-Factor Authentication

Two Factor authentication provides a wide range of benefits for businesses, including:

Improved Security: two factor authentication decreases the likelihood of an attacker gaining access to a users account. Even if the hacker has the username and password, they will not be able to access the account, due to the need of providing a second form of authentication in the form of a randomly generated code.

Increased Productivity and Flexibility: because users can now be more mobile and flexible due to the added layer of security. Workers can access corporate data securely, and the business owners can have peace of mind knowing that the corporate network, as well as sensitive data, is not at risk.

Reduce fraud: Because there is secondary security on logging into accounts, there is peace of mind knowing that your identity and data is more protected than single factor authentication alone.

Reduce harmful effects of human error: Even with an advanced and secure backend, all firms/business possess a critical security vulnerability: Human nature. Two factor authentication provides business/firms with the ability to further safeguard their data, and reduce the ability for human error to play a role in data breaches and hacks.

Getting Started: If you are a current i-worx client, implementing two factor authentication is fast and easy, and provides your firm with the highest possible level of security, at a reasonable monthly fee. Contact us today to learn more.