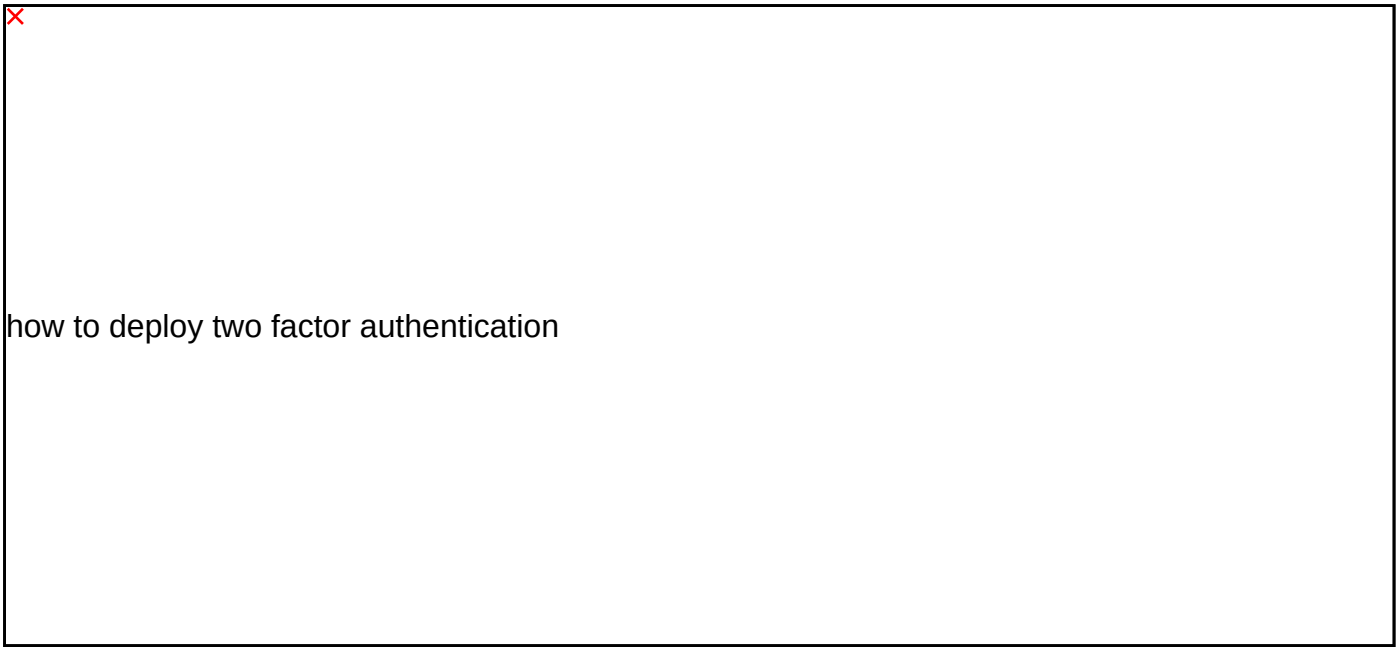
Deploying Two-Factor Authentication!

Posted At : November 20, 2019 2:59 PM | Posted By : Admin
Related Categories: Your Business, Security



Put those passwords in their place!

Cybercrime is constantly on the rise. It seems like every quarter there is a new breach of a major website, with hackers stealing the online credentials of hundreds of thousands to millions of unwitting users, including small businesses. A **Poneman Institute** study showed that the average cost of a data breach increased from $7.91 million in 2018 to $8.19 million in 2019 which is the highest cost globally.

Passwords offer one level of protection. But for a deeper level of protection, you also need two-factor authentication.

Two-factor authentication is a subset of multifactor authentication, which features two or more types of authentication. It's like getting married and having something old, new, borrowed and blue. With two-factor authentication you need something you know (a password), something you have (a code or hardware device) and/or something you have (like a biometric sign-on such as fingerprint or retinal scan).

The beauty of two-factor is that while a hacker might be able to figure out your password (they're notoriously good at that), they'll likely struggle cracking the second layer of protection because codes are set on-the-fly (they're constantly changing) and your biometrics are difficult to replicate.

The simplest way to set up two-factor authentication is to implement an authenticator app like Google Authenticator, Microsoft Authenticator, Authy and others.

Google Authenticator is a free smartphone app from Google that is available for Android and iOS. To use it, you must first enable two-factor authentication on your online services. The service will then ask the user to take a photo of a QR code it provides. Upon reading the code, Google Authenticator will randomly generate codes to serve as the second authentication. The codes provided by authenticator apps sync across your accounts.

Microsoft Authenticator is another free authenticator app that works very much like Google's – using QR codes – and supports Android, iOS and Windows 10 Mobile.

Meanwhile **Twilio's Authy** is an authenticator app that supports Android, IOS, Windows and Mac laptops, and the Chrome browser. Authy does not require users to take photos of QR codes, but instead stores users' authentication codes encrypted on the Twilio cloud servers and decrypts them when the user inputs their passcode.

Authy is free to starter accounts that use fewer than 100 authentications per month. There is a pay-as-you-go option that costs $.09 per authentication.

LastPass offers another variation of an authenticator. The free service enables one-tap push notifications that allow users to log in to sites on PCs with a click instead of entering codes. However, to use one-tap notifications you must have the LastPass extension installed in your browser and enabled.

Authenticator apps tend to make it easy on the user by not requiring specialized software development or IT pro assistance in setting up an effective two-factor authentication solution. They are good for small businesses that have 10 or fewer employees – particularly because 10 employees tend to be the cutoff for free access to many of the different commercial options.

Employees also often stand as the path of least resistance for hackers. One lax move by a careless worker can mean a substantial hit for your business and bottom line. This is why it might be more practical to simply use one of the many solutions that take care of the entire two-factor authentication process for you.

Cisco's Duo Security unit offers a cloud-based two-factor authentication service suitable for small businesses and enterprises alike that automates the entire authentication process. Duo's user experience only requires one tap on a smartphone to verify users are who they say they are. The service is free for teams of 10 or fewer. For multifactor authentication, Duo, costs $3 per user per month.

Meanwhile, **IBM Cloud Identity** provides multifactor authentication and other security services. Starting at $2.50 per employee per month, it comes with thousands of pre-built connectors to help you quickly provide access to popular apps; and pre-built templates to help integrate in-house apps. There is also a **free version**.

And Nexmo, a Vonage business unit, employs its **Verify** solution to provide hassle-free automated two-factor authentication. All you have to do is provide a phone number and Nexmo will take care of everything else and begin sending codes via SMS to verify that users are who they should be.

Two-phase authentication adds a much-needed level of security to your data, so that even if a big bad hacker gets your password in the clear they will not be able to do the kind of financial and reputational damage to your business because you added that second step of authentication. For at most a small monthly fee, you can help to ensure your business is not racking up losses due to cybercrime breaches.