双因素认证是一种采用时间同步技术的系统，采用了基于时间、事件和密钥三变量而产生的一次性密码来代替传统的静态密码。
简单来说，双因素身份认证就是通过你所知道再加上你所能拥有的这二个要素组合到一起才能发挥作用的身份认证系统。例如，在ATM上取款的银行卡就是一个双因素认证机制的例子，需要知道取款密码和银行卡这二个要素结合才能使用。
双要素身份验证通过要求额外的登录凭据，为您的在线帐户和数字设备提供了额外的安全保护。

双因素身份验证可以帮助保护您的企业帐户和数据免遭未经授权的访问

- 与仅使用密码的登录相比，两要素身份验证（2FA）提供了更高的帐户和设备安全性。
- 您的企业可以实现几种不同类型的多因素身份验证（MFA），包括PIN，一次性身份验证代码以及面部或语音识别。
- 为您的企业设置2FA时，请考虑可以包括哪些帐户，所需的系统要求以及最适合您的企业的身份验证因素。

对于大多数企业而言，大量敏感的财务和客户数据在线存储在其数字帐户和基于云的帐户中。这些数据的价值使小型企业成为数据泄露和勒索软件攻击的主要目标。Verizon
2020年的一项研究发现，在报告的所有数据泄露事件中，近30％涉及小型企业。

大多数用户认为他们的密码将使他们的帐户安全。但是，较弱的密码极易受到攻击，很容易被黑客入侵。而且，如果您是一个难以记住其密码的人，那么与网络犯罪分子相比，您更有可能保持自己的身份。

这就是引入两因素身份验证（2FA）的地方。此技术为每次登录增加了一层额外的安全性，以使您的数据和设备比纯密码登录更安全。此外，企业可以通过正确的2FA解决方案轻松地在现有网络中进行集成和管理。

如果您想提高系统的安全性，以下是2FA的工作原理，存在的各种因素以及如何将其用作解决方案以保护您的业务的摘要。

什么是双因素身份验证？

单因素身份验证涉及仅使用您的用户名和密码登录帐户或设备。双要素身份验证通过要求额外的登录凭据，为您的在线帐户和数字设备提供了额外的安全保护。

“因素”是指用来验证您的身份以便成功登录您尝试访问的帐户或设备的任何方式。使用2FA，帐户或设备会要求您输入第二个因素来证明您的身份，通常只有您才能访问。在输入密码后成功输入第二个因素，将授予您访问帐户或设备的权限。

双因素身份验证如何工作？

使用两因素身份验证，即使有人窃取了您的密码，他们也不太可能获得第二个标识符，因为这些因素往往只能通过您的其他设备之一或您自己产生。这使2FA比传统的密码登录更为安全，并且使用户和组织更具灵活性。

用户输入用户名和密码后，两步身份验证会要求提供其他信息。系统通常会要求三类第二因素：您所知道的东西，例如个人识别码（PIN）或安全问题的答案；您拥有的东西，例如发送给第三方设备或应用程序的一次性授权码；或涉及身体自我的事物，例如面部，指纹或语音识别。

使用2FA保护帐户或设备通常涉及使用2FA系统设置该帐户或设备。根据身份验证方式的不同，您可能需要配置安全问题，输入移动设备编号，向第三方应用程序注册或输入生物特征数据（通常仅在诸如iPhone的FaceID或指纹之类的移动平台上）才能成功设置您的多因素身份验证。

关键要点：
使用2FA，用户的帐户或设备将询问其他身份因素，例如安全性问题答案，身份验证码或生物特征数据。这使它比纯密码登录更加安全，因为用户通常是唯一可以提供第二个“因素”的人。

为什么双重身份验证很重要？

随着COVID-19大流行导致未来更多组织采用混合或远程工作人员，两要素身份验证是一种确保办公室内和远程工作人员同等安全的重要方法。

Fastest Labs首席执行官兼联合创始人Dave Claflin表示：“在2021年及以后的时间里，技术将继续（在工作场所中）发挥更大的作用，随之而来的是，需要保护更多的信息免受网络攻击。” 药物和DNA测试服务。 “当我们的加盟商在办公室工作

时，为他们的社区管理药物和DNA测试，测试结果和信息将以数字方式发送……并包含高度机密的信息，这些信息将被发送给雇主或个人。”

拥有2FA系统是确保您的业务和客户数据安全的最佳方法。网络攻击将继续变得更加复杂和有针对性，甚至小型数据泄露也可能破坏一家缺乏从攻击中恢复的资源的小型企业。

使用2FA，即使黑客拥有用户名和密码，他们也无法在没有其他身份验证因素的情况下访问用户的信息。当组织中的每个用户都使用相同的2FA解决方案时，黑客很难访问其网络。这不仅可以保护企业的员工，还可以保护与其合作的供应商，合作伙伴和客户。

关键要点：
随着网络攻击变得更具针对性和复杂性，即使网络犯罪分子获得了用户名和密码的访问权，2FA仍可帮助保护帐户免遭黑客攻击。

双因素身份验证的类型

组织可以使用许多不同类型的2FA因子。这些通常由用户将访问哪些设备或应用程序以及组织本身可以提供的内容来确定。以下是与2FA一起使用的五种常见因素：

1.短信/短信

最常见，最直接的身份验证因素之一是通过SMS或短信将登录代码发送到您的手机或移动设备。输入用户名和密码后，身份验证码将发送到您用您的帐户注册的移动设备，并且在收到密码后会提示您输入。

SMS消息代码确实存在一些安全风险，因为老练的黑客可能能够劫持移动设备以获取未经授权的帐户访问权限。因此，除非员工使用公司发行的安全移动设备，否则组织可能希望避免SMS身份验证。

2.认证申请

身份验证应用程序的工作方式类似于短信代码。登录后，它不会通过短信发送代码，而是通过经过认证的身份验证应用程序（例如Google Authenticator）生成对时间敏感的代码。如果用户遇到数据连接问题并且无法立即访问该应用程序，则这些应用程序中的许多应用程序还会提供备份代码。

使用这种形式的身份验证时，用户可以将其设备设置为从应用程序接收推送通知，告知他们验证码。这消除了网络钓鱼和网络渗透，但是如果用户的互联网连接不完整，则可能变得不可靠。

3.生物特征认证

生物特征认证要求用户提供自己的物理属性才能访问其帐户。最常见的因素往往是一个人的声音，面部或指纹。尽管这几乎是其他人无法复制的，但是此方法存在局限性。如果由于设备或校准问题而导致您正在使用其帐户访问的设备无法正确验证您的语音，面部，指纹或其他生物特征数据，那么您将无法访问它。

4.硬件令牌

硬件令牌是类似钥匙串的表链，每30秒产生一个数字代码。用户输入登录信息后，他们查看设备并输入令牌上的代码。由于这些单位的成本，对于大型组织而言，这可能是成本过高的。但是，除非有人偷了实物密钥卡，否则这是极其安全的，并且不可能被黑客入侵。

5.软件令牌

软件令牌是企业最流行的2FA形式之一。像硬件令牌一样，用户下载组织批准的软件程序，该程序会为该帐户生成一个随机的登录代码。这些令牌仅在30秒到1分钟之间的有限时间内显示代码。

关键要点：
在2FA保护方面，企业有多种选择，包括SMS代码，身份验证应用程序，生物特征认证以及硬件或软件令牌。

双因素身份验证解决方案可保护您的业务

许多常用的业务应用程序（例如Google Workspace，Dropbox，Salesforce，Slack，PayPal和社交媒体网站）已经可以选择设置两因素身份验证。如果您现在使用用户名和密码登录，则可以进入设置并在登录选项中添加两因素验证。从那里，您可以编辑将用作凭证的因素，以及需要2FA的设备。

要在所有业务帐户（甚至是本机不提供的帐户）中设置2FA，您可能需要考虑使用一个专用系统，该系统允许您通过单点登录（SSO）或身份访问管理来配置多因素

身份验证（ IAM ）门户。一些最适合企业的单点登录解决方案包括OneLogin，LastPass，Okta，Google Cloud和JumpCloud。

关键要点：
您可以在每个平台（如果有）中本机为企业帐户设置2FA，也可以通过单个登录或身份访问管理门户设置。

为您的业务设置2FA

以下是为您的企业设置2FA的方法：

1.确定要通过2FA保护的帐户。

设置2FA的第一步是确定需要保护哪些组织帐户。如果您要投资SSO或IAM解决方案，则可以使用多因素身份验证来保护所有连接的业务帐户。如果不是这样，则最好在允许您执行此操作的任何平台上本地实施双重身份验证。这可能包括电子邮件，消息服务，库存，财务软件和云存储帐户之类的应用程序。

2.如有必要，升级操作系统。

在研究要使用的2FA解决方案时，请确保您具有支持它的操作系统和基础结构。您要用于因素的系统中的所有设备都必须在同一操作系统上运行以保持一致性。

此外，某些2FA解决方案可能会要求您安装其他应用程序或软件。它们通常需要在设备或Web浏览器的最新操作系统上运行，因此请确保所有设备都是最新的。

3.确定哪个因素最适合您的组织。

您的企业中的每个用户登录2FA系统时都应使用相同的通用因子。使用相同的通用因素使组织中的每个人以及需要确定登录问题的IT支持人员都更加容易。

Fracture的高级IT运营经理Steve Panaghi说：“让员工易于使用至关重要。“如果您的[2FA]解决方案难以使用，则员工将不会使用它。”

简而言之，请使用对您的业务有意义的身份验证因素。例如，如果用户使用不支持生物识别解决方案的设备登录，则不要将面部，指纹或语音识别用作第二个身份验证因素。