SIMPLE, SAFE AND SECURE:

HOW 2FA PROTECTS YOUR BUSINESS FROM CYBER CRIMINALS

sendQuick®
By TalariaX

Whitepaper on Two-Factor Authentication

TABLE OF CONTENTS

“

IT TAKES 20 YEARS TO BUILD A REPUTATION AND FEW MINUTES OF CYBER-INCIDENT TO RUIN IT.

STEPHANE NAPPO

Advances in technology have enabled business to adopt a relatively mobile workforce. Employees are now able to log into their online portal to access data and communicate with their management and each other anywhere in the world.

Such levels of convenience through remote access also imposes increased levels of risk for your business. Increased workforce mobility exposes you and your company to cybercrime, and it is now important for you to ensure security for those trying to access your systems, networks and data.

Failure to protect your privacy makes you a huge target for criminals.While most companies still rely on password protection, they're too easily breached. According to TeleSign, 73% of the population reuse and recycle their passwords, therefore reducing their effectiveness and reliability against cyber-attacks.

Moreover, password protection normally is effective in only slowing down a cybercriminal's attempt to grab proprietary data and system access.

Simply put – password protection does not work in protecting you, your staff and your customers from data theft.

Two-factor authentication provides a robust defence than a simple query password system.

This paper discusses how two-factor authentication can make all the difference in foiling today's technologically savvy cybercriminals.

Brick-and-mortar offices are fast becoming a thing of the past, whether we like it or not. A virtual office springs into existence each time an employee logs in with their laptop and their mobile devices, and remote accessibility is fast becoming important for the employee's day-to-day needs.

More workers are now enjoying the flexibility and convenience of working from home, a hotel, an airplane, or even from a coffee shop. They can access their personal virtual office at any time from any location.

This improvement in office mobility has benefited employees with work arrangements that offer greater flexibility and convenience. The companies that employ the mobile workforce have also benefited from increases in productivity and a reduction in operational costs.

In many cases, mobility has enabled companies to keep a pool of talented workers ready and able to work on demand as needed, slashing costs during times when those workers aren't required.

There is, however, a dark cloud with that silver lining. Cybercriminals have done an outstanding job of keeping up with the technological advances that have enabled mobility. This means that backwards companies that still rely upon ancient pre-mobility security methodologies are prime prey for cybercriminals.

Perhaps the most outdated methods of security methodologies is the reliance upon a single password to prevent unauthorized entry into a system. Single-factor authentication is a security methodology that cybercriminals love, because they've found it so easy to break past that flimsy barrier. Phishing attacks, malware infections, keylogging and brute force attacks are just some of the tried and true methodologies used to illicitly harvest passwords by the millions every year.

Therefore, it is a simple and indisputable fact that with every single login attempt, the receipt of the correct password does not confirm that the user is a valid user.

The good news is, there’s still a way to confirm that users logging into a system are who they claim to be. Adding a second level of authentication, generated in real time and sent directly to the user’s phone, eliminates fraudulent attempts at gaining access to systems and data. Two-factor authentication is the key to realizing the benefits of mobility, while retaining the integrity of systems and data security.

According to CNET, many of the world's best-known technology companies — Google, Twitter, Facebook, Microsoft, Amazon, Apple and many others — now enjoy the enhanced security provided by a two-factor solution. Maximizing the potential of a two-factor authentication methodology, however, requires the installation of a system that delivers a full range of capabilities. The following should be considered must-have features for two factor solutions undergoing evaluation for deployment in any organization:

1. Easy Deployment: Difficulty in deployment sometimes prevent organizations from implementing a two-factor solution. Many of these solutions require the issuance of physical tokens — potentially to tens of thousands of users. Some solutions require the embedding of cryptographic keys within code, or the scanning and storage of biometric data such as fingerprints.

Two-factor solutions that impose requirements such as these can require massive effort and expense just to implement. They also tend to require user participation during the deployment process that is likely to be highly disruptive and, for a time, counterproductive. The ideal two-factor solution for most organizations demands no user participation to implement, requires little or no modification of existing code, and is a self-contained solution that does not rely upon physical tokens.

TalariaX's ConeXa provides a simple solution that strengthens authorization security. It is an all-in-one, single-box appliance that supports two-factor login authorization and authentication. This enables quick and easy plug-and-play implementation.

2. Low Implementation Cost:

Just as with solutions that are difficult to deploy, solutions that are exorbitantly expensive to implement present a significant stumbling block.

Many of the difficult and complex deployment requirements noted above tend to drive implementation costs to budget-busting levels. However, two-factor solutions are available that keep both the difficulty and cost of implementation quite low.

Ordinary two-factor security solutions are expensive, disruptive and time consuming. ConeXa's SMS messaging platform, however, eliminates the need for the distribution of physical token, helping your business save time and money.

3. Easy Integration:

Integrating a two-factor system with existing hardware, software and systems can be nightmarishly difficult. It doesn't always have to be like this, however. Organizations that carefully choose the right two-factor solution can expect easy integration with Active Directory, RADIUS and local/external databases.

4. Comprehensive SMS Alerting Capability:

The two-factor solution should have the capability of sending all types of alerts using SMS text, including customizable user messaging.

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word “workplace” must be redefined to be less location-specific and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones and other devices has transformed many enterprise roles into any place, any time propositions. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps in productivity that remote access enables.

This ongoing paradigm shift has required, however, that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of virtual public networks (VPNs) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justify the need for an increased focus upon security.

TalariaX's sendQuick ConeXa two-factor authentication solution has demonstrated the ability to consistently provide effective and consistent protection against data theft from cybercriminals.

TalariaX sendQuick ConeXa gives organizations worldwide the ability to easily and costeffectively implement two-factor authentication. TalariaX's two-factor authentication solution combines a crucial additional layer of security with a user-friendly and administration-friendly methodology. Second-factor authentication is enabled by sending the user a one-time password (OTP), generated in real-time after the user has entered the domain password.

Key features of sendQuick's ConeXa include:

Identity Protection: TalariaX's SMS notification is sent directly to the user's phone.

TalariaX sendQuick ConeXa uses an integrated SMS server that generates a one-time password for two-factor authentication that neither compromises the user's identity, nor places access to systems or data in the wrong hands.

Improved Network and Data Security:

TalariaX sendQuick ConeXa offers an effective, efficient methodology for restricting access to proprietary systems and data. Only authorized personnel will be able to receive the one-time password sent directly to users' phones via SMS messaging. And the short shelf life of the OTP — expiration time can be adjusted per client's preference — adds an additional layer of security that further reduces the likelihood of an unauthorized login.

SMS One-Time Passwords: SMS messaging is the most convenient, cost-effective method for the delivery of one-time passwords.

SMS-based password distribution eliminates the need for hardware `tokens or for additional hardware of any kind. Users only need their personal phones. SMS-based password distribution is also a clientless approach; there is no need to install or maintain software on users' phones. No other two-factor authentication methodology can compete with SMS messaging for easy and inexpensive implementation, minimal maintenance and support costs, and user convenience.

Transparent, Easy Process for Users:
Many two-factor authentication solutions are considerably less than user friendly. Some demand that the user always have a physical token on hand. Some require that specialized software be downloaded and maintained on users' phones. TalariaX's sendQuick ConeXa, however, may well be the most user-friendly two-factor authentication solution on the market.

During login to NetScaler, the user is required only to have their mobile phone at hand — and everyone always has their phone with them.

TalariaX handles everything else:
sendQuick ConeXa quickly generates a unique one-time password, sends it to the user's phone, and authenticates the user once they've entered the OTP. The OTPs are only six to ten characters; users don't have to endure the frustrating and error-prone process of typing in a huge, indecipherable string of characters.

No external third-party-owned hardware is required:
sendQuick ConeXa is a complete plug-and-play solution. And sendQuick ConeXa also reduces external dependencies by enabling complete in-house control. The solution can be configured 100 percent on site. TalariaX sendQuick ConeXa typically can be installed on existing machines, and ongoing administration is very simple — NetScaler and sendQuick ConeXa do all the work.

TalariaX helps to keep two-factor authentication affordable by permitting unlimited users: no user licenses are required. SendQuick ConeXa supports multiple VPN sessions, further bolstering efficiency and minimizing operational costs.

TalariaX sendQuick ConeXa Solution Detail

TalariaX sendQuick ConeXa uses SMS messaging to send one-time passwords to individual users for two-factor authentication. It may also be used to send customized messages and text alerts to individual users for all network, security and IT management issues. You can use sendQuick ConeXa, for example, to notify IT team members via SMS text about any issues requiring immediate response.

The self-contained, single-box design of sendQuick ConeXa provides a number of unique advantages, including:

- Fast response to user authentication requests and rapid OTP deliveries • Little downtime and minimal maintenance requirements
- Familiar SMS technology — almost everybody uses SMS on a daily basis — facilitating user convenience and ease of management

TalariaX has developed a sterling reputation for providing hassle-free support. Combined with sendQuick ConeXa’s support for unlimited users, TalariaX’s two-factor solution provides outstanding ROI for companies looking to move beyond a simple query-password security solution.

ABOUT TALARIAX

Give us a call today!

TalariaX developed sendQuick®, the industry's leading appliance-based SMS Text gateway solutions for enterprise messaging.

sendQuick has been used by over 1,500 corporations in 40 countries. Our solutions include IT alerts and notifications, 2-factor authentication with SMS OTP, marketing and emergency broadcasting for various industries such as banking, finance, insurance, manufacturing, retail, government, education, and healthcare. These have been effective to improve enterprise responsiveness, improved business workflows, and increased operational effectiveness.

FOR MORE INFORMATION, VISIT
WWW.TALARIAX.COM