USING SMS FOR TWO-FACTOR AUTHENTICATION

Deliver Security and Convenience While Protecting User Privacy
Introduction

If the pundits are on track, there will be more mobile phones on the planet than people in 2014. The utility, convenience and ubiquity of mobile and the cloud have redefined the way we engage in virtually every aspect of our lives—from what we communicate to how we shop, bank, and work. As more of life takes place in the digital world, increasing amounts of valuable and sensitive information are being stored in the cloud. The lure of that data has given rise to a new breed of cyber theft. Cyber criminals are savvy and organized. In many cases they are part of a syndicate whose sole purpose is to extract customer and corporate data for fraud, corporate espionage, extortion, and other criminal acts. A single breach at Adobe in 2013 resulted in the loss of more than 150 million username/password combinations as well as valuable source code. Popular retailer Target also had a data breach, which resulted in the theft of over 70 million credit and debit cards. As the mobile channel grows and matures, we can assume that the risk and security landscape will become increasingly complex.

Complexity is the Worst Enemy of Security

Before mobile, security consisted of protecting the PC and the user. With the advent of smart mobile devices, the game has totally changed. Mobile phones have unleashed users from a static environment, giving them a constant connection from virtually any location. As a result they’re doing more online—shopping, banking, downloading entertainment, socializing, and working. Having “always-on” access is a valuable convenience for users, but for enterprise businesses it creates more security risks and opportunities for data breaches.

Coping with this challenge usually falls to IT departments, which are already stretched. According to Bob Egram, CEO of Sepharim Group, “We’ve gone from a homogeneous environment to a heterogeneous environment with multiple screens and operating systems. It’s a capacity issue, a security and authentication issue and a policy issue. It’s a brave new world for organizations to deal with.”

The Problems with Passwords

The typical validation method employed on the Internet today is single-factor authentication, where users supply a username and password. However, that approach has significant drawbacks, particularly as cyber criminals become more organized and adept.

---

The volume of passwords is overwhelming

According to Microsoft, the average online consumer has 25 accounts, each of which requires login credentials. On any given day, an enterprise worker may require a half dozen or more passwords in the normal course of logging on to Windows, remote access, WiFi access, e-mail, and back-office applications. To simplify their personal and work lives, online users often resort to creating several complex passwords, which they use across multiple resources. The problem: once a hacker figures out just one, he’s got access to several accounts.

Convenience comes at the expense of security

Online users often choose the convenience of “Keep Me Logged In” when accessing frequently visited sites. Most don’t realize the inherent risk in doing so. The website stores a “cookie” on the computer. That cookie can be harvested by malware and sent to an attacker, who can use it to impersonate the valid user and steal online identities.

Static passwords magnify the issue

Many sites enable users to log in using their identities from social media sites like Facebook and LinkedIn. Users may assume that access is secure because they’re not supplying a password. The problem is that they’re simply reusing an existing, static password and creating another opportunity for hackers to breach their personal data.

What is Two-Factor Authentication?

As the threat landscape evolves, strong user validation that incorporates two-factor authentication (2FA) is becoming a vital component of the security framework. Two-factor authentication is not a new concept, but it is gaining popularity in today’s mobile age. Financial institutions, driven by banking regulations, already deploy 2FA for customers’ online transactions. For example, when a customer attempts to access an account, the bank sends an SMS (or text message) to the customer with a one-time PIN code that must be used to complete the transaction. Companies like Google, Yahoo, MSN, WordPress, Dropbox, and Evernote have adopted SMS-based 2FA, as have many social networking and e-commerce sites.
Authenticating a user’s identity can utilize three different factors:

- **Knowledge** — Something known only to the user, such as username and password
- **Possession** — Something only the user possesses, such as a physical card, a mobile phone, or a security token
- **Inherence** — A characteristic unique to the user, such as a fingerprint or other biometric trait

Typically, 2FA uses the knowledge (username/password) and possession (security token or mobile phone) factors. When both of these factors are required for authentication, the security model becomes much more complex, making it more difficult to bypass or hack. Today the most popular form of 2FA involves sending a unique, one-time PIN via SMS. Biometric options have also gained attention recently, but with their convenience comes trade-offs.

**Figure 1: Comparison of SMS and Biometric (fingerprint and iris) 2FA solutions**

<table>
<thead>
<tr>
<th>2FA Solutions</th>
<th>SMS</th>
<th>Biometric</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Requirements</strong></td>
<td>Any mobile phone</td>
<td>Device/software capable of fingerprint or iris scan</td>
</tr>
<tr>
<td><strong>Reach</strong></td>
<td>3 billion mobile subscribers</td>
<td>Unknown – limited to newest devices</td>
</tr>
<tr>
<td><strong>Privacy Concerns</strong></td>
<td>Users must provide their mobile phone number</td>
<td>Users must provide their fingerprints and/or iris scan</td>
</tr>
<tr>
<td><strong>Learning Curve</strong></td>
<td>Very low, most people already use SMS</td>
<td>Depends on device, software and user</td>
</tr>
<tr>
<td><strong>Static Password</strong></td>
<td>No. A unique PIN is generated for each authentication</td>
<td>Yes. Your fingerprints and iris don’t change</td>
</tr>
</tbody>
</table>

**Benefits of 2FA**

Two-factor authentication provides many business benefits, including tighter security, increased employee productivity, higher customer confidence and lower IT costs.

**Improve security**

The more factors used to establish identity, the greater the likelihood of authenticity. By requiring a second form of identification, 2FA decreases the probability that an attacker can impersonate a user and gain access to computers, accounts or other sensitive resources. Passwords can be easily lost or stolen. Even if a fraudster gains access to a password, he won’t have the second element required to authenticate.
Increase productivity and flexibility

Today’s workplace is no longer a closed environment. Employees are mobile and use multiple devices across locations. Enterprises are embracing mobility as it contributes to higher productivity. With SMS-based 2FA, employees can securely access corporate applications, data, documents, and back-office systems from virtually any device or location—without putting the corporate network and departmental information at risk.

Lower helpdesk and security management costs

The average customer calls the help desk 1.25 times per month. In an environment that’s experiencing unusual downtime or has had recent upgrades, that number can exceed three calls per month. The industry research group HDI, estimates at least 35 to 40 percent of those calls are related to password resets. Furthermore, each of those tickets consumes, on average, 20 minutes of the help desk technician’s time. Two-factor authentication can help eliminate time-consuming and costly password-reset calls by providing a safe and secure way for end users to reset their own passwords while improving enterprise-wide security.

Reduce fraud and build secure online relationships

Online fraud cost e-retailers $3.5 billion in 2012, and identity theft, which accounted for 17 percent of all fraud in 2013, is on the rise. Fraud in all its guises has a direct impact on the bottom line. Even worse, it can result in a loss of trust, credibility and brand equity, and destroy a customer relationship. Twenty-nine percent of fraud victims avoid certain retailers, even if the merchant wasn’t responsible for the data breach. To build an online relationship

SMS-Based 2FA in Action

During the first week of his new job, Henry needs to enroll in several benefit programs, one of which is healthcare. The HR team provides him with a URL to an online enrollment application, which is usable from his personal tablet. From home he accesses the site, and the first task he’s prompted to do is create a user account. The account setup page explains that Henry needs to do three things. First he needs to enter a difficult-to-guess username and password and his mobile phone number. Henry’s phone number gets linked to his account, which in itself is added security. After Henry submits his information, his employer sends a PIN to his mobile phone, and he needs to enter the PIN in order to proceed. Henry also has the option to request a PIN each time he accesses the site, which he does because it gives him added assurance that his information is secure. Henry’s able to complete the enrollment process without worrying that his personal information is at risk.

---


with a business, customers must have confidence that their transactions are secure and their personal and financial data is safe. By requiring a second authentication factor, 2FA provides an additional layer of protection that secures the site, the transaction and customer. Moreover, by creating a secure brand experience, businesses can increase their opportunity to create ongoing interactions with customers, a key step in building loyalty and driving repeat purchases.

**Implementing Two-Factor Authentication**

CTOs need to carefully consider several factors in their evaluation and implementation of a 2FA solution.

**In-house or partner**

The first question an enterprise must address is whether to implement two-factor authentication in-house or outsource it to a third party. Initially, many companies choose to implement their own solution using corporate IT resources. However, in the long run, that strategy often proves untenable. Supporting technologies for 2FA solutions are outside the domain of most IT departments. Furthermore, many IT departments are already constrained, dealing with integration and process challenges and supporting help desks. It makes more sense to focus internal resources on core business competencies and leverage partners for 2FA solutions.

**Single-purpose solution or mobile engagement platform**

Once the decision is made to deploy a third-party solution, CTOs have a host of options from which to choose. However, given the dynamic and complex nature of the mobile environment, CTOs should take a strategic view. Rather than implement 2FA as a standalone solution, CTOs should implement 2FA as one of many enterprise solutions that will be needed across their business. The best way to address the needs at hand while covering for the needs of the future is to implement on a mobile engagement platform that can serve many business use cases. Implementing 2FA via an engagement platform presents the opportunity to more completely think about a mobile engagement strategy. For example: How can mobile improve communications on a broader scale with customers and employees? For which processes and workflows can mobile reduce costs? How can a comprehensive mobile strategy improve customer relationships and add value?

By taking a broader approach with a mobile engagement platform, CTOs can implement a cost-effective SMS-based 2FA strategy as well as address a variety of operational and engagement use cases that impact the entire organization—sales and marketing, operations and logistics, customer service, IT and security, human resources and corporate communications.
Criteria for Selecting an SMS-based 2FA Platform Provider

Identifying a set of selection criteria will help enterprises secure the right partner to not only deliver 2FA, but also provide broad support for mobile engagement needs throughout their organizations. IT decision-makers leveraging third-party providers need effective mobile business partners who can deliver all of the following:

- Domain expertise for mobile solutions, regulatory compliance and industry best practices
- Service flexibility to meet unique business requirements and to support multiple use cases
- Demonstrated performance and reliability – especially critical for 2FA
- Global reach to all target audiences
- Simplified technical integrations and 24/7 customer support
- Corporate maturity encompassing financial stability, data security and privacy policies, and mature business practices
Conclusion

The utility, ubiquity and convenience of mobile phones have completely transformed the communication landscape. Today’s users are accustomed to having technology at their fingertips and the information and resources they need in the palm of their hand. This level of digital convenience offers huge potential for enterprise businesses, but it also introduces new security risks and vulnerabilities.

Strong user authentication that incorporates 2FA is becoming an essential component of a robust security framework. Given the dynamic and complex nature of the mobile environment, CTO/CIOs should take a strategic view when implementing a 2FA solution. Rather than addressing 2FA as a single mobile use case, they should view authentication in the context of an integrated mobile engagement strategy. By deploying a mobile engagement platform, enterprises can implement a cost-effective 2FA, and also support a wide variety of use cases that more broadly benefit the entire organization.

About OpenMarket

OpenMarket, a subsidiary of Amdocs, helps enterprises use mobile to transform their business. OpenMarket provides mobile engagement solutions for organizations to optimize their operations and enhance relationships with their customers and employees. Major enterprises choose OpenMarket for our domain expertise, service flexibility, demonstrated performance and reliability, global scale, and corporate maturity. We provide smart, interactive connectivity to more than 200 countries, enabling businesses to engage with nearly every mobile user around the world. Our clients trust us to power their mobile business. For more information, visit www.openmarket.com.

Contact Us

OpenMarket
Americas (Headquarters)
sales-us@openmarket.com
877.277.2801

OpenMarket
EMEA
sales-uk@openmarket.com
+44 20 8987 8855

OpenMarket
Australia
sales-australia@openmarket.com
+61 (0) 2 9332 2141

OpenMarket
India
sales-india@openmarket.com
+91 20 40157069

Terms of Use

Copyright © 2014. All rights reserved. No part of this publication may be reproduced, distributed, electronically stored, or translated into any language, in any form by any means, without the prior written permission of OpenMarket.