White paper
Two-Factor Authentication

Yuriy Mikitchenko, MBA
Head of Marketing
Messente Communications

Lauri Kinkar
CEO
Messente Communications

Executive Summary

Online security is a constant battle between organizations providing value to society and those who exploit the internet for financial gain or to cause harm. Nearly €80 billion has been spent in 2017 on information security, and the cost of malicious attacks amounts to roughly €300 billion in a twelve-month period.

There are several variables to information security. Headlines over the years not only illuminate flaws in information technology hardware and software, but also flaws in behavior and business processes. In other words, even the most well-funded informa-tion technology operations fall victim to attacks. For example, the Equifax breach announced early September 2017 stemmed from an exploited, unpatched server. Hence, it was the lack of a busi-ness process – a checklist of patches – that was the root cause of the hack which affected 143 million Americans.

It was a lack of enforced two-factor authentication that led 8tracks.com to lose 18 million usernames, emails, and passwords. A developer did not enable two-factor authentication on his GitHub account, which led to a hacker compromising the account through weak or stolen credentials. While a business process within GitHub could force two-factor authentication, it is mere user behavior at fault for 8tracks' hack.

Thus, the question at hand involves improvements to business processes and user behavior online, rather than the need for improvements to security technology.

To their own demise, small business owners and leaders believe that hackers strictly focus on targeting large organizations, as their return is greater. That's not the case, though; hackers are opportunistic and will take the opportunity to exploit any organization, regardless of size. In fact, hackers pursue small organizations because they are usually more vulnerable, as they do not expect to be attacked. For that reason, many small businesses close their doors after an attack, as they cannot recover from the financial loss and damage to their reputation.

It is compelling that a satisfactory two-factor authentication solution mitigates more financial risk than it costs to implement and pay the variable costs of such a solution. With 81% of hacking related breaches arising from weak or stolen credentials, the financial risk of a hack at any given point for a company with a combined 1000 employees and customers is about €38,000 (with some assumptions,) while 10,000 authentications with Messente costs less than €600 a month, plus up to €1,200 of a developer's time to implement Messente's entire toolkit. To complete the solution, the business would force two-factor authentication for all users –employees, customers, and partners.

While two-factor authentication is one piece of the online security puzzle, it is one of the most effective and least expensive ways to influence user behavior and improve business processes. The forthcoming report presents more information and builds a strong argument for all organizations that connect to the internet to implement two-factor authentication across the organization, as well as influence people to be more responsible citizens of the internet.

01 Introduction

IT and data security continue to be top priorities for technology professionals in business, as data breaches, malicious attacks, and ransomware headlines fill the news. Business technology leaders are continuing to invest in information security, as it tops IT projects lists.[1]

Digital security involves several variables. However, this document's purpose it to discuss a low-cost, yet high-impact, solution in one area of digital security: online security.

The information presented in this document illustrates the effectiveness of two-factor authentication to influence online user behavior, whether the user is a customer or an employee, in terms of a cost-benefit analysis.

- **Usernames and passwords are the primary culprits behind hacks and data breaches.** Malicious attacks exploit weak online credentials to gain access to online accounts and corporate intranets.

- **The costs of a potential online account hack leading to a data breach outweigh the costs of two-factor authentication.** Encouraging safer user behavior online using two-factor authentication is a low-cost method to prevent malicious online account activity. The business limits indemnification costs of due to account hijackings and improves online reputation.

- **Time-based one-time password (TOTP) mobile applications address security concerns around pin codes sent via SMS.** Signaling System No. 7 (SS7) has its flaws, as determined hackers find avenues to exploit security vulnerabilities to intercept SMS messages.[2]

- **Low-cost, high-impact.** Two-factor authentication encourages responsible online behavior, securing account access across the web, while mitigating financial risk at a low cost.

In addition, a cost analysis is presented based on financial risk probabilities and the cost of Messente's two-factor authentication tools.

[1] Tech Target
[2] Wired

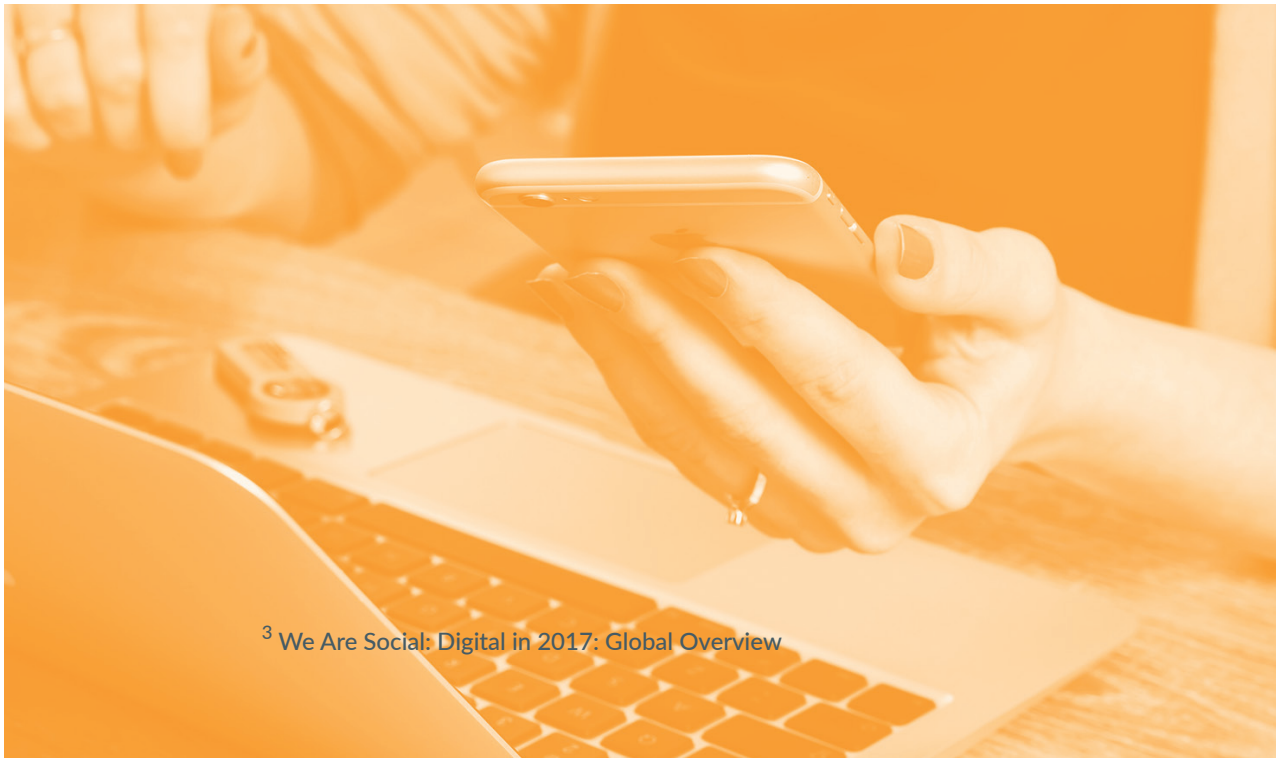
02
Two-Factor Authentication

The term 'two-factor authentication' is interchangeable with 'multi-factor authentication,' 'two-step verification,' and 'user verification.' Technically, the process of a second login factor is considered verification, as users verify that they maintain possession of another device, rather than authenticating their identity. Specifically, with mobile devices, users authenticate using their usernames and passwords, then verify that they possess the device associated with the phone number on the online profile or corporate identity. Verification occurs through the delivery of a PIN code sent to the mobile phone through an SMS message or a mobile application with a time-based one-time password (TOTP) synced with the corresponding server.

For the sake of consistency, this document uses 'two-factor authentication' (2FA,) as it is the commonly adopted term.

Other methods are used for two-factor authentication. While the result is the same, with the user inputting a code as the second authentication factor, some solutions include a different device, like a keychain that digitally displays the TOTP. However, as mobile devices are widely used across the globe, they are more feasible for online two-factor authentication, with SMS being the most ubiquitous mode of delivering PIN codes.

The analysis in this whitepaper solely focuses on using mobile devices with the ability to run iOS or Android applications.



[3] We Are Social: Digital in 2017: Global Overview

Most of the world's population has a mobile phone[3]. Thus, using mobile phones as the second authentication factor to improve online security proves obvious. Yet it wasn't until as of late that the most prominent online platforms have begun encouraging users to turn on two-factor authentication. In addition, any website that provides users an account, requesting the users to create usernames and passwords, is vulnerable to malicious activity leading to a data breach.

Businesses with an online presence do not have an excuse to not protect their users with two-factor authentication.

- Protect user data by adding more confidence that the right person is accessing appropriate data.
- Reduce the risk of a data breach with a second authentication factor to usernames and passwords, which are typically weak.
- The cost of two-factor authentication tools (applications, APIs, and variable costs) are a relatively inexpensive to mitigate the cost of a data breach.
- 81% of hacking related breaches leveraged stolen and weak online credentials, or default passwords.[5]

[4,5] Verizon Enterprise Solutions

2.1 Usernames and Passwords are Inherently Weak and Likely Compromised

Most data breaches and attacks include weak or stolen passwords[4].

- Nearly 4.8 billion (and growing) usernames and passwords are floating around the internet.[6]
- Username and password breaches span across industries, with many incidents coming from less-known websites.
- 66% of usernames and passwords were obtained through malware installed through a malicious email or through a fake website.[7]
- 75% of all breaches stemmed from outsiders.[8]
- Credential breaches are growing at an exponential rate, with over a billion usernames and passwords breached in 2016 alone.[9]
- Most hackers are seeking financial gain, and businesses are held responsible to indemnify users.[10]

The conversation around authentication is not new. Nonetheless, the data underlying the claim is staggering. People reuse passwords, make predictable variations, and even use simple, common passwords (i.e., "password123.") Most online users aren't even aware that their passwords are likely available online for hackers to buy.

Surprisingly, businesses that maintain online user accounts and associated passwords do not take responsibility for user behavior. Breaches that reach global headlines mostly refer to well-known brands (i.e., LinkedIn, Yahoo!, Adobe.) Smaller organizations assume immunity to breaches and hacks, which makes them more vulnerable, as they are ill-prepared. Nearly half of all cyber-attacks are on small to mid-sized business, with the chance of an SMB falling victim to a cybercrime being one in forty. In the United States, sixty percent of SMBs that experience a cyber-attack go out of business within six months.[11]

[6] Troy Hunt: Have I Been Pwned?
[7,8,9] Verizon Enterprise Solutions
[10] IBM & Ponemon
[11] US Securities and Exchange Commission

2.2
The Cost of a Breach

Large enterprises and well-known brands typically have the cash to recover from a data breach, yet they remain painful. Small to mid-sized businesses do not have that luxury, as breaches are not proportional to size of the company. According to the annual study of the cost of data breaches by IBM and the Ponemon Institute, the average cost of a lost or stolen record, which may contain confidential information, costs €131 per record. While SMBs likely store less confidential information, multiple confidential records per employee or customer exist.

Business leaders must think: How many pieces of confidential information are correlated to one user account? How do costs vary by industry? What are the local breach notification laws? Which countries are primarily targeted? (The following information is from the IBM & Ponemon Institute Cost of Data Breach Study.)

- Malicious attacks are more expensive, costing €137 per breached record, and are the most common causes for breaches.
- The probability of a breach in the next 24 months is 27.7%.
- Businesses in South Africa, India, and Brazil are the most likely to experience a data breach in the next 24 months.
- Average amount of lost customers due to breaches continues to rise.
- 201 days to discover a breach, on average.
- 70 days to contain a breach, on average.

- The United States has the highest breach notification costs and highest overall breach cost, at €197 per record.
- €330 per breached record in healthcare and €215 in financial services, being the two industries with the highest breach costs.
- Smaller data breaches are more common and organizations that have smaller data breaches are more likely to have them again.

Costs are attributed to variables like customer indemnification, paying for tools to protect identities post breach, lost customers and revenue, and a tarnished brand reputation.

03 Implementing Two-Factor Authentication

Deploying two-factor authentication requires more than mere deployment of software. For 2FA to be successful at strengthening authentication to deter attacks due to weak credentials, business processes must be improved. A process to force 2FA for both internal and external users must be in place. Internal users, like employees, must be required to authenticate beyond a username and password to use company systems and access data.

Messente recommends that external users, which may be customers or partners, to authenticate using SMS 2FA after a password – at a minimum. While time-based one-time passwords are safer, not all users are inclined to download and manage TOTP applications, or continue adding online services to a mobile application. Thus, asking for a mobile phone number and sending an SMS message during the signup process of an online service becomes a simple way to enforce a form of 2FA that is at least better than no 2FA at all.

3.1 Cost of Two-Factor Authentication

While there are multiple forms of two-factor authentication, Messente's expertise lies in time-based one-time passwords via a mobile app and SMS PIN codes. The proceeding analysis focuses on the more common 2FA methods now: SMS PIN codes and one-time passwords from a mobile app.

3.1.1 Authenticating users by verifying their phone numbers

Successfully authenticating users by verifying their phone numbers involves the following steps.

A

Build a two-factor authentication interface for the online service or mobile app.

First, when 2FA is not compulsory, creating functionality for users to enable it during and after the account creation process is required. Next, depending on the nature of the service, authentication triggers must be established and coded. Triggers may include making a transaction and logging in from a new location or device. However, online services commonly require a second authentication factor every time a user logs in.

Establishing two-factor authentication includes acquiring user mobile phone numbers and verifying them, which is the first authentication when using an API. Organizations have the option to build the interface and required processes, however, Messente has created the user interface for organizations as part of the verification and 2FA platform.

B
Verifying phone numbers and user authentication.

Messente's solution to two-factor authentication is an API (application programming interface) that generates, delivers, and validates PIN codes and time-based one-time passwords. Every authentication process involves a client's server making API calls when users need to authenticate.

Servers connect via HTTPS, which is a familiar protocol for developers creating websites and web services. Thus, utilizing an API does not require knowledge of telecommunications specific technology, like SMPP connections. Messente's technology translates API calls and sends instructions to mobile network operators, bridging the gap between technology used by creators of web services and technology specific to the telecom industry.

The most important parameter required in the API call is the user's phone number, which will receive the PIN code. More information is available in the documentation library on Messente.com.

3.1.2 Financial Cost

Investment in a two-factor authentication solution depends on the approach.

A
Build 2FA functionality in house.

Pro: More control over specific functionality.
Cons: Longer implementation time, larger investment, and handling all service and quality issues internally.

B
Use an API from a trusted partner.

Pros: Significantly lower implementation time and costs, optimized SMS delivery routes by the partner, and have the partner handle any delivery quality issues.

Con: Less control over specific functionality.

Based on a customer survey, developers typically dedicate 8-24 hours to deploy every verification and authentication tool available from Messente. The same survey revealed that it takes 5-6 weeks of fulltime developer hours to build an SMS-only 2FA solution for one online service. Extend the time to 8-10 weeks if the organization is looking for a 2FA solution handling TOTP.

The cost of developer time varies (San Francisco based developers are much more expensive than those in India.) An in-house fulltime developer in Europe costs 1,750 to 2,000 euros per week. Add 50% to the cost if the work is outsourced.

Thus, the estimated cost to build a fully-functioning 2FA solution is between 14,000 to 20,000 euros.

Then the firm must consider variable SMS costs, which are higher than working with a partner, as partners leverage high SMS volumes to negotiate lower costs from network operators. The internal team would then support the homegrown solution and handle support calls. Lastly, the firm must consider uptime of the solution and the implications to user experience if authentications fail.

The alternative is to adopt an API built by a trusted partner.

The estimated cost of deploying Messente's API is developer time, which is 350 to 1,200 euros. Messente does not charge for the API or deployment. In addition, the firm must pay variable costs based on each authentication. SMS PIN code costs depend on the geographical market and TOTP authentications are fixed, but much less expensive than SMS authentications. Messente handles software maintenance, delivery quality and reliability, and support at no additional cost.

04
The Case For Time-Based One-Time Passwords

While two-factor authentication significantly reduces the probability of breaches due to hijacked accounts, security concerns regarding SMS-based PIN codes arise.

Mobile network providers use a protocol called Signaling System 7 (SS7) to communicate with one another when routing calls, SMS messages, and internet data. This protocol was built in the 1980s and designed to maintain calls when users moved across cell towers.

The problem, demonstrated in 2014, is that the functionality enabling mobile phone traffic to move from one tower to another makes it possible for hackers to divert calls and text messages. Hackers can monitor or save the data before forwarding the information to the intended recipient. Note, this is very expensive to do, meaning the hacker must be highly motivated and targeted.[12]

Although messages carrying PIN codes are encrypted by the mobile carriers, global use of SS7 to send SMS PIN codes implies that interception is possible.

The flaw in SS7 protocols can be patched by implementing a series of firewalls and filtering rules, but as a Federal Communications Commission in the United States concluded in March 2017, "the global traffic size using SS7 protocol today is overwhelming and the patching needs to be done in a way that avoids collateral network impacts."[13]

4.1
What does this mean for 2FA?

To make authentication convenient for users and avoid security issues regarding SS7, organizations have begun adopting time-based one-time passwords as a second form of authentication, rather than randomly generated PIN codes sent via SMS.

A time-based one-time password is a code calculated based on a secret key, unique to every online service and the current time. Utilizing a user's secret key, TOTP is calculated by a 2FA mobile application and the online service the user is attempting to access. Like the PIN code, TOTP is only valid for a short period defined by the online service.

[12] The Register
[13] Federal Communication Commission

TOTP eliminates the need to send PIN codes to the user. Instead, a code is computed by the TOTP algorithm on both sides of the authentication process. However, using TOTP requires the use of a 2FA mobile app or another physical security token.

While it is simple to download a mobile app, and sync it with a service, user behavior has shown that most people do not use a TOTP app and prefer to receive codes via SMS, as it is more convenient. Therefore, organizations must influence user behavior to adopt TOTP and the use of a 2FA app, yet need to provide SMS-based PIN codes as a fallback option.

Based on Messente's usage data, 70% of PIN codes are sent over SMS despite security threats originating from SS7. Our conclusion to the greater use of SMS is the fact that not having 2FA is much less secure than having PIN codes sent using a vulnerable protocol.

However, Messente has invested in developing a user 2FA application free to download by anyone, with a minimal-branding design and simple user interface, encouraging firms to promote the use of TOTP with our enhanced 2FA API.

05 Conclusion: Low-Cost, High-Impact

As 81% of hacking related breaches stem for weak or compromised passwords and the cost of two-factor authentication is a small proportion of the potential cost of a breach, the argument for 2FA for all users is strong.

The table below illustrates the potential financial impact of a hacking-related breach, and the financial impact based on the probability of a breach in the next 24 months.

Records	Breach Financial Potential	Financial Impact by Breach Probability
100	€ 13,700.00	€ 3,794.90
1,000	€ 137,000.00	€ 37,949.00
10,000	€ 1,370,000.00	€ 379,490.00
100,000	€ 13,700,000.00	€ 3,794,900.00
500,000	€ 68,500,000.00	€ 18,974,500.00

The next table illustrates the variable costs of two-factor authentication by the number of authentications (based on list prices for the French market.)The next table illustrates the variable costs of two-factor authentication by the number of authentications (based on list prices for the French market.)

Authentications	Cost of per SMS Authentication	Cost of per TOTP Authentication
1,000	€ 53.00	€ 26.50
10,000	€ 530.00	€ 265.00
100,000	€ 5,300.00	€ 2,650.00
1,000,000	€ 53,000.00	€ 26,500.00
5,000,000	€ 265,000.00	€ 132,500.00

The cost versus benefit distinction is clear: the cost of two-factor authentication is proportionally minimal compared to the risk of hacking-related breaches stemming from weak credentials. At the extreme, the cost of 5 million SMS authentications is € 265,000, while at any point the financial risk based on probability is nearly €375,500 for 10,000 records, with a potential financial loss of €1,370,000. The numbers vary based on digital records handled and the number of verifications, however, realistic scenarios prove that the cost of using 2FA to mitigate the risk discussed is substantially less than the probable financial fallout of the risk.

06 About Messente

Messente Communications, Ltd. provides global SMS communication, user verification, and two-factor authentication services to businesses and public-sector organizations. Building application programming interfaces (APIs,) Messente focuses on business-critical communication, sending SMS messages and PIN codes to over 190 countries and through over 800 mobile networks.

In addition, the company has built a two-factor authentication toolkit for web services and mobile applications. The toolkit includes an API that handles both SMS-delivered PIN codes and time-based one-time passwords synced to online services with an authentication app. The toolkit also includes Messente's own authenticator mobile app, called Verigator, which is a brand wholly owned by the company. Verigator is free to the public and can be downloaded on the Apple App Store or the Google Play Store.

07 References

"2017 DBIR: Understand Your Cybersecurity Threats." *Verizon Enterprise Solutions*, 2 May 2017, www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

"2017 Internet Security Threat Report." *Symantec*, www.symantec.com/security-center/threat-report.

"2017 Ponemon Cost of Data Breach Study." *IBM 2017 Cost of Data Breach Study - United States*, 28 July 2017, www.ibm.com/security/data-breach/index.html.

"CIOs Make Security a Priority for 2016, but Not Privacy." *TechTarget*, searchcio.techtarget.com/blog/TotalCIO/CIOs-make-security-a-priority-for-2016-but-not-privacy.

"Communications Security, Reliability and Interoperability Council V." *Federal Communications Commission*, 16 Mar. 2017, www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability.

"Cyber Security Bill for 2015: $75 Billion Spent, $300 Billion Lost." *Adaware*, www.adaware.com/blog/cyber-security-bill-for-2015-75-billion-spent-300-billion-lost.

"Digital in 2017: Global Overview." *We Are Social*, wearesocial.com/special-reports/digital-in-2017-global-overview.

Fox-Brewster, Thomas. "How Hackers Broke Equifax: Exploiting A Patchable Vulnerability." *Forbes*, Forbes Magazine, 14 Sept. 2017, www.forbes.com/sites/thomasbrewster/2017/09/14/equifax-hack-the-result-of-patched-vulnerability/#d7da6aa5cda4

"Have I Been Pwned? Check If Your Email Has Been Compromised in a Data Breach." *Have I Been Pwned? Check If Your Email Has Been Compromised in a Data Breach*, haveibeenpwned.com/.

John Leyden & Simon Rockman
26 Dec 2014. "White Hats Do an NSA, Figure out LIVE PHONE TRACKING via Protocol Vuln." *The Register® - Biting the Hand That Feeds IT*, www.theregister.co.uk/2014/12/26/ss7_attacks/.

Khandelwal, Swati. "Hackers Can Read Your Private SMS and Listen to Phone Calls." *The Hacker News*, 19 Dec. 2014, thehackernews.com/2014/12/hackers-can-read-your-private-sms-and.html.

Muresan, Razvan. “Cyber Security Spending to Reach $90 Billion in 2017, Gartner Says.” *Business Insights in Virtualization and Cloud Security by Bitdefender*, businessinsights.bitdefender.com/cyber-security-spending-2017.

“The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses.” *SEC Emblem*, 19 Oct. 2015, www.sec.gov/news/statement/cybersecurity-challenges-for-small-mid-size-businesses.html#_edn6.

Newman, Lily Hay. “A Cell Network Flaw Lets Hackers Drain Bank Accounts. Here's How to Fix It.” *Wired*, Conde Nast, 2 June 2017, www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/.

Zaleski, Andrew. “Congress Addresses Cyberwar on Small Business: 14 Million Hacked over Last 12 Months.” *CNBC*, CNBC, 5 Apr. 2017, www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html.