TOPIC 18: SECURING CREDIT UNION SYSTEMS WITH TWO-FACTOR AUTHENTICATION (YEAR: 2018)

Akash Gill

Sr. Software Engineer, USA.

Abstract

The protection of financial institutions, especially credit unions, has become a concern due to the prevalent and evolved cybercrime. This paper focuses on using two-factor authentication models to shield credit union systems, focusing on the case of Genisys Credit Union's adoption of the method. Credit unions remain highly susceptible to such attacks because they use single-factor authentication and seek to protect significant amounts of financial and personal data. These weaknesses place these institutions at the mercy of phishing and credentialing and abiding by regulatory requirements. To overcome these risks, two-factor authentication works by requesting two completely separate types of identification, such as a password and a unique one-use code or fingerprint. The advantages of 2FA are increased protection from unauthorized access, meeting regulations and requirements such as PCI DSS, and increased member trust. Implementing 2FA is not without problems due to users' reluctance, technical integration issues, and costs. This article describes a step-by-step guide for credit unions to adopt 2FA proactively. Credit unions can adopt phases, train employees and members on the procedure, and constantly monitor the new systems. The practical outcome can be illustrated by the case of Genisys Credit Union, which applied 2FA and proved that the measure eliminates unauthorized access while increasing trust among stakeholders. With cyber threats emerging rapidly, credit unions must implement multiple levels of cyber security controls along with 2FA to protect accounts, remain compliant, and preserve members' trust. This article recognizes the need to safeguard the financial sector as the world becomes more digital and innovative.

Keywords;
Cybersecurity, Authentication, Compliance, Encryption, Data Breach, Risk Management, Access Control, Biometrics, Phishing, Passwords, Financial Regulations, Two-Factor

Introduction

The digitalization of the financial sector exposed institutions to higher risks while receiving numerous advantages due to advancing technology. Credit unions claiming to provide services to their members face more cyber threats regarding their financial data (Goddard et al., 2008). As these organizations expand their online presence, protecting members' data and organizational frameworks becomes critical. They include email spoofing, a man-in-the-middle attack, phishing, and others known to cause great havoc, especially when executing some business-critical processes online. One of the most effective measures of implementing 2FA has later proved to be very effective in enhancing the security of systems as a security device that acts as a barrier against the threats above while executing business-critical processes online.

Two-factor authentication is an example of security when the subject is authorized after proving his identity in two ways, the first factoring and the second factoring being different (Kowalski, 2011). It can be a password and mobile phone, a password, an identification token, or any other biometric. This double protection system greatly minimizes the chances of cybercrimes; this is so compared to the archaic method of single-factor security where a password is used. Where credit unions may fall prey to advanced attacks like phishing or credential theft, 2FA provides credit unions with a strong line of defense, considering the escalating concern for data security and the regulations that come with it.

Credit unions have specific security concerns because they are financial institutions and non-profit member cooperatives. The sites contain highly confidential information about their users and members, account information, and transaction history, making them vulnerable to cybercriminals. Consequences of a breach are also unfavorable, including monetary losses, eradication of the organization’s reputation, and the resultant deterioration of trust among members of the alliance. Therefore, credit unions must implement high-security measures that protect assets and comply with emerging laws such as PCI DSS and the NCUA guidelines (Bair, 2010).

The necessity to increase the level of protection was previously illustrated by the example of Genisys Credit Union, which adopted 2FA in its internal environment. This proactive measure helped to add an extra layer of security around its structure and inflicted an extra level of protection on data that threats might compromise. The achievements of Genisys serve as an example of how it is high time to focus on modern practices in the sphere of security struggles in the context of the growing usage of informational technologies. This included the enhancement of core industry encryption mechanisms as well as a focus on maintaining the compatibility of the system, which greatly minimized cases of intrusions. It enhanced member confidence since the institution could assure them that their information was safe had joined the initiative.

This paper discusses the importance of two-factor authentication in protecting credit union systems (Mihsin et al., 2017). It explores Genisys Credit Union’s implementation of 2FA, the problems that credit unions encounter, how 2FA works, and how to implement this technology. It then broadens to the advantages and disadvantages of 2FA and the notion of the multiple-vector approach to protecting digital assets. With the latest cyber threats looming, imbibing measures like 2FA is not only best practice but mandatory. As signified in this detailed reference guide, credit union systems must be strengthened by 2FA prominence to counter escalating risks and reassure their stakeholders.

1. Challenges of Credit Union Security before 2FA

Credit unions' several security problems made opening 2FA the only protection option against cyber threats. These challenges have been due to reliance on traditional forms of authentication, the evolving threat landscape, regulatory compliance, and the need for businesses to be more aggressive in protecting their assets. This section presents five critical areas credit unions had faced before using 2FA (Stanislav, 2015). These organizations needed to improve security to safeguard members' information and credit unions' reputations.

Figure 1: Two-Factor Authentication Challenges

a) Weaknesses of Single-Factor Authentication Systems

The initial verification system used by the majority of the credit unions prior to the implementation of 2FA was a single factor, including a username and password. This was easy to implement yet posed a significant security risk to the procedure. Passwords tend to be repetitive and simple and appear in large volumes in instances where the database of accounts has been compromised. The choice of passwords is also not very strong; in many cases, users can get through easily through brute force when there is no second confirmation level. A simple password exposes the intruders to any resource and information within the company.

This was made worse by phishing attacks where the attackers are rampant because they impersonate corporate accounts and make users reveal their login information (Jakobsson, 2012). Banks, particularly credit unions, as they received financial data on members, were often targeted in such scams. Once the attackers have legitimate credentials, they could break into systems and get data or manipulate accounts, which lead to heavy losses and losses of reputation.

b) Increased Risk of Data Breaches

Credit unions are financial institutions that operate with much information from their members, other balances, history of transactions, and other credit information. However, this information was vulnerable since most organizations still do not have strong security features. It also surfaced that breaches led to immediate monetary losses. Credit unions also faced risks such as lawsuits, fines from regulators, and long-term loss of image. Cyber terrorists use malware and other tools to access network system weaknesses and extract information (Rudner, 2013). It observed that credit unions did not have multi-layered security where such threats could be addressed in real time. The post-breach incidents entailed numerous processes, such as member notification and expensive system improvements, which greatly exploited resources.

c) Challenges in Regulatory Compliance

Credit unions must maintain high levels of compliance with policies intended to safeguard member data and control operations. Some social insurance organizations, like the National CU Administration or NCUA, and some standard systems, such as the Payment Card Industry Data Security Standard or PCI DSS, comprise potent security protocols to shield financial data. Relying on these older authentication methods puts many credit unions low regarding compliance needs. Private sanctions for non-compliance included fines, being subjected to closer supervision, and losing reputation (Svetiev et al., 2014). Also, single-factor authentication was deemed insufficient for guarding access to the data, which became an added concern for credit unions to apply for more complex security measures.

Figure 2: Levels of Regulatory Compliance

d) Evolving Cyber Threat Landscape

Cybersecurity warfare's latest realities are notorious because a clear picture transforms, and persecutors continue inventing new and novel strategies to penetrate systems. Credit unions were unable to meet these emerging threats before implementing 2FA. Methods such as credential stuffing, in which hackers use stolen usernames and passwords harvested from other violent data breaches on other targets, were especially effective among institutions using single-factor authentication. Insiders remain a problem for the following reasons. It is always possible that employees who have been granted access to the systems could inadvertently or intentionally violate the security of organizational systems or even through identity attacks such as phishing and others. Credit unions had no way to identify attempts at logging in other than the password input, making them more vulnerable to such threats (Randazzo et al., 2004).

e) Impact on Member Trust and Confidence

Credit union members must have faith in their institution since it is one of the pillars that runs most credit unions. This puts the security of personal and financial data at the core of credit unions, which is different from traditional banks. Unauthorized access or data breaches have eroded this trust, resulting in dissatisfaction and, likely, member churn. The lack of apparent active security also undermined people's confidence. They also wanted their financial institutions to consider cybersecurity important, and a lack of sophisticated authentication meant that there was no strong desire to safeguard their information.

f) Growing Need for Advanced Security Solutions

These challenges could not have gone unnoticed by credit unions, which saw the need to develop stronger security systems. Using only a single-factor authentication, posing new threats and strict regulations, was insufficient. The demand moved towards solutions that provided a higher level of protection, although not at the cost of freedom. Two-factor authentication is a natural evolution of single-factor authentication that has solved many problems with single-factor systems. However, because it uses a second verification form, 2FA greatly lowered the odds of someone gaining access to an account even if they had the password. Additionally, it provided evidence of other precaution techniques, which encourage credit unions to regain members' trust and meet all regulatory requirements (Carmichael et al., 2002).

Figure 3: Higher Levels of Protection

The previous era, where 2FA was nonexistent, had credit union security systems exposed to many vulnerabilities. The significant reliance of institutions on single-factor authentication has left them open to data breaches, regulatory fines, and, last but not least, loss of members' trust. Cyber threats change a lot and become more dangerous very fast, to overload traditional protection tools. Credit unions started implementing solutions such as 2FA, which defined creating more stable systems. This transition not only saved the confidentiality of important information but also regained the trust of members in the organization's capacity in a world that continues to be integrated with computers.

Table 1: Security Challenges before the Implementation of Two-Factor Authentication

Challenge	Description	Impact
Weak Single-Factor Authentication	Reliance on simple passwords made systems vulnerable to phishing and brute force attacks.	High risk of unauthorized access and data breaches.

Data Breach Risks	Lack of multi-layered security exposed sensitive financial data to malware and cyber threats.	Monetary losses, reputational damage, and regulatory penalties.
Evolving Cyber Threats	Emerging attacks like credential stuffing and phishing outpaced outdated security measures.	Inadequate protection against advanced threats.
Regulatory Compliance Challenges	Single-factor methods failed to meet standards like PCI DSS and NCUA guidelines.	Risk of fines and closer regulatory scrutiny.
Declining Member Trust	Breaches undermined members' confidence in the institution's ability to secure personal and financial data.	Loss of trust, dissatisfaction, and potential member attrition.

2. What is Two-Factor Authentication?

Two-factor authentication (2FA) is a security measure that makes accounts and systems more secure by requiring the user to authenticate himself in two ways (Dmitrienko et al., 2014). This method removes the single factor of authentication, where one is required to enter a username and password. By incorporating two identification methods, the risk of unauthorized access is greatly minimized, even if one of the factors is somehow breached. In today's rapidly evolving security environment, 2FA has become a must-have element of any sophisticated cybersecurity strategy, giving it the necessary protection against almost every attack.

The concept of 2FA is built on the principle of requiring two independent credentials that fall into different categories, such as knowledge possession and adherence. Possession is something that the user has and can be a smartphone, a hardware token, a security key, or any other item. Inherence concerns an attribute that the user possesses. These include fingerprint, facial, or voice recognition. Two of these classes are incorporated in 2FA, thus making it impossible to compromise the entire authentication mechanism in cases where the first factor is breached. One of the most familiar use cases of 2FA is provided by an example of logging into an online banking application. If the username and password entered are correct, the user may be required to enter a one-time password sent to the registered mobile number or email address. They may have an application on their mobile phone that generates a readable code only at a particular time. This next step means that even if the attacker gets hold of the password, they have to wake the user's phone or get their hands on the specific app to log in.

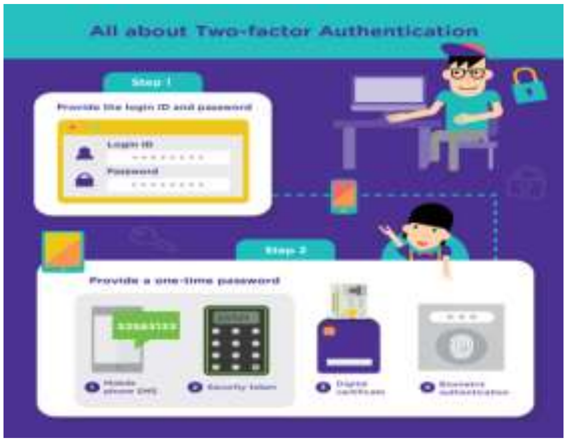


Figure 4: Definition of Two-Factor Authentication

a) Types of Two-Factor Authentication

2FA is not a single process but a set of different options in security and usability. One of the most popular methods is OTP, which can be implemented via SMS, email, or an authenticator application. Using the SMP regime of OTPs can be easy and convenient for a user. They are also exposed to the risk of SIM swapping, where a hacker controls their phone number. There are two types of two-factor codes such as bank apps and generators like Google or Microsoft Authenticator. These are believed to be more secure because they have genealogical passcodes.

Another common form of 2FA is using applications' physical tokens, usually as key fobs that produce one-time codes or use NFC to verify users. Such tokens like YubiKey provide strong security and are usually used in the corporate world (Haynes, 2009). Another type of 2FA is biometric authentication, which embraces fingerprint examples or face contour. Although considered highly secure, biometric methods are often expensive to adopt and might now and then experience some elements of flaw. Push-based authentication is becoming one of the most common forms of 2FA since it makes the authentication process much easier. In this one, a notification is triggered on the user's mobile device requesting the user to either accept or decline a login attempt. It removes the burden of coding entry and offers both security and convenience over having to type in the codes.

b) Benefits of Two-Factor Authentication

The benefits of 2FA are apparent through various dimensions and can be regarded as a critical tool for credit unions and other affiliated financial institutions. It is useful in enhancing security as an additional barrier must be breached. Even if the attacker gets through the user's password, he cannot access such an account without the second factor of a two-step authentic activation code. This added layer of protection prevents many hackers, as it raises the work's difficulty penetrating a system. 2FA also prevents general attacks like phishing, where users are deceived into typing their credentials. With 2FA, what cybercriminals steal, namely passwords, will not be sufficient to allow them entry because the second factor is usually different and would not fall into the hands of the phisher. 2FA reduces risks connected with stolen passwords since the attacker cannot log in even with stolen username and password credentials.

2FA is useful regarding the nature and proportionate risk levels that allow credit unions to meet the requirements of legal norms to protect financial data. Techniques like the Payment Card Industry Data Security Standard (PCI DSS) and the direction from the National Credit Union Administration (NCUA) frequently require multi-factor authentication as their safety standards (Betz, 2016). Thus, by adopting 2FA, the requirements for ITAR compliance are met, and, in addition, members' data protection is proven to be an organization's priority. In addition, 2FA increases the trust among members because it proves an organization's commitment to security. When security protocols like 2FA are displayed, credit union members are more likely to feel secure about their information and money. All this translates to better member relationships and a competitive advantage in the financial services market.

c) Limitations of Two-Factor Authentication

The following are the disadvantages of using 2FA, even if it is supposed to have many advantages. There is a limit, for example, the negative reaction of users who do not understand new types of authentication. Other users may prefer this extra step to begin with, so they can be discouraged or lose interest fast as they feel the process is tedious. Financial institutions must resolve these issues by adjusting user-friendly 2FA solutions and offering guidelines about their utilization (Cutshaw, 2015). Some technical factors are bound to manifest themselves while implementing 2FA. Adopting 2FA can be a complex process mainly because of integrating the systems, especially when the organization has outdated systems. Also, all the most used 2FA methods operate over mobile devices, raising risks connected with loss, theft, or failure. Such situations must have contingency measures, such as the backup forms of authentication at the institutions. Even 2FA has flaws, as it is contorted and easily hacked. More advanced crooks can easily defeat 2FA through SIM-swapping, social engineering, or session hijacking. Therefore, other layers of security features, such as firewalls, encryption, and monitoring, must augment 2FA.

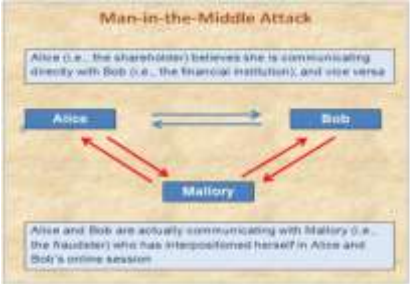

Man-in-the-Middle Attack
Alice (i.e., the shareholder) believes she is communicating directly with Bob (i.e., the financial institution), and vice versa
Alice
Bob
Mallory
Alice and Bob are actually communicating with Mallory (i.e., the fraudster) who has interpositioned herself in Alice and Bob's online session

Figure 5: Drawbacks of 2F Authentication

Two-factor authentication is a key application in increasing security for organizations such as credit unions and financial firms, as it demands two separate authentication methods. The possibility of a compromised account lowers offering and protection from easily exploitable attacks such as phishing and credential harvesting. Like all security features, 2FA is not without its challenges, but the benefits far outweigh the challenges, and that is why 2FA is critical to security. In light of the ongoing growth of various cyber threats, integrating 2FA is an effective step in financial data safety and in developing the necessary level of trust among members.

3. Case Study: Genisys Credit Union's 2FA Implementation

A prominent financial institution, Genisys Credit Union, pursued an initiative to enhance its cybersecurity systems due to escalating threats. When dealing with its members' data and banking, the organization realized a need to enhance security measures against intrusion. Among the measures was the introduction of two-factor authentication (2FA) to a range of internal corporate systems. This paper describes Genisys credit union's process of adopting 2FA, its reasoning, and results with another credit union in mind in case other credit unions wish to improve their security measures.

a) Background and Challenges

Genisys Credit Union has been established as a member-oriented credit union that provides individuals with all the necessary credit products and services. As with many credit unions, it mainly experienced increased levels of threat activity, higher attempt rates, highly developed phishing campaigns, and possible data loss incidents (Sullivan, 2014). These threats worsened when organizations only used single factors to authenticate users. A password was all that was needed.

As ordinary security features, passwords were no longer reliable assets to fortify the organization's security. At first, they were exposed to phishing attacks, brute force attempts, and account impersonation due to growing concerns about the security of their members' information and the law's requirements in terms of data protection. Genisys realized that it required a more secure authentication mode.

b) Rationale for Adopting Two-Factor Authentication

Genisys implemented 2FA to achieve several important objectives, as explained below. First, Genisys sought to minimize the chances of hackers attacking its networks or obtaining unauthorized access to its valuable information. As implemented, 2FA would add an extra layer of security in that even if the password becomes compromised, access would still need a second factor. Secondly, Genisys implemented 2FA to meet local regulatory requirements, including the PCI DSS and some of the advisories provided by the NCUA. These frameworks call for strong authentication, particularly where the information processed is financial, and Genisys's implementation sought to align with acceptable standards.

Figure 6: Minimizing Attacks with 2F Authentication

The credit union aimed to increase members' and employees' trust in the organization's cybersecurity practices. Because of the rising rates of cybercrimes, measures such as 2FA are perceived to be very effective in protecting the data, giving a positive perception to clients and other stakeholders.

c) Implementation Process

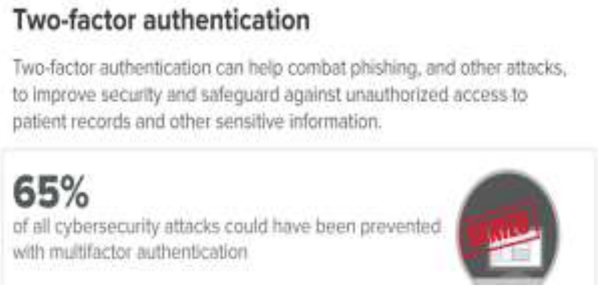
To safeguard 2FA, Genisys Credit Union's management adopted a systematic approach to deploying second-factor authentication, relying on SCEP protocols compatible with industry-adopted encryption patterns. The initial study involved assessing the status of existing systems to identify weak points that would prompt the institution to adopt appropriate 2FA (Lane et al., 2010). After researching the best approach for 2FA, Genisys settled on app-based authentication and SMS-based one-time passcodes (OTPs) as the go-to options. App-based authentication provided a secure means of creating the code on the device itself, unlike SMS-based OTP, which was the only acceptable option to some employees who did not have smartphones.

The next step was implementation, where Genisys's IT department had to coordinate with other third-party suppliers to integrate the system with existing systems. For the 2FA rollout, the team targeted systems containing critical information people crossed for, like employee interfaces accessing their personal data and financial processes involving money transfers. A major strategy was to subject the system to extensive user emulation to check for and rectify early symptoms of technical problems once implemented. One strategy used during the implementation process was employee training. To assuage such concerns about Genisys's new 2FA system, the company developed training programs to ensure all employees were aware of it. Effective communication highlighted the importance of 2FA and how to use it effectively.

Further, Genisys developed means for reaching out to employees throughout the change process to help, thus making the whole rolling-out process effective.

d) Outcomes and Benefits

This research showed that applying the 2FA system also brought meaningful outcomes to Genisys Credit Union. The most obvious change observed was that the number of failed attempts to gain unauthorized access to the system also decreased. In cases where the passwords were breached, the second level of Authentication minimized the chances of the attackers pinning down the organization's internal network. Another major achievement was enhanced regulatory compliance, which enabled the firm to achieve perfect compliance with the various regulatory benchmarks. Genisys achieved compliance with the key security frameworks when adopting 2FA and thereby eliminated the risk of penalties in the form of fines. This success also proved the institution's readiness to protect its member data, improving its stand within the financial market.



Two-factor authentication

Two-factor authentication can help combat phishing, and other attacks, to improve security and safeguard against unauthorized access to patient records and other sensitive information.

65%

of all cybersecurity attacks could have been prevented with multifactor authentication

Figure 7: Minimizing Cyberattacks with 2F Authentication

2FA improved employee and member confidence. Regarding the security measures, workers noticed a positive change. In turn, the members were also glad that the credit union took extra precautions to safeguard their information. This has helped foster better relations between Genisys and its stakeholders, supporting the institution's member-centric tactics. The implementation process provided a starting point for subsequent security projects (Carman et al., 2000). Genisys ensured all its systems were stronger and ready to advance to higher security measures in the client organization by developing a strong 2FA framework for protection against ever-rising cyber risks.

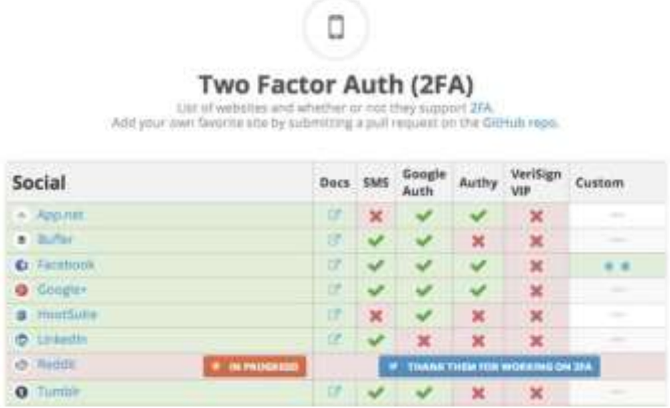
e) Lessons Learned and Broader Implications

The experience of Genisys Credit Union and its positive outcome has important implications for other credit unions and financial organizations that plan 2FA implementation. Technology transitions should be approached with caution, and there is a need for careful selection and implementation of the appropriate 2FA products. Institutions need to assess the particular requirements for security and consider user expectations to achieve the maximum effect.

No-less-important is the factor that relates to the condition that an employee must undertake the training and receive support while working on the implementation. To avoid developing resistance to change, more communication and guided experiences are useful to make transitions that are necessary for security more effective (Kotter et al., 2012). The Genisys solution demonstrates exactly how a 2FA solution can turn the tide and improve cybersecurity and compliance. As the dangers of cyber attacks progress, credit unions need to implement countermeasures such as 2FA to ensure the security of the systems and members' data.

4. Steps to Implement 2FA in Credit Union Systems

With 2FA technology, credit union system designers must factor in planning, implementation, and continuous support. Since financial data forms sensitive information and cyber threats emerge, 2FA has emerged as critical in protecting these critical systems, not forgetting to fulfill regulatory compliances. The following is a step-by-step guide on how to choose, deploy, and evaluate 2FA on credit union systems with consideration of the key factors at each step (Laux et al., 2011).



Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.
Add your own favorite site by submitting a pull request on the GitHub repo.

Social	Docs	SMS	Google Auth	Authy	VeriSign VIP	Custom
App.net	↗	✗	✓	✓	✗	—
Buffer	↗	✓	✓	✗	✗	—
Facebook	↗	✓	✓	✓	✗	• •
Google+	↗	✓	✓	✓	✗	—
HootSuite	↗	✗	✓	✗	✗	—
LinkedIn	↗	✓	✗	✗	✗	—
Reddit IN PROGRESS		THANK THEM FOR WORKING ON 2FA				
Tumblr	↗	✓	✓	✗	✗	—

Figure 8: Planning and Implementing Two-Factor Authentication

a) **Step 1: Evaluate Security Needs**

The initial activity of 2FA is identifying the security threats currently at play in the credit union system. This includes establishing possible weaknesses of the current authentication style and evaluating the risk aspects of cyber threats. A good risk analysis must be performed to identify risks, including the organization using only one form of identification or easily falling prey to phishing. The data include member accounts, employee access, and financial transaction platforms that credit unions must safeguard. Consultants or cybersecurity experts must be enlisted to highlight or ascertain the most relevant areas and understand the probable implications of a breach. They also evaluate components relating to regulatory bodies' current and past requirements. Frameworks such as the Payment Card Industry Data Security Standard (PCI DSS) and regulation from the National Credit Union Administration (NCUA) call for multi-factor authentication because it is a strong security measure that is not flawed (Smedinghoff, 2008). Knowledge of these requirements will ensure that the 2FA implementation complies with compliance laws and regulations, hence no fines or penalties.

b) **Step 2: Choose the Right 2FA Solution**

Selecting the proper 2FA method is one of the most strategic actions that define the project's future success. Credit unions have to weigh various factors related to the security offered, ease of use, cost, and suitability for scaling. It is important to try to balance a strong level of protection and the ease of use of the solutions by the employees and members. When it comes to implementing 2FA, there are several available forms. By sending a code to the user's end device, Google or Microsoft Authenticator is more secure than app-based authentication. Examples of hardware tokens include YubiKey, which is very secure but could also incur higher costs and challenges regarding distribution. Given the SIM-swapping attacks, organizations use easy-to-send tokens such as one-time passcodes (OTPs) via the short messaging system (SMS). Security at a higher level could be embraced by using features such as fingerprints or facial identification, but this comes hand in hand with many costs regarding technology and hardware (Bennett et al., 2013). These options should be measured against credit unions' needs and competencies. If the users differ, the facilities can use both methods depending on the prevailing circumstances and the user's interest.

For instance, the fundamentally preferred approach is app-based authentication, and the fallback is SMS-based OTPs for employees who do not own a smartphone.

c) Step 3: Design a Comprehensive Implementation Plan

When a decision for a 2FA solution is made, it should follow all four steps. This plan has to define which systems and user groups, when, how, and with what resources, and who will act. Multi-stakeholder cooperation is critical for IT, security, and vendors to address all significant implementation aspects. In this stage, credit unions need to ensure that the soon-to-be-adopted 2FA solution will not have any issues in terms of integration with their current systems. Integration may also involve retrofitting your current structure or buying new systems and tools. Much attention should be paid to testing since many technical problems may occur during implementation. This means the tests must closely resemble the actual operation so that it is possible to determine the readiness of the 2FA system to prevent login attempts using the hacked passwords. However, one must also prepare for some obstacles, like some employees or members might reject the 2FA, claiming it is a bother. Expecting such challenges and developing a plan for handling them is helpful, as is making the interfaces more user-friendly, among other things (Wilson, 2009).

d) Step 4: Deploy 2FA in Phases

This paper has shown that there is merit in adopting a phased approach to deploying 2FA to credit union systems. This approach enables the organization to introduce a pilot before scaling the entire system, allowing researchers to scrutinize its effectiveness. The pilot can target specific users and include only IT employees and persons authorized to deal with strict confidentiality data. After implementing the pilot program, 2FA will be easy to scale to other systems or users. It should be targeted towards areas of higher risk exposure, including member account portals and online banking. This way of functioning also ensures that problems are solved before other users are equally affected by an outbreak of problems. Engagement with such users should be communicated clearly during the deployment process. End-users should know why 2FA is being introduced, how it works, and what it brings to the organization and them. This segment means that various instructions and several frequently asked questions should be given to support the users' confidence in embracing the new system (Veryzer et al., 2005).

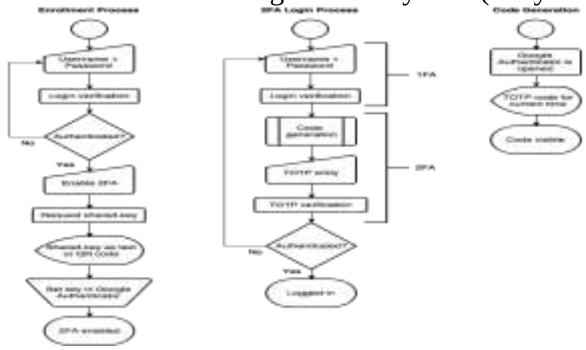


Figure 9: Phases of Two-Factor Authentication

e) Step 5: Train Employees and Educate Members

Another important factor that causes or contributes to 2FA implementation is user education (De Cristofaro et al., 2013). In addition, specific training for reasonable suspicion should be undertaken to ensure the employees understand the new system and concerns. The user training should involve explaining such processes as 2FA, the selected types of authentication methods, and what to do in case some complications occur, such as losing a device or encountering difficulties while logging into a specific account. While credit union members realize the value proposition of educational campaigns, specifically where 2FA optimizes security, 2FA directions must be clear without confusing terms and give a brief process of setting 2FA up. Communication through emails, instructional videos, and website tutorials asserts members that they have embraced the change. Collecting feedback from the users can also enhance the 2FA experience.

f) Step 6: Monitor and Maintain the System

Controlling 2FA is not only a one-time job. It is a continuous process to guarantee its efficiency. Periodic audits of the system are recommended to assess its efficiency in terms of the outcome of the threats and risks it poses and to establish new threats within the system. Cybersecurity is changing dynamically, and credit unions cannot sleep, hoping the problem will pass (Pelton et al., 2015). Standard monitoring devices can be applied to different logins and indicate at least frequent failed attempts and access to resources from unfamiliar IP addresses. Such tools can help credit unions to act as soon as possible in case of threats and prevent breaches. The 2FA system requires frequent updates and patching to maintain reliability. Software releases may fix known security threats or improve interaction capabilities to protect the structure from new threats. Credit unions must also budget for routine end-user training to refresh workers' and members' knowledge of the system and new tips.

Figure 10: Regular Monitoring of 2F Authentication

g) Step 7: Plan for Contingencies

Any system has weaknesses, and it is crucial that credit unions expect that there will be circumstances in which 2FA will become problematic. For instance, users may misplace their device or software with a token, which causes an error. Some measures are implemented as a precaution to enable users to get back into their accounts without necessarily exposing them to more sensitive information. These are situations that help desks, and IT departments should have mechanisms for dealing with as soon as possible. Credit unions may also devise policies for ascertaining the identity of customers on other occasions of merited restrictions, for example, before resetting the adopted authentications.

Incorporation of two-factor authentication in credit union systems takes a longer process that entails evaluation, design, deployment, and testing (Lott et al., 2015). Thus, credit unions can improve security concerning threats and conform to regulation rules by crediting and evaluating security threats, adopting proper decisions, and implementing 2FA step by step. Adopting new technologies, changing employee behavior, imitating the transformation, and providing members with training and knowledge are required. Constant supervision and course-of-action planning also ensure the sustainability of the system in the long run. When done correctly, credit unions can easily uphold the interests of their members, meet valuable financial goals, and decrease the chances of a cyber breach when handling important members' data. With threats to the cyber world on the rise, measures such as 2FA are necessary preventative mechanisms used to protect the financial sector in the digital realm.

5. Benefits and Limitations of 2FA

Two-factor authentication or two-step verification 2FA is common in organizations' information security strategies. This is more so for credit unions, which deal with members' financial and identification details, which cyber criminals regularly magnetize. 2FA has many benefits in increasing security and trust in systems. However, 2FA has drawbacks. For credit unions, the benefits and drawbacks of 2FA are discussed above to assist in coming up with concrete decisions about employing this security method in their general security frameworks.

a) Benefits of Two-Factor Authentication

The major advantage of 2FA is that it can help to enhance security significantly by introducing an additional factor to the actual authentication process. Password-only authentication has been common for many years, but it has numerous weaknesses and is easily compromised via phishing, brute force, and other methods (Elftmann, 2006). 2FA avoids these issues by offering a second authentication plane with an OTP code, transmission identification device, or biometric data. Even if an attacker gets a hold of a user's password, they cannot log into the account without the second factor, hence minimizing the level of vulnerability in instance an attacker gains a hold of the password.

Two-factor authentication is useful against phishing attacks and is one of the most popular cyber threats. Phishing schemes are meant to deceive people into offering their username and password to a fake entity claiming to be a genuine site, especially social networking sites. When 2FA is implemented, a stolen password is not enough to allow the attacker in, meaning many phishing attempts fail. This enhanced protection is specifically important in credit unions since one breach can encompass significant data of a financial nature. The other advantage of using 2FA is its usefulness in fulfilling regulatory requirements. Financial institutions have precise requirements to protect data, such as the Payment Card Industry Data Security Standard (PCI DSS) and the National Credit Union Administration (NCUA). These frameworks require the application of MFA to protect critical systems and member information. If credit unions perform 2FA, they can prove that they fulfill these criteria,s and penalties under their focus on cybersecurity.

Figure 11: Does 2F Authentication Prevent Phishing?

2FA also helps boost member trust and confidence. The users will feel safe transacting with the organization. Its members expect credit unions to protect their data and strengthen it by implementing the 2FA to counter cyber threats. This increased trust is good because the relationships between individual members and the institution are enhanced. In the process, the institution will have a more sought-after security of acting as a reliable financial partner. Employees also get the nobility of having their accounts and work systems safeguarded, enhancing the organization's security. 2FA can be used flexibly and at any company's size. There is nothing specific about the choice of 2FA methods that credit unions should implement. They can provide such methods as app-based, SMS-based OTP, tokens, and biometrics for the users. This flexibility helps institutions to use the solutions that will ensure the insecurity and convenience of the users based on the different cases that will come across and different users.

b) Limitations of Two-Factor Authentication

The numeric methods of 2FA are far from perfect, and they still can have several drawbacks. Such an important impediment to the incident plan is user resistance. Some users might even feel it is an additional step while logging in. They may not know what the other options are all about. This often creates resistance that makes it hard to adopt the application, causing much frustration to the end users when employees already use it. However, there are instances where they struggle to use the application due to the challenges that are associated with it. To overcome these issues, financial institutions are responsible for giving clear instructions, training, and support so that users have a smooth run-in.

Time could also be a weakness for the 2FA implementation, depending on the organizational credit union's budget (Kuhmonen, 2017). 2FA adoption constitutes an initial cost in the form of hardware, software, and integration within the current setup. Also, continuous maintenance, updating, and technical support can increase the costs. Although the benefits of 2FA overcome these costs in larger institutions, implementing this technique could be costly to some small institutions. Technical issues may also be experienced while deploying and implementing 2FA systems. The integrations needed with older systems imply massive updates or major replacements, which implies further complication and cost. Moreover, using mobile devices or a hardware token to authenticate all the most popular 2FA methods adds some risks. For instance, users may forget their devices or technical problems may occur that affect the main systems' operation. To counter these scenarios, institutions must develop contingency measures, such as backup forms of authentication.

2FA imposes considerable security enhancements, but it is not vulnerable to anticipating cyber threats. More advanced hackers may hack the system by intercepting the OTPs by applying SIM-swapping or using other trickery methods to connect the other factor of authorization from the user. Also, session hijacking or an attack known as the man in the middle can pose as a genuine user in the case of 2FA. Such risks highlight that utilizing a 2FA system should be considered just as the first line of defense against cyber threats. Another constraint of 2FA is that it depends on the user's compliance. The system becomes compromised when the second factor is not properly configured or when users infrequently engage it. For instance, if users decide to deactivate their 2FA accounts for one or two reasons, such as convenience or neglect to update their details, such as their phone numbers or email addresses, the system may not work well. This means that all such systems' users must be educated continuously, while security policies must be enforced properly to encourage the consistent utilization of 2FA.

c) Striking a Balance: Maximizing 2FA's Effectiveness.

Credit unions must demonstrate three best practices for using 2FA to fully harness its advantages while mitigating its disadvantages (Tirman, 2016). 2FA techniques, such as push notifications or biometric authentication, should be chosen as convenient and easy to use. Ensuring a solid framework for training both the employees and the members provides a foundation for appreciation of the training framework. 2FA is a tool that is necessary for the protection of accounts.

Figure 12: Making 2FA More Effective

Cost issues can be dealt with by ranking systems and user groups according to the level of risk they present, thus implementing them in phases at differing time intervals. Deployment of versions on 2FA solutions hosted in the cloud can also benefit the company by cutting infrastructure expenses further. Finally, using 2FA with firewalls, encryption, and monitoring, among others, creates a network that tackles a range of go-beyond authentication. Periodic reviews and updates are important factors in implementing 2FA. Cyber threats are constantly adapting, and credit unions need to constantly solve new problems, fix newly discovered holes, and adapt to new strategies. Users need to be reminded about new threats and how to avoid them, and this will help them remain proactive in their security.

The application of two-factor authentication is an excellent tool for improving credit unions' security and protecting against the credit union's intrusion, phishing, and regulatory noncompliance. This tool is beneficial to financial institutions because it can establish member trust and enhance security levels. Nonetheless, 2FA's disadvantages mean that user adoption remains a problem, is expensive, and requires technical expertise to implement. This shows that security professionals must plan meticulously and pursue a layered approach to security. With these obstacles regarding 2FA's optimization, credit unions can use it to protect their systems and the loyalty of their members in an environment that becomes more digital but dangerous (Muraleedharan, 2014).

6. Best Practices for Securing Credit Union Systems

Protecting credit union systems has become an important task in the contemporary world, especially considering that hackers continually attack the institutions. The ever-increasing threat means that credit unions must employ stringent and complex security solutions to safeguard the information effectively, meet the legal and regulatory necessities, and reassure members and clients. Two-factor authentication is widely popular but is one of many steps to create a fully-fledged security shield. Credit unions can apply the following recommendations to strengthen their security measures for the organizations.

Table 2: Strategies for Protection against Cyber Threats

Practice	Description	Example	Benefit
Multi-Layered Security	Use firewalls, encryption, and segmentation.	Separate member accounts systems	Reduces risks from unauthorized access.
Strong Access Controls	Restrict access based on roles and privilege levels.	Enforce password policies	Limits data exposure to unauthorized users.

Employee & Member Education	Train users on recognizing cyber threats like phishing.	Conduct quarterly training	Builds awareness and reduces vulnerability.
Incident Response Planning	Establish plans for identifying and containing breaches.	Simulate breach scenarios	Ensures quick and effective threat mitigation.

a) Adopt a Multi-Layered Security Approach

Having 2FA is already protective but should not be the only form of protection (Wang et al., 2014). Cybersecurity, when undertaken at different levels, involves the use of several layers, which in turn offers a fight against the vast kinds of threats. To avoid unauthorized access to their networks, credit unions should ensure they have firewalls that keep out unwelcome users. They should also have intrusion detection systems to alert them of a possible breach and encryption to secure the data when it is transferred and stored.

Another important practice is network segmentation, which means splitting the IT infrastructure into separate parts. This reduces the prospects of disruption by an attacker when a person gains access to the network, as access to other areas of the network is limited. For example, decentralizing member account systems from general administrative systems means that a compromise in one area is not a compromise of the entire organization. It is important to update software and systems as frequently as possible. This is a seat of virtual attackers who take careless steps of the smallest size to find new doors cracking owing to the shortcomings of unpatched software. Credit unions should also implement endpoint protection solutions for devices like workstations, laptops, and mobile devices for employees and members.

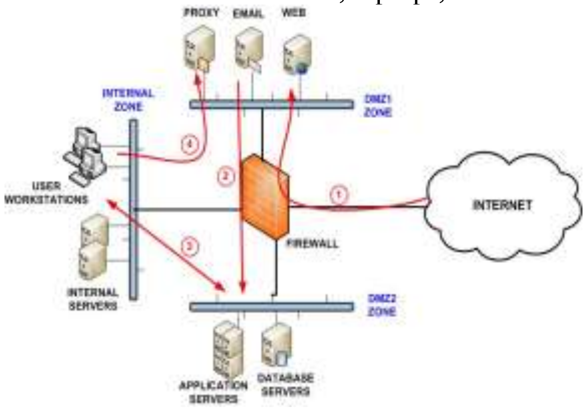


Figure 13: Perks of Network Segmentation

b) Implement Strong Access Controls

Controlling access to such systems and data is a basic principle of preventing the access of such unauthorized individuals. Credit unions should learn the principle of least privilege (PoLP), where an employee has only the amount of access needed to perform a given task. This minimizes the individuals who have access to the information, and in the unlikely event some attacker gains access, then the harm that can be caused is limited.

Another efficient method is role-based access control RBAC. Since RBAC assigns permissions in accordance with roles, this approach helps simplify the work of managing permissions for system users (Chakraborty et al., 2006). Changes to access controls must be made, and they should be done in a standard format, more so when roles are changed or employees have left the company entirely. Other measures that should be adopted to complement 2FA include the institution's need for strong password policies.

Employees and members should be compelled to use difficult, lengthy passwords and, whenever possible, encouraged to change them often. Credit unions can boost password security to improve security and enforce good password practices with the help of password managers.

c) Educate Employees and Members on Cybersecurity

Employees combine with the hackers to contribute equally to the threat, making awareness important. Credit unions must ensure that all employees and members know about threats like phishing, social engineering, and malware, how to identify them, and what to do about them. Employees should undergo training at least every quarter to be aware of issues like recognition of phishing emails, protection and security of authentication, and data protection measures. Fake security-related emails can be useful in evaluating the level of sophistication of the employees and the frequency at which the employees fall prey to particular types of fake emails, like phishing emails. This can help further train the employees in the areas in which they are weak.

Members should be guided by the promotion of the understanding amongst its members on educational programs and measures on individual protection from cyber threats (Anderson et al., 2010). A section on the credit union's website with instructional videos, handouts, tips, and frequently asked questions about safety measures, including 2FA, password creation, and scams such as phishing, can also be helpful. Members must be informed to avoid losing their accounts and minimize the chances of the success of the credit union attack.

d) Conduct Regular Security Audits and Risk Assessments

Credit unions must regularly perform security audits and risk analyses to counteract new emerging threats. Security audits decide the relevancy of current security measures and standards, existing risks, and compliance with current legislation. Such audits should be broad and general, comprising the servers, networks, applications, and devices related to IT.

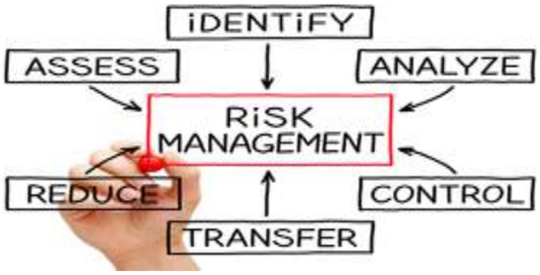


Figure 14: Regular Risk Assessment

Risk assessments are even more advanced than analyzing threats and their implications for the firm. Potential threats can then be grouped according to their level of risk, and measures can be put in place to ensure that credit unions tackle these issues individually. For instance, member-related data or an organization's financial information ought to be granted extra consideration and safeguarding. Outsourcing cybersecurity or getting an outside auditor can give an independent assessment of the credit union's position and suggestions of what needs to be done to enhance security. Also, contrary to typical security assessments, penetration testing can mimic real-world attacks for weak spots to discover and evaluate the company's response.

e) Develop a Robust Incident Response Plan

It is impossible to protect any system against cyber risks completely (Subashini et al., 2011). There is no option for credit unions to create an incident response plan to deal with such breaches if they are to operate efficiently. This plan describes what should be done in the case of a security and management breach to ensure the harm is controlled and the situation is resolved as soon as possible. The essential elements of an incident response plan are how to identify and contain the breach, how to evaluate the breach, and which parties should be informed. Credit unions also have a legal and regulatory obligation regarding breach notification, whereby they have to report breaches to the regulators and notify members.

Communication plans developed during the response processes should be reviewed periodically using tabletop and simulations to acquaint employees with the roles and responsibilities expected of them. These tests can uncover weaknesses in the plan and practice inter-team relations during a true event.

f) Leverage Advanced Security Technologies

There are also opportunities to use new technologies to improve the systems security of Credit unions. For instance, in synthesis with AI and ML, actions such as identifying and mitigating anomalous activity in real time enhance the organization's capability to ward off cyber attacks. These threat intelligence platforms based on Artificial Intelligence will be able to assess the various forms of threats and likely attacks. Password-less methods include using fingerprints or touch IDs, which are even more secure than 2FA, which most credit unions may consider integrating. Although these technologies may entail higher initial costs, their application will yield improved security in the long run and user convenience.

Hacking credit union systems is possible, but proper protection requires better policies that are hard to get or hack. Credit unions understand that 2FA, strong desktop and employee access controls, constant training and education of employees and members. Additionally, reviewing security procedures systematically and implementing some of the most effective advanced technologies are key approaches that must be incorporated to create a tough line of defense against cyber attacks. In addition to the best practices of the applied domain, including the principle of least privilege, network segmentation, the identification of possible incidents, and response planning. The systems remain progressive in the face of constantly evolving threats. Safeguarding personal information is key to implementing information security measures, developing members' confidence, and enhancing the credit union's image as a secure financial organization (Council et al., 2006). With the ever-increasing threats of cyber threats, adopting the above best practices is crucial for preparing the credit union's future operations.

Conclusion

The world is now interconnected. Ensuring the security of the members of financial institutions such as credit unions is very important due to the protection of personal and confidential data. This guide has provided an understanding of issues that credit unions encounter, the advantages and disadvantages of 2FA, and the processes required to put it into practice. The tool's applicability is best illustrated through the case of Genisys Credit Union, which adopted Two-Factor Authentication to secure its applications. It becomes clear that 2FA is a must-have tool in the arsenal of any financial institution that seeks to protect its operations and systems from continuously evolving threats. Two-factor authentication rectifies several deficiencies that exist in first-generation simple single-factor systems. With an extra identification step, 2FA greatly decreases the threat level even when a user's credentials have been stolen. For credit unions, where credibility is at the highest risk since data protects people's financial information, 2FA is critical. It also complies with high-profile compliance standards like the PCI DSS and the NCUA compliance standards that are critical to financial organizations.

The Genisys Credit Union is an excellent example of why more contemporary safety measures must be applied. Implementing 2FA solved two problems at once for Genisys, namely improved cybersecurity and increased trust among employees. This approach should inspire other credit unions and can gradually be used when properly planned and implemented in phases accompanied by constant evaluation. The results described in the paper as having a positive impact on Genisys, including a decrease in the number of unauthorized attempts to access it and enhanced compliance, prove that regular cybersecurity measures can be effective. 2FA is not flawless, and these are the limitations of the technique. It can, nevertheless, encounter attendant difficulties such as user resistance, technical issues, and high costs. To surmount the named challenges, there is a need to empower the users through employee and membership education on the significance of 2FA and its implementation methods. However, 2FA should be a part of layered security, encompassing firewalls, encryption, and periodic security audits as measures that comprehensively contain threats.

A conclusion can be made regarding credit union security, which has to do with credit unions' innovation and flexibility. When adjusting to continuously changing cyber threats, financial institutions must turn to modern technologies like AI-based threat identification and passwordless authentication. Therefore, preventing cyber threats avoids risks leading to the leakage of members' information and failure to meet regulatory standards and member expectations. This guide is a rallying cry and a plan of action for credit unions and other similarly situated institutions. Using 2FA is not just the right thing to do. It is required in today's threat environment. The time to act is now. Credit unions must invest in reliable security measures, such as 2FA and the culture of information security, to protect members' information and guarantee the stability and effectiveness of credit unions' operations in the following years. The approach that calls for two-factor authentication significantly enhances credit union system protection. The benefits override the limitations put on 2FA, making it a critical element in modern cybersecurity measures. In light of the outcomes of Genisys Credit Union's case and the credit union's desire to formalize security action plans, credit unions can embrace the future of the digital age and mitigate the threats to their members to improve the credibility of the services they provide.

References;

1. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS quarterly, 613-643.
2. Bair, S. C. (2010). Improving access to the US banking system among recent Latin American immigrants.
3. Bennett, C. J., & Lyon, D. (2013). Playing the identity card: Surveillance, security and identification in global perspective. Routledge.
4. Betz, L. (2016). An analysis of the relationship between security information technology enhancements and computer security breaches and incidents.
5. Carman, D. W., Kruus, P. S., & Matt, B. J. (2000). Constraints and approaches for distributed sensor network security (final). DARPA project report,(cryptographic technologies group, trusted information system, NAI labs), 1(1), 1-39.
6. Carmichael, J., & Pomerleano, M. (2002). The development and regulation of non-bank financial institutions. World Bank Publications.
7. Chakraborty, S., & Ray, I. (2006, June). TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In Proceedings of the eleventh ACM symposium on Access control models and technologies (pp. 49-58).
8. Council, F. F. I. E. (2005). Authentication in an internet banking environment. Retrieved June, 28, 2006.
9. Cutshaw, J. (2015). Online authentication challenges for financial institutions in a complex digital era (Master's thesis, Utica College).

10. De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. arXiv preprint arXiv:1309.5344.
11. Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. R. (2014). On the (in) security of mobile two-factor authentication. In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18 (pp. 365-383). Springer Berlin Heidelberg.
12. Elftmann, P. (2006). Secure alternatives to password-based authentication mechanisms. Lab. for Dependable Distributed Systems, RWTH Aachen Univ.
13. Goddard, J., McKillop, D., & Wilson, J. O. (2008). The diversification and financial performance of US credit unions. Journal of banking & finance, 32(9), 1836-1849.
14. Haynes, B. (2009). A Multi-factor Authentication Provider for the DotNetNuke® Open-Source Content Management Web Application Framework. USA: Harvard.
15. Jakobsson, M. (Ed.). (2012). The death of the internet. John Wiley & Sons.
16. Kotter, J. P., & Cohen, D. S. (2012). The heart of change: Real-life stories of how people change their organizations. Harvard Business Press.
17. Kowalski, K. (2011, October). Multi-factored Verification of Students in Online Testing. In E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (pp. 706-711). Association for the Advancement of Computing in Education (AACE).
18. Kuhmonen, S. (2017). One-Time Password Implementation for Two-Factor Authentication.
19. Lane, M., & Marie, M. (2010). The adoption of single sign-on and multifactor authentication in organisations–a critical evaluation using toe framework. Information in Motion, 7, 161.
20. Laux, D., Luse, A., Mennecke, B., & Townsend, A. M. (2011). Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems. Journal of Organizational Computing and Electronic Commerce, 21(3), 221-245.
21. Lott, D., & Expert, P. R. (2015). Improving customer authentication. Federal Reserve Bank of Atlanta: Atlanta, GA, USA.
22. Mohsin, J. K., Han, L., Hammoudeh, M., & Hegarty, R. (2017, July). Two factor vs multi-factor, an authentication battle in mobile cloud computing environments. In Proceedings of the international conference on future networks and distributed systems (pp. 1-10).
23. Muraleedharan, D. (2014). Modern banking: theory and practice. PHI Learning Pvt. Ltd..
24. Pelton, J., & Singh, I. B. (2015). Digital defense: A cybersecurity primer. Springer.
25. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector (p. 25). United States Secret Service.
26. Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453-481.
27. Smedinghoff, T. J. (2008). Information security law: The emerging standard for corporate compliance. IT Governance Ltd.
28. Stanislav, M. (2015). Two-factor authentication (Vol. 4). IT Governance Ltd.
29. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
30. Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. Federal Reserve Bank of Kansas City, Economic Review, 99(3), 47-78.
31. Svetiev, Y., & Ottow, A. (2014). Financial supervision in the interstices between private and public law. European Review of Contract Law, 10(4), 496-544.
32. Tirman, V. J. (2016). The current state of mHealth applications and the need for improved regulatory guidelines to protect the privacy of patient health information. Alliant International University.

33. Veryzer, R. W., & Borja de Mozota, B. (2005). The impact of user-oriented design on new product development: An examination of fundamental relationships. Journal of product innovation management, 22(2), 128-143.
34. Wang, D., & Wang, P. (2014). On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Computer Networks, 73, 41-57.
35. Wilson, C. (2009). User experience re-mastered: your guide to getting the right design. Morgan Kaufmann.