Eliminating Password Woes: A Biometric Solution to Cyber Threats

Jayson Gochez

Old Dominion University

Entrepreneurship in Professional Studies

Akeyla Porcher

April 21, 2023

Introduction

The world is undergoing extraordinary technological developments, and as a result, many companies and organizations are becoming increasingly dependent on computers and their systems to function. There are numerous advantages to technical advancements since they make discovering, collecting, and sharing information much more effortless. However, as individuals' reliance on and use of technology increases, so do cyber threats (Park, 2021). Because most systems are run on devices that connect to the internet, these systems must stay secure. A strong password is the first line of defense against cyber threats, just like the first line of home security is a locked door. Most Organizations ensure password security by implementing some type of password policy, a set of rules that a person must follow for their passwords to be strong enough and survive cyber intruder attacks. Although password regulations were designed to be a solution, this set of rules presents several problems and vulnerabilities which can compromise users' accounts. Most data breaches occur due to weak passwords and human error. Manjares states, "81% of hacking-related breaches used stolen or weak passwords" (2021). Inadequate passwords constitute a significant issue because many businesses and organizations provide services required for society to operate or function properly. Because the community relies on those services, access to those systems falling into the wrong hands could have disastrous consequences and cause financial burdens to the organization and the user connected to them.

People want to be secure, but only at their convenience, which is a problem. In a study commissioned by the analytics software firm FICO (2018), researchers found that of 2,000 U.S. adults, 81 percent did not see a need for what they considered to be unnecessary security procedures, 47 percent said they were sick of having to answer endless security questions, and 64 percent are upset over having to create elaborate passwords that feature a mix of numbers,

symbols and capital letters. In that same survey, 71 percent think there are too many security measures nowadays. However, the bottom line is that without passwords, private data and information would be accessible to everyone, which would most certainly cause pandemonium.

This entrepreneur team has created a solution to eliminate password issues by creating an electronic I.D. that uses biometrics. Not only will the I.D. be used by employees to authenticate themselves into the networks, but also as an identification device for entry to the facilities. The ID will have a photo of the employee they must scan to enter the building. Once the employee arrives at their workstation, the user will scan the I.D. and fingerprint on the personal computer. The device will create a token to allow the user to access all their systems without having to type the password every time a system is accessed, similar to a single sign-on but using biometrics.

This method eliminates the need to store and create several passwords for each program which will also help eliminate human error. The token will only be available for 24 hours, and once the token has expired, the user will be required to follow the same steps to access their computer. This method will provide multiple layers of security for the user because it will be impossible for a cyber intruder to obtain the physical I.D. and the biometric fingerprint simultaneously. Companies can feel more confident in their security measures with this passwordless strategy, especially those storing confidential data, like government agencies and banking institutions requiring numerous protection levels. The following section of this document aims to go over more concrete reasons why password practices are becoming riskier. In addition, the literature will present additional material to demonstrate why our team innovation is the best option to correct password errors and provide a summary of the following steps for this innovation.

Why Are Passwords Becoming A Security Risk?

Password authentication is a cyber security method that has been around for decades now. It is a method that programmers have used since the creation of computer systems. According to MacInnis, this method of security was introduced in the year of 1961 (2017). The security method provided excellent security for many decades. However, hackers have continuously found new ways to bypass security control in recent years. This issue was not an alarming concern in the past because people did not rely so much on computers to run daily operations. However, now everything is connected to the internet, from card payments to industrial services, so it is crucial that all organizations keep their systems well protected.

In 2021, Israel announced a cyber-attack on one of its financial institutions which caused significant damage to the country's banking economy. The Iranian nuclear infrastructure was breached the same year (Amer, 2021). Many speculate that one of these attacks resulted from an account hack. Hackers are employing various tactics to compromise user credentials, which is becoming increasingly concerning. These cyber-attacks are not only starting to affect larger institutions but also have collateral damage on everyday citizens. Another cyber attack was reported to Israel's water and sanitation system, although they responded and fixed this issue almost immediately. If the problem had persisted, it would have affected many people and even resulted in water shortages (Amer, 2021). The United States experienced a similar attack last year when hackers halted the services for one of the most extensive fuel line supplies. Luckily the system was restored in a few days, but the issue could have been worse. If the denial of service had continued, it would have profoundly impacted many organizations' supply chains. Fuel is such an essential resource for many countries that it makes the nation vulnerable to other attacks of a similar nature.

Password Authentication Issues

A research study shows that "the problems with the use of alphanumeric passwords have been known for more than 20 years, but unfortunately, so far, we have made little progress" (Ives, Walsh, & Schneider, 2004). Password security is becoming less effective because of all the rules and regulations to create passwords, and the speed of new computers makes it easy for weak passwords to be cracked. Computer programs used for penetration testing can verify anywhere from 10,000 to 1 billion passwords per second; weak passwords can be cracked immediately or in up to two minutes (Grigas, 2022).

This issue not only happens to the average person but also to government officials. Many government employees still need to comply with password regulations set forth by the federal government. One study by Choong et al. (2014) found that U.S. employees must manage about nine passwords at work. While the average user has nine accounts, about 25 % of DOC employees have between 11 and 20 accounts they must manage at work. Of those surveyed, over one-third of participants feel overwhelmed by the password management system requirements enforced by government agencies.

Password policies are becoming overwhelming for any user, causing them to construct simple, easy-to-remember passwords because they must memorize a vast amount. Research shows that users consistently use simplistic, easily predictable practices when constructing and using passwords. This includes using meaningful words or personal dates that are easy to remember (Bishop & Klein, 1995). People are starting to resort to using basic words found in a dictionary (Vu, Bhargav & Proctor, 2003). These practices make passwords simpler to remember but compromise the security that passwords are intended to provide (Chaparro, 2006). Even if people use passwords with numbers and symbols, e.g., "h@m3" there is a particular attack called

a dictionary attack. This attack can crack this kind of password in about an hour. Dictionary attacks work with the assumption that users will use basic words, such as "password," "123abc," and "123456," or other predictable patterns, such as the previous example, "h@m3=home" (Bareckas, 2021).

Additionally, research shows that 68% of users make inadequate modifications to words when replacing their passwords. In most instances, they only change one character. For example, "password1" is changed to "password2," as explained before, this type of password is fragile. If a hacker cracks the password the first time, they will not have any issues performing the same attack (Hoonaker).

Most modern jobs require multiple systems, and for every system, the user has to create a complex password that contains a combination of characters, symbols, or numbers. Nowadays, some companies have already set policies for passwords to be 8 to 16 characters long. Most companies are updating these policies to align with the recommendations from the National Institute of Standards and Technology (2017). These rigid requirements make it difficult for the average user to memorize their passwords, so users usually resort to saving a password in their system or writing it on a Post-It note near their workstation, making security more vulnerable. If a cyber-criminal can penetrate the system for some reason, the passwords can be easily compromised and used for lateral moves within the networks. An employee writing passwords on paper poses an enormous threat to a company because that full paper may end up in the trash. In response, hackers dumpster-dive through that trash, searching for sensitive information and passwords (Games, 2022). This idea sounds ridiculous; however, it is a prevalent technique. Computers have evolved over the years; however, we continue to have the same security problems. We continue to use the same techniques to mitigate security concerns. Password

security strategies need to be entirely shifted-especially for larger organizations that hold sensitive information and provide essential services.

The world Without Passwords

Since password rules are becoming increasingly difficult to implement and continue to be a security risk due to human error, the method should be simplified. Our team created a product to eliminate the hassle of maintaining too many passwords. It feels surreal to imagine a world without the burden of juggling passwords, where staff members can settle into their workspace and launch the application of their choice. This invention eliminates the need for employees to input a password for every application they launch, meaning no more memorizing or writing down passwords to operate (Wyatt, 2016).

The device only consists of an electronic I.D. with a picture of the employee. Past research shows that smart cards have positive results over password security. Over a decade ago, the U.S. Department of Defense (DoD) was already aware of how common password-centric attacks were. As a response, the DoD replaced passwords with Common Access Cards (CAC) for all log-on to DoD computers and networks. Jeremy Grant (2011) states that the DoD's network intrusions dropped almost 46 percent immediately. Around that same time, President Barack Obama signed the National Strategy for Trusted Identities in Cyberspace (NSTIC), which aimed to facilitate the transition away from passwords towards online identification technologies that are secure and trusted, such as the one used at the DoD (Grant, 2011). The results from this research clearly show how effective an I.D. card is. Hence, the innovation includes a physical I.D. as one of the features.

Another research shows a similar product that uses an I.D. to create multiple levels of security; however, the identification card still requires a password. One of the most commonly

used two-factor user authentication mechanisms is based on a smart-card and password. The issue is that the user must have a smart-card *and* know the password to gain access to the server (Yang, 2008). This strategy was evaluated during the development of the passwordless I.D.; the strategy is excellent but does not eradicate the problems associated with password memorization. Hence, We took a different path with the password-less invention; our team reviewed another study that found that humans and how they interact with computer systems are the weakest link in computer information security (Hoonaker, 2013). Because of this research, the possibility of passwords was abolished. Human error will be reduced to a large extent using this strategy.

The ID will allow employees access to the work areas without requiring them to provide a password, and the gadget will be capable of scanning entry points. The group concluded that providing numerous functions would make the device more effective. One of the main features added to this gadget is the registration of the employee's fingerprint. This biometrical security was included to provide multiple layers of security to the device. Research shows biometrics are unlike passwords and other authentication forms because they cannot be counterfeited (O'Gorman, 2003). Hence, the passwordless I.D. has been paired with a fingerprint. When the user arrives at the workstation, the I.D. will be inserted into a scanner, and the user will be required to scan their fingerprint. If, for some reason, the employee forgets to take the card out, the scanner will beep. Similar to an atm when the card is forgotten. This will ensure the user does not leave their I.D. in the office. Once the employee completes this process, the computer will unlock and allow access to all applications and systems required to operate. The system will unlock once the I.D. and fingerprint are verified, and the software will generate a one-time passcode or token, which will only last for 24 hours. In their most basic form, tokens are extended passwords that a computer generates for a specific time range. Because of this security

feature, the users will no longer be routinely required to invent new passwords; instead, the device will do so on their behalf.

Our innovation utilizes the physical card, the biometric fingerprint, and the token generation in tandem to provide three layers of protection. Because there are several layers of protection, it will be difficult for hackers to penetrate the system and get access. Not only will it be hard for a hacker to get beyond the security of the building, but they also will not be able to get their hands on the user's physical I.D. or fingerprint.

Innovation Obstacles

Most of the issues within companies occur due to human error. Because this device is physical, employees are expected to lose or forget it at home occasionally. To resolve this problem, security officers at the facilities will store additional I.D.s in a safe. Only the security personnel have authorization to temporarily activate the devices and attach the users' biometric profiles. The temporary devices will deactivate themselves after 24 hours as an added precaution in case one is taken home by mistake.

Another issue expected with the I.D. is that biometrics can be costly, so the product may not be within everyone's reach. The target clientele for this product is more prominent companies that hold extremely delicate information, such as financial institutions and government agencies. According to Cishow Hardware (2022), fingerprint scanners cost around $50.00 to $2,500.00 each. The cost of this type of scanner may seem high, but when compared to a successful cyber-attack, the price is minimal. In 2011, hackers infiltrated Sony Entertainment's data room, using compromised accounts to steal 100 million customers' records (Agrafiotis, 2018). The incident left Sony with a financial burden of 171 million dollars and a significantly damaged reputation.

Acquiring advanced biometric technology may seem like a massive expense; however, it is an investment that has the potential to save companies millions of dollars.

Courses Taken Related to Problem-Solving and Innovation

There are a few courses at Old Dominion University that helped with product development and problem-solving. Interdisciplinary studies are one of the required courses that aid students during this process because it focuses on using knowledge and methods from different fields to solve complicated and new problems. A good analogy for interdisciplinary studies is when someone is looking to paint their house a new color, and they do not want their home to look like everyone else's in the neighborhood. So, to fix the problem, the painter mixes different paint colors until the desired color is obtained and the customer is satisfied. The same happens during the process of innovation; in order to solve a problem or develop a product, numerous perspectives and ideas must be considered to ensure the best solution is obtained and that no room for error is left behind. With an interdisciplinary approach, success expectations for problem-solving are high.

In addition, interdisciplinary studies teach students how to collaborate in groups to generate ideas and provide fresh perspectives on a subject. Creating passwordless innovation would not have been possible without using interdisciplinary studies as a foundation, and group collaboration was an essential part of the process. With the multiple perspectives from our group, the team concluded that password security is one of the areas in cybersecurity that needs much attention. The evolution of new technologies is creating new problems with password security. Therefore, a multidisciplinary approach is needed to tackle this arising issue.

The study of criminology is another elective outside the cybersecurity program that can be applied with innovation. Comparable to multidisciplinary studies, criminology employs a

variety of viewpoints to comprehend the causes of crime. Crime evolves with time in the same way that technologies do. Consequently, a new study is required to address the new tactics criminals use to engage in illegal activity. Criminologists analyze data from a population to see the types of crime being committed and, depending on that data, select an approach to eradicate the behavior. They then modify their approach until they obtain the desired results. The same goes for the creation of an innovation; in order to fix any functionalities issues of a new product, they must review data logs and feedback. Once they review the data, they make modifications until they solve the problem.

In addition, digital literacy also applies to the creation of a product. Especially today, digital skill is required for almost everything, and technology is constantly evolving. Digital Literacy means "to use technology to find information, evaluate sources, create content, and communicate with others effectively. It is a skill set used to navigate the new technological paradigm in which society operates" (Lynch, 2017). Digital literacy has several components that apply to innovation. For example, it allows people to be more aware of new technologies as they arise. A person actively learning new technological information has an advantage over those who do not. A person who stays current will find solutions to new challenges more quickly. An analogy for this is when a mechanic with newer equipment at a shop; their shop will always be more efficient than an outdated one. Digital literacy brings many advantages, especially regarding innovation; learning digital literacy skills makes research and problem-solving more efficient.

Testing the Product Effectiveness

To validate that the product is working successfully, the device must go through the last phase of the design thinking model: validation. The method of validation used is the A/B

comparison. The product will be rolled out to a smaller group of users to compare it to the previous authentication method. With employee feedback, the product will show if it is successfully working or not. Piloting the product will also help improve the areas that are not working correctly before rolling it out to the entire organization (Landaeta, 2020). Once the invention works appropriately and achieves the desired results, our team will continue monitoring the metrics and adjusting any necessary controls. The product will endure ongoing testing to ensure that it works efficiently.

After the product is rolled out to a smaller group of users, collecting feedback on their experience with the new authentication method is essential. This feedback will be crucial in determining whether the product is successfully working as intended or if there are areas that need improvement. The A/B comparison method is best because it preemptively identifies specific pain points or potential areas for improvement before the product is rolled out to the larger organization.

Piloting the product is also a good idea to fix any technical issues not caught during the design phase, allowing the team to make necessary adjustments and ensure that the product functions correctly before being released to the entire organization. Even after the product is rolled out to the entire organization, continuous metric monitoring is imperative to help identify any new issues and ensure that the product functions efficiently. Ongoing testing is also crucial to guarantee that any updates or modifications made to the product do not interfere with its performance.

Being a part of the testing process is the best method to determine if a product performs as desired. As a result, our developers will put the product through usability testing, which will involve sitting next to or shadowing the user as they use the product. With this testing type,

errors may be addressed immediately rather than waiting for employee feedback. Furthermore, development teams can uncover issues before coding them into the device. When problems are detected and fixed early, fixing them costs less money since time and effort are saved.

Finally, the company will use test logs as the final effectiveness test. These logs contain detailed information on how the application on this device is performing. The logs are vital during testing since they document issues while the application operates. Using this strategy, our testing team can identify the cause of problems and why the program may have software errors (Lambdatest, n.d.).

Turning the Innovation Into Reality

1. Process

A detailed process is crucial to turn an idea into reality. When people think of the word innovation, people often say, "It is all about execution; ideas are easy" or "Innovation is about creativity, and only creative people can innovate" (Pslek, 1997). However, turning an idea into a reality requires a plan and a shared commitment to improvement. Innovation is not just about coming up with creative and unique ideas; it requires a lot more than that. The essential components of a business plan include a clear strategy, continuous improvement, collaboration, and a willingness to adapt. The process should also involve everything from conducting market research to identifying key stakeholders and developing a detailed project plan.

2. Collaboration

If the planning process is the framework of an idea coming to life, collaboration is the foundation. Collaboration is the key to achieving positive results. Innovation usually occurs when multiple stakeholders collaborate to share their ideas and perspectives. Pslek (1997) agrees that the collaboration of the entire team and partners is necessary to achieve positive results.

3. Marketing and Competitor Analysis

Now that the groundwork has been laid out, the next step in the business plan focuses on looking at competitors and analyzing customer needs. Doing so ensures that the innovation solves a common problem uniquely and demonstrates a solid value for potential customers. Most importantly, it saves time by providing the product with a clear market need. For passwordless innovation, our team has conducted research to detect potential competitors and has determined that there are no similar products in the market. Having few to no competitors positions our product firmly in the market for potential investors and business partners, increasing the prospects of developing the product for smaller-scale businesses. For example, we plan to partner with a security consulting firm or a cybersecurity training provider to offer our passwordless authentication solution as part of their services.

The passwordless innovation was designed to be *disruptive,* or a process whereby a smaller company with fewer resources can successfully challenge established incumbent businesses (Christensen, 2015). Our plan to make this idea a reality is to take an approach similar to Netflix by pioneering this concept of passwordless security and disrupting the cybersecurity industry. As Netflix redefined the cable industry, we plan to redefine password protection. Netflix became a business pioneer, forcing other companies to reimagine their approach to video rental. The passwordless innovation has been designed with a similar thought process, and we are confident that it will achieve similar results that will appeal to investors.

After conducting market research to identify customers' needs, potential pain points include the hassle of remembering and resetting passwords, security concerns around traditional authentication methods, and the need for a more convenient and user-friendly solution. Our unique selling point is the security and convenience of a passwordless authentication solution.

Passwordless authentication eliminates the need for remembering passwords, improves safety, and comprehensively provides a better user experience.

4. Target Market

The target market for passwordless authentication is broad and includes many industries looking for a highly secure and efficient authentication solution. Government agencies with high-security requirements may be interested in passwordless authentication solutions to improve security and streamline access control processes. Financial institutions, including banks and insurance companies, deal with sensitive customer information and must ensure that their authentication processes are secure. Passwordless authentication can help mitigate the risk of data breaches and improve customer experience. Healthcare providers deal with sensitive patient data and must comply with strict privacy regulations. Passwordless authentication can ensure that only authorized personnel can access patient data while improving workflow efficiency. These institutions have continued to be one of the most targeted by cyber intruders in recent years. In February of this year, the U.S. Justice Department was hacked, compromising data about an investigative target and agency employees (Guinness, 2023). To remain secure, high-profile organizations must evolve in their approach, and the passwordless design supports that by eliminating any loopholes in human error with traditional password policies. Also, the application has been created to be user-friendly and make it simple to understand. With this design, we plan to attract the intended target buyers.

5. Marketing Channels

Another aspect to consider when turning an idea into a reality is choosing the proper marketing channels. Choosing the most effective channels is crucial to reach the targeted clientele. This step is an integral part of an innovation's survival because without being able to

reach the target audience, the product will fail. Most individuals conduct product research through marketing channels, with 76% using social media and 51% using other search engines. When launching a new product, it is critical to gain attention; this strategy has proven to be the most effective. The greater the product's visibility, the more likely someone will choose it (Jeromchek, 2022). Since social media is one of the most vital marketing channels to reach investors, it will be one of the channels used by the password-less product. With this channel, the product should be noticed by many financial institutions not only around the country but also internationally. Social media will also significantly impact government agencies' attention since Twitter is the most popular media many politicians use (Rooyen, 2019). By using the proper marketing channels to advertise the passwordless innovation, the product will not have any issues reaching potential buyers and investors.

Summary of Next Steps

Once the product has been rolled out and advertised and the partnership has been established, the mission is to continue to expand. Once the product has been proven valuable, the demand should increase. It is vital to consider hiring more staff or partnering with third-party manufacturers to make production more efficient. Not having a sustainable supply chain can result in unmet clientele expectations. A company not ready to meet business demand can cost a business many opportunities (Reed, 2013).

For the company to maintain its competitive edge, it is essential to continually develop new features for the product and improve existing ones. To accomplish this, the company will need to perform market research to examine the competition, gather customer feedback, and invest in product development.

Finding reputable partners is yet another stage that will play a significant role in the expansion of the product. Putting together a strong team is essential to the success of any business, especially when a company is just starting its expansion. Building a solid team has many advantages, including better communication, increased production, collaborative problem-solving, and an increased capacity for ingenuity.

Conclusion

In conclusion, technological advancements have improved the quality of operations for many organizations, but human error endures. Instances of cyber-attacks capitalizing on human error via password authentication are increasing at an accelerated pace. Over the years, security professionals have tried to make passwords more robust and intricate. While password policies were developed to mitigate this risk, they are not a universal solution. Most data breaches continue to occur due to weak passwords; therefore, it is paramount for companies that hold sensitive information to find a more comprehensive solution to counter the problem. Although businesses attempt to offset these risks with drastic measures, password policies can only become so strict before fostering non-compliance. With this, a significant market need has emerged for innovation to counterbalance the vulnerabilities of password security while maintaining convenience for employees and efficiency for businesses.

This passwordless innovation is marketed as a more secure and user-friendly alternative to traditional password-based authentication. Simplifying the authentication process eliminates employees' need to remember or jot down passwords for every program or system, making the process more secure and convenient. This invention simultaneously reduces the risk of cyber-attacks and improves employee user experiences. Such a unique selling point gives our business model a competitive advantage by delivering a disruptive innovation while addressing

consumers' needs and offering substantial value to investors and clients. With a streamlined strategy and extensive stakeholder involvement, this invention has the potential to alleviate many password-based authentication safety concerns and inconveniences.

References

Amer, A. (2021). The cyberwar between Israel and Iran is heating up. Middle East Monitor. https://www.middleeastmonitor.com/20211108-the-cyberwar-between-israel-and-iran-is-heating-up/.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). doi:10.1093/cybsec/tyy006.

Bareckas, K. (2020). What is a dictionary attack and how to prevent it? NordVPN Blog. Retrieved April 21, 2023.

Bishop, M., & Klein, D.V. (1995). Improving system security via proactive password checking. *Comput. Secur.*, *14*, 233-249.

Choong, Y.-Y., Theofanos, M. and Liu, H.-K. (2014) "United States Federal Employees' password management behaviors a Department of Commerce Case Study," United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study [Preprint]. Available at: https://doi.org/10.6028/nist.ir.7991.

Christensen, C. (2023, April 06). What is disruptive innovation? Retrieved April 22, 2023, from https://hbr.org/2015/12/what-is-disruptive-innovation

Chaparro, B.S., & Riley, S.R. (2006). Password Security: What Users Know and What They Actually Do.

CishoHarware. (2022). How much do fingerprint readers typically cost? C&I show security.

FICO. (2018). Survey: Americans are frustrated by security measures. FICO Decisions Blog. Retrieved March 3, 2023, from https://www.fico.com/blogs/survey-americans-are-frustrated-security-measures.

Grant, J. (2011). The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. IEEE Internet Computing, 15(6), 80-84.

Grigas, L. (2022). Brute force attack: What is it and how to stay safe. NordPass Blog. Retrieved April 21, 2023.

Guinness, H. (2021, March 3). A brief history of US government agencies hacking: From the Cold War to Stuxnet. Popular Science. Retrieved April 21, 2023, from https://www.popsci.com/technology/us-government-agencies-hacking-history/.

Hoonakker, P. L. T., Corcoran, C., & Clarkson, J. D. (2013). Password authentication from a human factors perspective: Results of a survey among end-users. International Journal of

Human-Computer Interaction, 29(9), 577-589. https://doi.org/10.1080/10447318.2013.795769.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. Communications of the ACM, 47(4), 75-78.

Jeromcheck, M. (2022). Marketing Channels: The Importance of Cohesive Messaging. CoSchedule Blog. Retrieved April 21, 2023, from https://coschedule.com/marketing-strategy/marketing-channels/marketing-channel-importance.

Kim, R. (2007). 2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary. Pleasanton, CA: Javelin Strategy & Research.

LambdaTest. (n.d.). Test Log: Everything you need to know. LambdaTest Learning Hub. Retrieved April 21, 2023, from https://www.lambdatest.com/learning-hub/test-log

MacInnis, J. (2017). A brief history of the password & why it matters. Retrieved April 21, 2023, from https://blog.hidglobal.com/es/node/34972.

Lynch, M. (2018). What is Digital Literacy? The Edvocate. Retrieved April 21, 2023, from https://www.theedadvocate.org/what-is-digital-literacy/

Manjarres, S. (2021). 2021 World Password Day: How many will be stolen this year? - secplicity - security simplified. Secplicity. Retrieved March 3, 2023.

National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). doi: 10.6028/NIST.SP.800-63b

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040. doi:10.1109/jproc.2003.819611

Park, J., Kim, J., B. Gupta, B., & Park, N. (2021). Network Log-based SSH brute-force attack detection model. Computers, Materials & Continua, 68(1), 887–901.

Plsek PE. Creativity, Innovation and Quality, ASQ Quality Press, 1997.

Prasad, N. R., & Dhurandher, S. K. (2021). IoT based Structural Health Monitoring System for Smart Cities. Computers, Materials & Continua, 69(1), 1357-1374.

U.S. Department of Health & Human Services. (n.d.). Usability Testing. Usability.gov. Retrieved April 21, 2023.

Reed, B. (2013). Supply chain innovation is a double edged sword for Sustainability. Retrieved April 22, 2023, from https://www.theguardian.com/sustainable-business/supply-chain-innovation-double-edged-sword

Rooyen, G. (2019). 5 social media platforms perfect for government organizations. Retrieved April 22, 2023, from https://blog.pagefreezer.com/5-social-media-platforms-perfect-for-government-organizations.

Vu, K.-P. L., Bhargav, A., & Proctor, R. W. (2003). Imposing Password Restrictions for Multiple Accounts: Impact on Generation and Recall of Passwords. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 47(11), 1331–1335. https://doi.org/10.1177/154193120304701103

Wyatt, M. (2016). A world beyond passwords: Improving security, efficiency, and user experience in digital transformation. Retrieved April 21, 2023, from https://www2.deloitte.com/uk/en/insights/deloitte-review/issue-19/moving-beyond-passwords-cybersecurity.html.

Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences, 74(7), 1160-1172. doi:10.1016/j.jcss.2008.04.002.