Kayla Dudek

November 6, 2024

CSIT 100

**Password Security**

Historically, individuals wanting to protect important documents, finances, and identity did so by finding a “safe space” in their homes. Others, with enough financial resources, paid for the added security of a safety deposit box at banks or installed security systems in their homes. While those services still exist, our ability to interact in a digital world has magnified to a new level, creating various benefits and challenges for individuals and corporations. This paper investigates the components of password security, the common risk factors related to passwords, and the future of digital protection.

Passwords have evolved from children on playgrounds asking for the “password” before sharing the neighborhood news. Today, individuals, companies, and organizations are tasked with protecting their personal information in a digital environment. In a world where password security has become essential, and the threats associated with them are increasing, passwords have become a critical component of daily life.  Passwords offer protection for accounts, devices, and digital platforms and applications. Cisco Systems defines passwords by stating, “Password security and password protection are practices for establishing and verifying identity and restricting access to devices, files, and accounts” (Cisco, 2024, p.1). The company further states that people and organizations alike are managing more passwords than ever.

With the increase in password usage comes an increase in risk and vulnerability. Data security breaches are events when access to protected information is granted to unauthorized users. The access can lead to the exposure, theft, and misuse of personal, financial, or corporate information by malicious individuals. These cybercriminals use unlawful acts including, but far from limited to, hacking, phishing, and malware to threaten the lives of individuals and organizations. Each crime has its own unique set of challenges presented to victims. All cybercrimes involve criminal activity targeting computers using viruses and other types of malwares and or criminal activity using computers to commit other crimes.

Hacking is not always used to cause harm; however, for the purpose of this research, hacking will be presented as being related to cybercrime. According to a contributor for IBM, Matthew Kosinski, “Hacking (also called cyber hacking) is the use of unconventional or illicit means to gain unauthorized access to a digital device, computer system or computer network. The classic example is a cybercriminal who exploits security vulnerabilities to break into a network and steal data” (Kosinski, 2024, p. 1). After gaining access to the information, criminal hackers are able to manipulate the data and accounts as if they were the righteous owners.

Phishing attempts, also referred to as scams, trick individuals into providing information through altered emails, messages, and phone calls, all often with a sense of urgency to distract vulnerable individuals into agreeing to share privatized information. Cyber criminals using phishing practices often employ the use of appearing legitimate through social media, email, and familiar branding. Victims fall prey to being directed to artificial websites made to mimic official sites. In transactions on these fake sites, without knowing, they are providing personal information to their attackers.

Malware is software that infiltrates systems. It is considered a cybercrime that threatens one's ability to navigate one’s accounts. Ransomware, botnets, Trojan horses, and spyware are types of malware that allow cybercriminals to lock individuals from their own accounts, spread internet viruses, gain unlawful access to accounts, and act secretly to gain information. Once inside a user’s system, malware can steal information, complicate operations, and compromise data access. Malicious software can effectively attack computer systems, networks, and devices.

An explosion in the increase of acts of cybercrime leads to a critical need for awareness of best practices that can help protect people and organizations from security threats and breaches. Password security is essential in the protection of personal and sensitive information. The design of a strong password is crucial for managing transactions on devices and accounts to protect from financial loss, identity theft, customer trust, and the legal ramifications related to an attack. In any event, there are measures suggested to take including creating a strong password and protecting it as a first line of defense.

To create passwords that are considered strong, experts agree that they should generally be longer, complex, and unique. A strong password should be at least 12-16 characters. The characters should mix uppercase and lowercase letters, numbers, and special characters.  Each password should be unique to the different accounts of an individual. This prevents leaving multiple passwords vulnerable when one is compromised.  These characteristics help to prevent people and organizations from becoming victims of security threats.

Many challenges those affected by cybercrimes face include the commonality of several factors, including weak passwords and reused passwords. The United States Federal Trade Commission/Consumer Advice states, “The internet has been called the information superhighway. But with scammers, hackers, and other bad guys trying to steal your personal information online, it’s a good idea to know how to lock down your devices, network, and information” (Miller, Puig 2024). There are additional strategies to combat vulnerability connected with password security. People and organizations are encouraged to become educated on the dangers of weak passwords. Researched password managers, and monitoring companies can aid in the protection of personal information. There is also the importance of updating passwords regularly. According to Meghan Anderson of NIST, National Institute of Standards and Technology, U.S. Department of Commerce, “ Strong passwords act as barriers against unauthorized access, making it more difficult for malicious actors to compromise personal accounts, sensitive information, and valuable data. Robust passwords not only prevent identity theft but also provide a foundational layer of security for verifying and managing digital identities” (Anderson, 2023, p. 7).

Despite strong passwords, cybercrimes continue to occur as new technologies develop to prevent them. A most recent event triggering reminders to anxious consumers about password security occurred in October 2024. The Atlanta Division of the FBI shared that cybercriminals are maliciously finding their way into personal email accounts and gaining access by stealing cookies from personal computers. The “cookie,” or small piece of data that a website sends to a computer grants permission for a website to “remember” details, such as login information, preferences, or items in a shopping cart. Suppose a cybercriminal gains access to a Remember-Me cookie from a user’s recent login to their web email. In that case, they can use it to sign in as the user without needing their username, password, or multifactor authentication (MFA). Public Affairs Specialist Jenna Sellitto of the FBI states, “For these reasons, cybercriminals are increasingly focused on stealing Remember-Me cookies and using them as their preferred way of accessing a victim’s email. Victims unknowingly provide their cookies to cybercriminals when they visit suspicious websites or click on phishing links that download malicious software onto their computer.” (Sellitto, 2024, p. 2).

As mentioned above, cyber threats continue to grow and change with the industry. However, one thing remains the same: the need for awareness and the evolution of technologies to combat cyber criminal activity.  Advancements have been continuous since the dawn of the early computing era. With the onset of the Internet new challenges were faced. Following its progression, the digital world experienced the challenges of the September 11 attacks and the pandemic. Both situations brought to attention the need for advanced security for its users. Presently, new threats are gaining momentum in disrupting the increasing number of users in our digital world. Organizations and the IT world must continue to be proactive in protecting systems, data, and patrons. Technology prevention strategies include regular security assessments, employee training, data encryption, and having a solid plan in place for responding when an attack occurs. Assessing the risk factors of individual accounts is encouraged on the personal level as well as those associated with major corporations. Keeping a close watch prevents situations from escalating and, often, occurring at all. Providing training to employees protects the employee, the company, and the consumer allows for teamwork against cyber criminals. Data encryption helps protect from unauthorized access to personal and business accounts by using secret codes to hide information.

These practices are a foundation for protection, but more needs to be done. Advancements in the implementation of new technologies are in progress, and improvements are consistently being made to update password security. An article from Villanova University, posed a question about the best alternatives to passwords. Jenner Holden, Director of Information Security at LifeLock responded by saying, “Passwords may never go away completely, but they will be increasingly supplemented by other, better forms of authentication. These other forms of authentication will go beyond what we currently think of as multi-factor authentication. These useful bits of authentication attributes include the specific devices people use, facial recognition, voice recognition, or movement patterns. These attributes can be combined with smaller, simpler passwords, or pins, to achieve a much better approximation of true authentication than passwords alone” (Luker, Holden, 2023, Q3, p.2). Emerging technologies referenced by this expert include the implementation of biometric authentication, which uses biological traits such as fingerprints, facial features, and eye scans to secure identification. These systems would allow for a higher level of security but could compromise privacy, and data storage could also be a concern.

Another security measure for password protection does not include a password at all; instead, it uses passwordless authentication.  To reduce attacks, one-time codes and links sent through email eliminate the use of traditional passwords. Cisco’s Duo eBook explains this type of security protection as a way to “Reduce the risk of credential theft by enabling users to securely access their applications with a single username and password…Passwordless authentication establishes a strong assurance of a user’s identity without relying on passwords, allowing users to authenticate using biometrics, security keys or a mobile device”(Cisco Duo, n.d.).With more accuracy and less risk for weak or repeated passwords, this authentication type may prove more beneficial.

Adaptive authentication can also reduce risk factors and offers the convenience of improving user experience and can be customized. This type of authentication allows for the assessment of risk factors related to the location of a device. A user logging in from a new space will be prompted to verify additional information. This layer of protection offers confirmation of credentials prior to gaining complete access to secure data. Through this method of authentication, a balance of security needs and convenience is maintained.

Behavioral biometrics include the analysis of user habits. Through the tracking of digital behaviors like mouse clicks and typing speed, technology can provide another layer of security. These traits are different from measuring physical traits such as fingerprints and facial recognition. Patterns such as these allow for the user to be recognized by artificial intelligence and can flag suspicious behavior.

The United States Bureau of International Narcotics and Law Enforcement Affairs warns, “Cybercrime poses a significant and potent threat to U.S. national and economic security. Despite the scale and impact of the problem, cybercrime is under-enforced globally, making cybercrime a low-risk, high-reward criminal activity. In 2020 alone, the FBI estimated more than $4 billion was lost to cybercrime in the United States” (U.S. Department of State, 2024). Despite the technological advancements, challenges continue. Users must remain guarded against the attacks of cyber criminals and adopt best practices related to password security. Organizations must continue developing protocols to cope with data breaches. Authentication developers must continue to work tirelessly at creating protection methods to keep up with safeguarding against cybercrimes.

In conclusion, password security is a critical component in safeguarding personal and organizational data in the ever-changing digital world. By understanding the vulnerabilities of weak passwords, and the consequences of cyber attacks, users can take proactive measures of protection. Practicing strong password policies, assessing risk exposures, and adopting multi-factor identification can help in the reduction of unauthorized digital access. Password security will continue to evolve as efforts are made to secure users without compromising the ease and enjoyment of the experience. As organizations implement security measures that provide protection and productivity, the landscape of password protection will always require diligence on the part of the user.

References

Alicia Luker. (2023, August 18). *Experts’ view on the future of password security*. Villanova University. [Experts' View on the Future of Password Security](https://www.villanovau.com/articles/cybersecurity/experts-view-password-security-future/)

Anderson, M., & Choong, Y.-Y. (2023, October 10). *Cybersecurity Awareness month 2023 blog series: Using strong passwords and a password manager*. NIST. [Cybersecurity Awareness Month 2023 Blog Series | Using Strong Passwords and a Password Manager | NIST](https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2023-blog-series-using-strong-passwords)

Cisco Systems. (n.d.). *Passwordless - the future of authentication*. Cisco Duo. <https://duo.com/resources/ebooks/passwordless-the-future-of-authentication?utm_source=google&utm_medium=paid_search&utm_campaign=DUO_AMER_NA_GS_Nonbrand_Passwordless_T3&utm_content=Passwordless&_bt=650482702971&_bk=passwordless+security&_bm=p&_bn=g&_bg=146748778277&gad_source=1&gclid=Cj0KCQjwvpy5BhDTARIsAHSilylzjFNrDjISkNo2sbs0g3zAFFD_y3CvX1Q9U4XqdynAeDCT1_KsRIAaArDHEALw_wcB>

Cisco. (2024, November 1). *What are password security and protection?*. Cisco. <https://www.cisco.com/c/en/us/products/security/what-are-password-security-and-protection.html>

Kim, E., Miller, T., & Puig, A. (2024, October 11). *Creating strong passwords and other ways to protect your accounts*. Consumer Advice. <https://consumer.ftc.gov/articles/creating-strong-passwords-and-other-ways-protect-your-accounts>

Kosinski, M. (2024, October 1). *What is hacking?*. IBM. <https://www.ibm.com/topics/cyber-hacking>

Sellitto**,** J. (2024, October 30). *Cybercriminals are stealing cookies to bypass multifactor authentication*. FBI. <https://www.fbi.gov/contact-us/field-offices/atlanta/news/cybercriminals-are-stealing-cookies-to-bypass-multifactor-authentication>

U.S. Department of State. (n.d.). *Cybercrime*. U.S. Department of <https://www.state.gov/cybercrime>