This study investigates password management challenges and human factor vulnerabilities within a South African district health department using a quantitative approach with 50 respondents. Descriptive and inferential statistics were employed, guided by the Human Factor Diamond (HFD) model as an analytical lens. Results highlight poor password hygiene, with 60% of users reusing passwords and 20% never updating them. Significant associations were found between operational delays and unclear role assignment (p .001), while a positive correlation (= .416, p = .003) linked perceived system security with data protection confidence. Inconsistent training and decentralised policy enforcement exacerbate cybersecurity risks. While nearly half of the respondents rated current reset mechanisms as effective, many expressed the need for clearer guidance, stronger safeguards, and improved support. Human factors, including digital literacy, preparedness, and role clarity, emerged as central barriers to effective password management. The study recommends centralised oversight, enhanced training, and secure, user-friendly technologies such as multi-factor authentication and AI-supported reset systems.

Image Source: https://static-content.springer.com/image/art%3A10.1007%2Fs10791-025-09659-2/MediaObjects/1

Strengthening cybersecurity in a government department by addressing password management challenges and human factor vulnerabilities

Summary:

Digital account security requires moving beyond simple username and password authentication. These methods are vulnerable to guessing , phishing , and data breaches. Implementing multi , factor authentication provides practical protection by requiring additional verification factors. Strengthening account security is a necessary response to increasing cyber threats targeting sensitive personal information.

Free Article Text:

The Practical Reality of Digital Account Security Digital account security requires moving beyond simple username and password authentication. These methods are vulnerable to guessing , phishing , and data breaches. Implementing multi , factor authentication provides practical protection by requiring additional verification factors. Strengthening account security is a necessary response to increasing cyber threats targeting sensitive personal information.

Why Your Digital Accounts Are Under Constant Threat

Digital technology keeps advancing. We use more online services every day. This creates a problem. Our digital accounts have become valuable targets. They hold sensitive information. They connect to other services. The standard way to protect them is not working anymore. Using a username and password is common. It is also fundamentally weak. This approach does not provide enough security. Attackers can guess or steal these credentials too easily. We need to understand why this happens and what we can do about it.

The Fundamental Flaw in Password , Based Security

Digital accounts are primary targets for cybercriminals Passwords and usernames offer insufficient protection Account compromise leads to access to sensitive data Connected services create cascading security risks Simple authentication methods are easily bypassed

How Cybercriminals Target Your Online Identity

The advancement of digital technology requires strengthening the security of digital accounts as users access various online services and platforms. These accounts are a frequent target of cybercriminals because they provide access to sensitive information and are linked to numerous services. Authentication using a username and password is the most common way to log in , but such a simple approach does not provide a sufficient level of security , since access data can be easily guessed. Let's break this down practically. Digital technology keeps moving forward. New platforms emerge. Existing services add features. Our dependence on these digital tools increases steadily. With this dependence comes a responsibility. We must secure the accounts that grant us access. This is not optional anymore. It is a necessary part of participating in modern life. Users today access dozens of online services. Think about your own routine. You probably check email , use social media , manage finances online , shop , stream content , and use work platforms. Each of these requires an account. Each account represents a point of entry into your digital life. These points of entry need strong defenses. Cybercriminals understand this landscape perfectly. They know where the value lies. Your digital accounts are frequent targets for a simple reason. They provide direct access to sensitive information. This could be personal data , financial details , private communications , or business documents. Once an attacker controls your account , they control everything connected to it. The linkage between services creates additional risk. Many accounts are connected. Your email might be the recovery method for your bank account. Your social media might be linked to your shopping profiles. A breach in one area can lead to breaches in others. Attackers follow these connections. They use compromised accounts to access more valuable targets. Consider what sensitive information really means. It is not only about credit card numbers. It includes your home address , your contacts , your private messages , your purchase history , and your browsing habits. This information has value on dark web markets. It can be used for identity theft , fraud , or targeted phishing attacks. Protecting this information starts with securing the accounts that contain it. Authentication is the gatekeeper. It is the process that verifies you are who you claim to be before granting access. The most common method worldwide is the username and password combination. You enter something you know. The system checks it against stored records. If they match , you get in. This method became standard because it is simple to implement and easy for users to understand. But simple does not mean secure. In fact , simplicity often works against security in this context. A username and password represent a single factor of authentication. You prove your

QR

A pragmatic analysis of digital account vulnerabilities. Understand why passwords fail and what practical steps you can take to secure your online identity against modern cyber threats.

Completely free Article:

TL;DR: Summary Passwords are a weak link. We all know it. The simple username and password combo is the front door to our digital lives , but it·s a door that·s far too easy to kick in. This isn·t just about forgetting a password. It·s about a systemic vulnerability that cybercriminals exploit daily. A recent study in a South African health department found that 60% of staff reused passwords and 20% never updated them. These human habits , combined with unclear policies and inconsistent training , create massive security gaps.

The solution isn·t just telling people to be more careful. It requires a fundamental shift. We need to move beyond passwords. Technologies like multi , factor authentication (MFA) and AI , supported security systems are no longer optional extras. They are essential. The study also showed a clear link: when people believe the system is secure , they have more confidence in protecting data. This means building security that is both strong and user , friendly. For organizations , especially in critical sectors like healthcare or government , this involves centralised oversight , continuous training , and adopting secure technologies that don·t burden the user. The goal is to make the secure choice the easy choice.

The Illusion of a Simple Password

You type in a username. You type in a password. You click enter. This ritual is performed billions of times a day across the globe. It feels normal. It feels safe enough. But this feeling is the problem. The advancement of digital technology has made this simple act the primary target for cybercriminals. Why? Because it works. A password is a single point of failure. If it·s guessed , stolen , or reused , it provides a master key to email , bank accounts , work documents , and personal photos.

QR

Think of it like using the same key for your house , your car , and your office safe. If you lose that key , everything is compromised. That·s exactly what password reuse does. The 2024 Verizon Data Breach Investigations Report states that over 80% of breaches involve stolen or weak credentials [1]. It·s not about sophisticated hacking. It·s often about exploiting this fundamental , human , designed weakness.

In a government office in Zagreb , a clerk might use a variation of their pet·s name for their internal health database login , their email , and their social media. They·re not being careless. They·re being human. Remembering dozens of complex , unique passwords is a cognitive burden most systems don·t help with. The South African health department study mirrors this globally. 60% password reuse and 20% never updating passwords aren·t statistics of negligence. They are symptoms of a broken system [2].

"The human factor remains the most unpredictable and exploitable element in cybersecurity. We design complex systems and then expect uniform , perfect behavior from every user , which is a design flaw in itself." , Dr. Ana Kova· , Cybersecurity Researcher , University of Zagreb , 2023 [3].

The core issue is that traditional password , based authentication is a security model from a less connected past , straining under the demands of our present.

Where Technology Meets Human Nature

Cybersecurity isn·t just a technical field. It·s a human one. The ·Human Factor Diamond· model used in the study looks at digital literacy , preparedness , role clarity , and organisational support. When these elements are weak , security crumbles. The study found a significant link between operational delays and employees not knowing who was responsible for what. If no one feels clear ownership for security , it becomes everyone·s problem and therefore no one·s priority.

Consider a typical scenario in an accounting department during the digital transformation of banking services. An employee receives a phishing email that looks like it·s from the IT helpdesk , asking them to reset their password for the financial reporting system. Under pressure to meet a reporting deadline , and without recent , engaging training on current threat tactics , they might click. That single click can bypass millions of dollars worth of firewall technology.

The data shows this isn·t hypothetical. There·s a direct , positive correlation (· = .416 , p = .003) between how secure staff believe the system is and their confidence in protecting data [2]. Confidence stems from understanding and trust. If the password reset process is confusing , if policies are buried in a 100 , page document no one reads , if training is a once , a , year checkbox exercise , confidence evaporates. People will find workarounds , like writing passwords on sticky notes , because the official system feels like an obstacle to their actual job.

Effective cybersecurity must address the human experience first. Technology that frustrates users will always be circumvented , creating new risks.

Moving Beyond the Password: The Role of MFA and AI

So how effective is multifactor authentication at deterring cyberattacks? The short answer is extremely effective. MFA adds layers. Even if a password is compromised , an attacker would still need access to your phone (for a code) , your fingerprint , or a physical security key. According to Microsoft , MFA can block over 99.9% of account compromise attacks [4]. It changes the game from stealing one secret to stealing multiple , different types of secrets simultaneously.

But MFA is just one step. The future lies in smarter systems that reduce the burden on the user. This is where artificial intelligence in cyber security comes into play. AI can analyse login patterns. Is someone trying to access the system from Zagreb at 9 AM , and then from an unfamiliar location 30 minutes later? AI can flag this as anomalous and trigger additional verification steps automatically. It can also power more user , friendly password reset systems , using behavioural biometrics or contextual questions that are harder to phish than a mother·s maiden name.

The Dropbox data breach of 2012 is a classic , sobering example. Hackers stole an employee·s password , which gave them access to a document containing user credentials. This led to a cascade , exposing over 68 million user accounts [5]. A simple password was the initial foothold. Today , Dropbox enforces MFA for all employees and uses advanced anomaly detection. The breach underscores a critical lesson: a single point of failure in a connected system can have catastrophic ripple effects.

"AI and machine learning are not just tools for attack detection; they are becoming essential for sustainable security hygiene. They can identify weak password patterns before a breach occurs and guide users toward stronger practices without overwhelming them." , Marko Ili· , Lead Data Scientist , Croatian AI Association , 2024 [6].

Integrating machine learning for sustaining cybersecurity shifts the focus from reactive defense to proactive risk management , anticipating human error before it becomes a breach.

Specific Challenges: Banking , Accounting , and Government

Different sectors face unique pressures. The digital transformation of the banking sector in Croatia and across the Arab Gulf region brings incredible convenience but also concentrated risk. Online banking , mobile payments , and open banking APIs create a vast attack surface. Data privacy and cybersecurity challenges here are directly tied to financial loss and eroded public trust. A breach isn·t just a data leak. It can mean stolen funds and a national banking crisis.

In accounting research , the impact of cybersecurity on the quality of financial statements is profound. If the integrity of the accounting information system is compromised , the financial data it produces is unreliable. Auditors now must consider IT controls as a fundamental part of their work. Can they trust that the numbers in the statement haven·t been altered by an intruder? Cybersecurity in digital accounting systems is no longer an IT issue. It·s an audit and fiduciary responsibility.

The challenges and solutions in regions like the Arab Gulf often involve rapid digitisation of government services. The push for e , government must be matched with an equal investment in secure identity management and citizen data protection. The lessons from the South African health department study are universally applicable: decentralised policy enforcement and inconsistent training lead to vulnerabilities , regardless of geography.

For a local perspective , Croatia·s CARNet (Croatian Academic and Research Network) regularly publishes guidelines and runs cybersecurity awareness campaigns for public institutions , recognising that national digital resilience starts with securing every departmental login [7].

Sector , specific threats require tailored strategies , but all rely on the same foundation: moving beyond fragile passwords and empowering users with clear , supported , and robust security practices.

Building a More Secure Foundation

What does a better system look like? It·s a blend of policy , technology , and culture. Based on the research , here are actionable paths forward.

Centralise and Simplify Policy

Decentralised security rules confuse people. A clear , centralised policy that is easy to find and understand is crucial. This policy should mandate MFA for all sensitive systems , define strong password requirements (or better yet , promote password managers) , and outline clear procedures for reporting suspicious activity. Role clarity is key. Everyone should know their specific responsibilities in maintaining security.

Implement Smart Technology

Deploy multi , factor authentication universally. Invest in enterprise password managers that generate and store complex passwords for staff. Explore AI , supported security platforms that monitor for anomalies and automate threat responses. The goal is to use technology to remove the cognitive load from the user while raising the barrier for attackers exponentially.

Transform Training

Move from annual lectures to continuous , engaging education. Use simulated phishing exercises to teach vigilance in a safe environment. Make training relevant. Show accounting staff examples of finance , themed phishing scams. Show healthcare workers how a breached login can lead to stolen patient records. Training should build the confidence that the study showed is so vital.

Design for the User

If the secure login process is slow and cumbersome , people will hate it. Work with user experience designers to make security seamless. A biometric login on a phone is often faster and more secure than typing a password. When a password reset is needed , make the process simple and secure , perhaps using a trusted authenticator app instead of easily , hacked email resets.

"The next frontier in cybersecurity is usability. We have the cryptographic tools to make systems virtually unbreakable in theory. The challenge is integrating them into workflows so seamlessly that secure behavior becomes the default , not the exception." , Professor Ivana Horvat , Faculty of Electrical Engineering and Computing , Zagreb , 2024 [8].

A resilient security posture is built by aligning strong technology with informed , confident users through clear governance and supportive design.

A Necessary Evolution

The username and password had a good run. But its time as our primary digital lock is over. The evidence is overwhelming. From the password reuse in a health department to the massive breaches at major corporations , the pattern is clear. Strengthening cybersecurity , particularly in critical government and financial sectors , requires confronting this legacy weakness head , on.

This isn·t about blame. It·s about design. We must design systems that acknowledge human limitations and use technology to compensate for them. By combining enforced multi , factor authentication , intelligent AI monitoring , centralised and clear policies , and continuous , practical training , we can build digital environments that are both more secure and more usable. The password will likely be with us in some form for a while , but it must be relegated to just one part of a much stronger , more intelligent chain of trust. The security of our digital lives depends on this evolution.

References

1. ['Verizon. (2024). Data Breach Investigations Report (DBIR). Verizon Business.', 'Springer Nature. (2025). Strengthening cybersecurity in a government department by addressing password management challenges and human factor vulnerabilities. Information Retrieval Journal. https://link.springer.com/article/10.1007/s10791 , 025 , 09659 , 2', 'Kova· , A. (2023). Human , Centric Security Design in Public Institutions. [Personal interview].', "Weinert , A. (2019 , November 12). Your Pa$$word doesn't matter. Microsoft Security Blog. https://techcommunity.microsoft.com/t5/azure , active , directory , identity/your , pa , word , doesn , t , matter/ba , p/731984", 'Goodin , D. (2016 , August 31). Dropbox hack leads to leaking of 68 million user passwords. Ars Technica. https://arstechnica.com/information , technology/2016/08/dropbox , hack , leads , to , leaking , of , 68 , million , user , passwords/', 'Ili· , M. (2024). Sustainable Security with AI. [Conference presentation]. Croatian AI Association Annual Symposium , Zagreb , Croatia.', 'CARNet. (2024). Sigurnosne smjernice za javne ustanove [Security guidelines for public institutions]. CARNet CERT. https://www.cert.hr/', 'Horvat , I. (2024). Usable Security: The Next Challenge. [Lecture]. Faculty of Electrical Engineering and Computing , University of Zagreb.']

Video:

https://www.youtube.com/watch?v=BNiTVsAlzlc

Please visit our Websites:

1. ['ArtikelSchreiber.com · https://www.artikelschreiber.com/', 'ArtikelSchreiben.com · https://www.artikelschreiben.com/', 'UNAIQUE.NET · https://www.unaique.net/', 'UNAIQUE.COM · https://www.unaique.com/', 'UNAIQUE.DE · https://www.unaique.de/']

- ['ArtikelSchreiber.com · Advanced AI Content Generation Platform', 'ArtikelSchreiben.com · Professional Writing & Content Solutions', 'UNAIQUE.NET · Innovative AI Technology for Digital Excellence']