RCHUB: JOURNAL OF COMPUTATIONAL INTELLIGENCE SCIENCE AND ENGINEERING (JCISE)
VOL: 2, ISSUE 3, JULY - SEPTEMBER 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

A STUDY ON THE SECURITY USABILITY PARADOX: DOES STRONGER CYBERSECURITY CREATE LESS SECURE USER BEHAVIOR

Dr. S. Jayasri[1]
Assistant Professor, Department of Computer Applications, Shri Shankarlal Sundarbai Shasun Jain College for Women, T. Nagar, Chennai-600 017

Mahathi Balaji[2]
Student, Department of Computer Applications, Shri Shankarlal Sundarbai Shasun Jain College for Women, T. Nagar, Chennai-600 017

Abstract

Security is supposed to protect people, but in everyday use it can also make life harder. This paper looks at the security–usability paradox: the idea that stronger security controls can sometimes lead users to take shortcuts that are less safe. Instead of treating this as a theory alone, the paper brings together selected usable-security studies and codes them along two simple scales: how much friction a control creates and how likely it is to encourage risky behavior. The synthesis points to a clear pattern. Controls such as repeated login prompts, complex password rules, and frequent interruptions tend to create frustration and workarounds, while controls like single sign-on, clearer authentication flows, and practical password support are linked with better behavior. Three visuals are used to show this: a bar chart of common awareness-program pain points, a scatter plot showing the coded friction-behavior relationship, and a heatmap that compares security controls with their usability impact. The main takeaway is simple: stronger cybersecurity is not automatically safer if people cannot use it comfortably and consistently.

Keywords: Cybersecurity, Usable Security, Security–Usability Paradox, Security Friction, User Behaviour, Human Factors, User Compliance, Security Controls, Risk Perception, Authentication Usability, Security Awareness, Behavioural Security, Security Effectiveness.

1. Introduction

Cybersecurity is often described as a technical problem, but in practice it is also a human problem. People choose passwords, respond to warnings, approve login requests, and decide whether a rule feels worth following. When a security control is clear and practical, people

VOL: 2, ISSUE 3, JULY - SEPTEMBER 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

usually tolerate it. When it feels repetitive, confusing, or heavy-handed, they often start looking for shortcuts.

That is where the security–usability paradox shows up. A control can be stronger on paper and still perform worse in the real world if it pushes users toward ignoring alerts, reusing passwords, writing things down, or avoiding the control altogether. So the real question is not only whether a control is secure, but whether people can live with it well enough to use it correctly.

This study asks a straightforward question: does stronger cybersecurity create less secure user behavior when the control introduces too much friction? The goal is not to argue against security. It is to understand where the balance breaks down.

2. Literature Review

The usable-security literature keeps returning to the same idea: security works better when it fits the way people actually behave. Haney argues that users are not the weak link in some abstract sense; more often, they are responding normally to systems that demand too much effort.

Password research makes that very easy to see. In studies of employee password management, people rarely behave carelessly for no reason. They manage too many credentials, deal with too many password rules, and then adopt coping habits such as reuse, simplification, or note-taking. Those habits are imperfect, but they are also predictable responses to pressure.

The same pattern appears in awareness training and phishing research. Completion rates can look good while actual behavior remains shaky. Users may click through because the warning is unclear, because they are busy, or because the message looks like every other warning they have seen that week. In other words, the measure is often compliance, not change.

NIST guidance also supports this broader view. Its authentication and usable-security work repeatedly emphasizes that security controls should reduce risk without creating unnecessary burden. That does not mean security should be easy in a careless way. It means security should be usable enough that people can follow it consistently.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

Table 1. Selected sources used in the synthesis

Source	Main idea	Why it matters here
NISTIR 7991	Password policies shape behavior, not just login security.	Shows how password rules can create friction.
NIST.IR.8420A	Awareness programs struggle to show true behavior change.	Shows completion is not the same as secure behavior.
SP 800-63B	Authentication should reduce burden as well as risk.	Directly supports the usability argument.
Greene et al.	User context affects phishing susceptibility.	Shows people do not react in the same way.
Canham et al.	Repeat clicking depends on context and individual differences.	Supports a behavior-based view of risk.
Haney	Usable security should work with human habits, not against them.	Frames the paradox clearly.

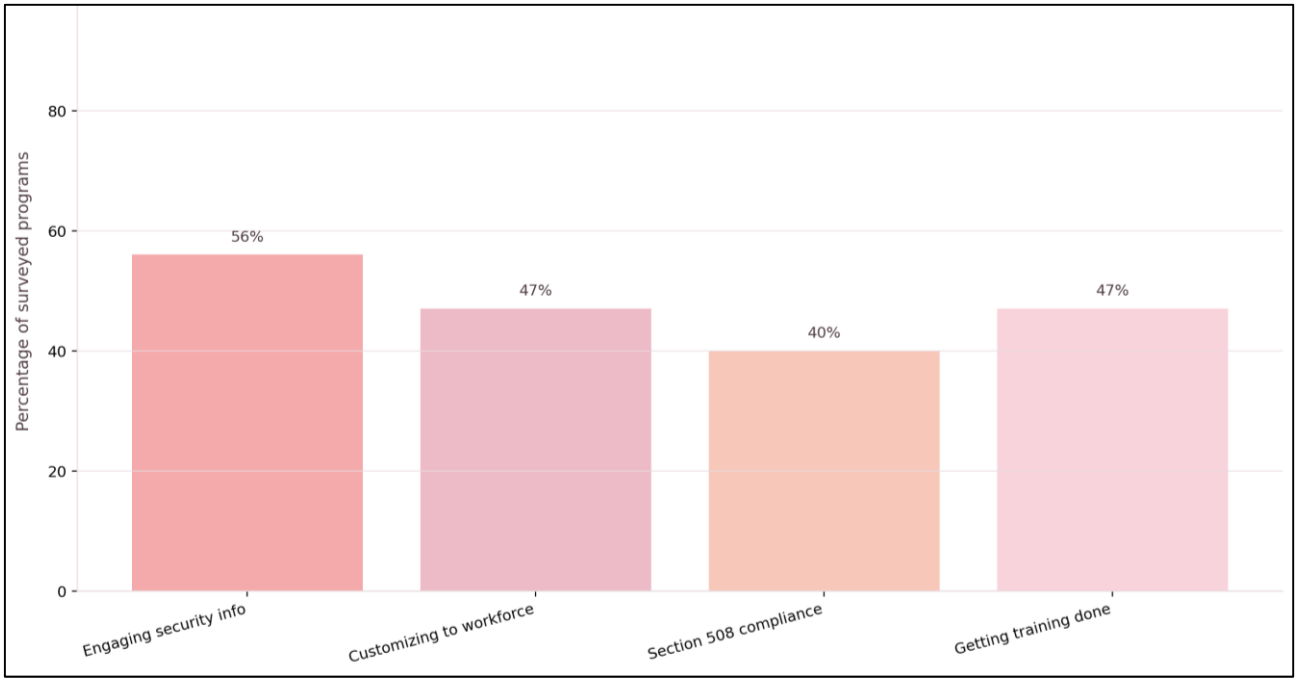

Figure 1. Percentages from NIST.IR.8420A showing where awareness programs most often struggle.

VOL: 2, ISSUE 3, JULY - SEPTEMBER 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

3. Existing System / Problem Background

In many organizations, security is still added in layers: longer passwords, more prompts, more reminders, more warnings, and more training sessions. That approach can look responsible, but it sometimes measures effort instead of effectiveness.

A team may proudly report that everyone completed a training module or that every user passed a phishing simulation. Those numbers matter, but they do not automatically show that everyday behavior improved. If people still reuse passwords, ignore warnings, or click through prompts to get work done, the apparent success is only partial.

This is the real problem behind the paradox. Strong controls can become weak in practice when they create enough friction for users to work around them. The paper treats that mismatch as the central issue.

4. Research Questions and Hypotheses

Research question: When cybersecurity controls become more demanding, do people respond with safer behavior or with more shortcuts?

- H1: Higher security friction is associated with more insecure behavior, especially password reuse, delay, and workarounds.
- H2: The same security control does not affect every user in the same way; context changes the response.
- H3: Measures based only on completion or compliance can overstate true security effectiveness.
- H4: Controls that reduce unnecessary burden, such as single sign-on or clearer prompts, are more likely to support secure behavior over time.

5. Proposed Methodology

This paper uses a structured literature synthesis rather than a live lab experiment. The idea is to read a set of relevant usable-security sources, identify what each source says about friction or risky behavior, and then code those findings in a consistent way.

RCHUB: JOURNAL OF COMPUTATIONAL INTELLIGENCE SCIENCE AND ENGINEERING (JCISE)
VOL: 2, ISSUE 3, JULY - SEPTEMBER 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

Each source was scored on two simple scales. The first was security friction, meaning how much effort, interruption, or confusion the control seemed to create. The second was insecure-behavior tendency, meaning how likely the source suggested users were to ignore, bypass, or resent the control.

The bar chart comes from published NIST survey percentages showing common pain points in security awareness programs. The scatter plot and heatmap summarize the coded reading of the literature. They are not random decorations; they are visual versions of the paper's logic.

This kind of method works well for a small research paper because it turns a broad discussion into something readable, comparable, and easy to defend.

Figure 2. Coded friction and unsafe behavior

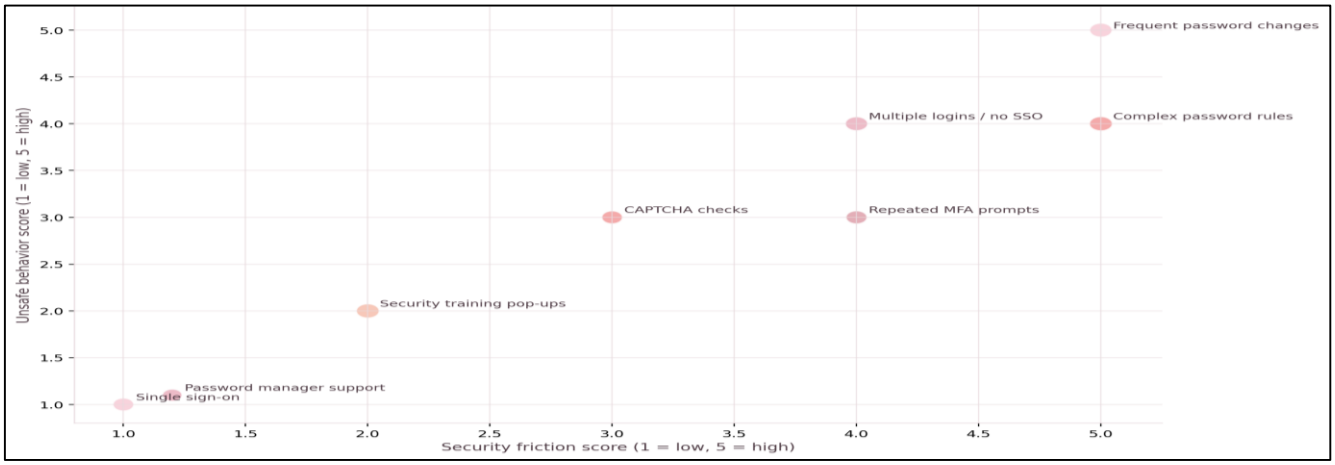

Figure 2. Literature-coded relationship between friction and unsafe behavior.

6. Results and Analysis

The first chart shows that the biggest complaints in awareness programs are not all technical. The top issues are making security information engaging, tailoring it to the workforce, and getting training done in the first place. That already hints at the paradox: a program can exist, but if it does not feel relevant, people stop paying attention.

The scatter plot is the clearest visual summary of the paper's main idea. Controls with more friction, such as complex password rules, repeated logins, and frequent password changes, sit

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

higher on the unsafe-behavior scale. Lighter controls, such as single sign-on and password manager support, sit lower because they reduce stress and interruptions.

The heatmap gives a more detailed view. Password complexity and expiration create the strongest mix of frustration, time waste, and password reuse. Security warnings and repeated prompts are closely linked with alert fatigue. Single sign-on stands out as the calmest option because it lowers the need for repeated action.

Taken together, the figures do not say that security controls are bad. They say that poorly balanced controls can push users into habits that quietly weaken security.

Figure 3. Heatmap of usability impact by security control

Figure 3. Ordinal coding based on the reviewed sources.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

7. Discussion

The biggest lesson here is that cybersecurity cannot be judged only by strength in theory. A policy may look stricter, but if it annoys users enough, the practical result can be worse.

This is why usability is not a soft extra. It is part of the security design itself. A login flow that is easier to understand, a warning that is shorter and clearer, or a password policy that is demanding but not absurd can do more for real security than a heavier rule that everyone resents.

The findings also suggest that awareness programs should be measured by behavior, not just attendance. A training module may check a box, but that does not tell us whether people changed what they do under pressure.

The best position, then, is not to choose between security and usability. The better goal is to remove friction where it does not add much protection and keep friction where it actually stops risk.

8. Practical Recommendations

Area	What to do	Why it helps
Passwords	Prefer passphrases and password managers instead of endless complexity rules.	Users remember them better and reuse them less.
Login flow	Use single sign-on where possible so users do not need to solve the same problem repeatedly.	Fewer interruptions usually means fewer workarounds.
Warnings	Make alerts short, specific, and hard to ignore.	Clear warnings are more likely to change behavior.
Training	Measure behavior after training, not just attendance.	Completion alone does not prove safety.

Table 2. Practical recommendations from the synthesis.

9. Conclusion

The security–usability paradox is real enough to matter. Stronger cybersecurity does not automatically create better behavior. In some cases, it creates frustration, shortcuts, and habits that quietly weaken protection.

The paper's synthesis shows a simple pattern: controls that are easy to understand and reasonable to use are more likely to be followed correctly. Controls that feel heavy, repetitive, or unclear are more likely to be bypassed in small but meaningful ways.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/3/007

The main takeaway is practical. Security should not be designed as a contest to see how much burden users can bear. It should be designed so that secure behavior is the easiest behavior to keep doing.

References

[1.] Canham, M., et al. (2024). Not all victims are created equal: Investigating differential phishing susceptibility. National Institute of Standards and Technology.
[2.] Choong, Y.-Y. (2014). United States Federal Employees' Password Management Behaviors: A Department of Commerce case study. NISTIR 7991.
[3.] Greene, K., et al. (2018). User context: An explanatory variable in phishing susceptibility. National Institute of Standards and Technology.
[4.] Haney, J. (2023). Users are not stupid: Six cybersecurity pitfalls overturned. Cyber Security: A Peer-Reviewed Journal, 6(3), 230–241.
[5.] Haney, J., et al. (2022). Approaches and challenges of federal cybersecurity awareness programs. NIST.IR.8420A.
[6.] National Institute of Standards and Technology. (2025). SP 800-63B: Digital Identity Guidelines—Auth entication and Lifecycl e Managem ent.
[7.] Akhawe, D., & Felt, A. P. (2013). Alice in Warningland: A large-scale field study of browser security warning effectiveness. Proceedings of the 22nd USENIX Security Symposium, 257–272.
[8.] Fagan, M., & Khan, M. M. H. (2016). Why do they do what they do? A study of what motivates users to (not) follow computer security advice. Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS), 161–175.
[9.] Stobert, E., & Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS), 243–255.
[10.] Habib, H., Emami Naeini, P., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N., & Cranor, L. F. (2018). User behaviors and attitudes under password expiration policies. Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS), 13–30.
[11.] Vance, A., Eargle, D., Jenkins, J. L., Kirwan, C. B., & Anderson, B. B. (2019). The fog of warnings: How non-essential notifications blur with security warnings. Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS), 407–420.
[12.] Wash, R., Nthala, N., & Rader, E. (2021). Knowledge and capabilities that non-expert users bring to phishing detection. Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS), 377–396.
[13.] Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS), 259–284.