TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Human Error: The weakest link in cybersecurity

Even with Ultra-Modern Security measures, organizations or companies remain unprotected and exposed because of human mistakes. This brings out a very urgent matter_ Human error is the weakest link in cybersecurity.

By Hamna Shafiq | University of Agriculture, Faisalabad | Published: June 2026
hamnshafiq83@gmail.com | Position: Student

Introduction

In today's technological era, cybersecurity has developed into utmost concern of any organization. Organizations invest in advanced technologies like encryption, security software and firewalls to safeguard their data from activities like theft, threats and misuse. Yet their data is just as vulnerable as leaf just because of the errors made by humans. Human little mistakes like clicking on unknown and suspicious links, having repeated and weak passwords or neglecting important security instructions can easily reveal sensitive and important data to unknown threats. This indicates that no matter how modern technology molds, Human errors are gonna be the weakest link in cybersecurity.

> ***"In the world of cybersecurity, the greatest threat is often not the hacker, but the human user.***

Types of Human Errors in Cybersecurity

The most frequent and prominent human errors in cybersecurity are:

1. **Phishing Attacks:**

   Phishing error is the error is the error that occurs when a person is tricked into clicking suspicious links to unveil sensitive information.

   For example, A person receives an email claiming from their respective bank but actually attacker is tricking him into clicking his own link to get his bank data.

2. **Repeated and weak passwords:**

   Using same and easy to guess passwords repeatedly allows the attacker to access and steal data.

   For example, You set a password "12345678" .This is the most common password ever exist. The hacker can easily guess this and can gain access.

3. **Accidental Data Exposure**

   Mistakes like unintentionally exposing your data like sending personal pictures or emails to wrong person or uploading confidential information of company to unknown site can have serious impacts.

   For example: A employee lost his laptop that have client's confidential data that is not protected with encryption. Now anyone can see that data in the laptop.

Technology Overview

Today's cybersecurity heavily depends on the advanced technologies design to secure your systems from cyber threats. Companies use systems like antivirus software, Encryption techniques, IDS and firewalls to protect from unauthorized access and illegal activities.

For example, Firewall like Cisco Secure Firewall assist to keep check on incoming or outgoing traffic and antivirus software like Window Defender find and remove suspicious software.

Many organizations also use multi-factor authentication using frameworks like Microsoft authenticator or Google authenticator, which give more security other than password. Yet, even after these modern technologies, cybersecurity can never be foolproof. Human still make mistakes like ignoring alert notifications and not implementing proper instructions. This pinpoints that although technology can be the most important in cybersecurity, yet we cannot completely get rid of human errors in cybersecurity.

Figure 1: Explaining Technology overview in cybersecurity.

Impact

Impacts: Human error can have major impact for persons as individuals and for companies as well. Even a very minor negligence or mistake may lead to huge disasters.

The biggest impact is **Data Breach.** When personal information like someone's ATM number or Medical history gets leaked, it can be used in illegal activities or can also be used to harm him personally.

Another major effect is **financial loss**. In today's times, every individual, business or organization is using online banking. If confidential data of any bank gets stolen, everybody is going to bear the damage.

Reputation of any organization is also at risk if company's systems got hacked or attacked.

What's Next? (Solutions)

Solutions: Even though we can't completely eliminate human errors but still we can overcome them by proper measures.

The most reliable and effective measure is **Public awareness and training.** Users and employees should be educated about common threats like weak passwords and phishing.

Another way to reduce error is **unique and strong passwords**. Passwords should not be common that can be easily guessed but combination of random letters and numbers to avoid guessing.

Companies and organization should also deploy **Multi-factor authentication (MFA).** This adds an extra layer to security even if attacker have the password, it would be difficult for him to gain access.

Regular security updates and reminders to the users can also help reduce errors. Simple alerts and instructions helps user follow safe practices.

Conclusion

To conclude, while some advancements have taken place within the realm of cyber security technology in order to ensure better protection from attack, the one weak link in any chain is invariably the human element. Simple mistakes like using weak passwords, falling for phishing attacks and ignoring security notifications can bring huge disaster.

By using strong passwords, raising awareness among people, providing regular training and regular updates can overcome security threats. Ultimately, educating people and strengthening human element are essential to create a secure and reliable cybersecurity environment.

About the Author

Hamna Shafiq is a IT student at Agricultural university. She can be reached at hamnashafiq83@email.com.

References

[1] National institute of standard and technology (2023). *Cybersecurity Framework*.

[2] Cisco. (2024). *Cybersecurity Basics*.