Human Error as the Primary Attack Vector in Modern Cyber Security

Written by: Sabit Esati – Cyber Security & IT
Education: RMIT University & Chisholm Institute

Introduction

In modern cyber security, organisations invest heavily in security mechanisms such as firewalls, endpoint protection, encryption, and intrusion detection systems. While all of these are important, they do not remove one key vulnerability in any system — the human user.

Human factors remain a major threat in cyber security, with a large percentage of attacks occurring not because of technical failures, but due to human error (Verizon, 2024). Attackers increasingly exploit human behaviour through weaknesses such as deception, manipulation, and psychological tactics, allowing them to bypass even well-designed security systems. This shows that cyber security is not purely a technical field, but one that must also consider human behaviour.

Understanding Human Error in Cyber Security

Human error in cyber security refers to mistakes or decisions made by users that can put the confidentiality, integrity, or availability of systems and data at risk. In most cases, these actions are not malicious and usually happen during normal working conditions, such as time pressure, multitasking, or simply not thinking twice in the moment.

For example, an employee working under pressure might open an email attachment without properly checking where it came from. Another common situation is password reuse, where users choose the same password across multiple platforms because it is easier to remember. These actions aren't done with bad intent but are a result of normal human behaviour and the tendency to prioritise convenience.

Human error can also occur during system setup or configuration. Misconfigured cloud storage, incorrect permissions, or missed updates can lead to sensitive information being exposed. In many cases, this isn't because the user lacks technical knowledge, but because systems can be complex and easy to get wrong (European Union Agency for Cybersecurity, 2023).

Why Attackers Target the Human Element

From an attacker's perspective, targeting users is often easier than trying to break through the technical security of modern systems. Most systems today are designed to detect and block suspicious activity, which makes direct attacks more difficult and time-consuming.

People, on the other hand, are generally more predictable and easier to influence. Attackers take advantage of this by using psychological tactics such as urgency, authority, and trust. For example, a common phishing email might warn a user that their account will be blocked unless they take immediate action. Under pressure, users are more likely to react quickly without properly checking the situation.

A typical scenario involves an attacker pretending to be part of the company's IT department and asking employees to reset their password using a link sent via email. When the user clicks the link, they are redirected to a fake login page where their credentials are captured. The attacker can then use this information to access internal systems as a legitimate user.

In cases like this, the attacker isn't breaking into the system directly. Instead, they rely on normal human behaviour to gain access, effectively bypassing security controls.

Common Human-Centric Attack Methods

Phishing remains one of the most commonly used attack methods, as many users are targeted through deceptive emails or messages (Proofpoint, 2023). These messages are often designed to look legitimate and are usually sent in the name of trusted or well-known organisations, which makes them harder to detect.

Password-related issues are another common problem. Many people reuse the same password across multiple websites or choose simple, easy-to-remember combinations. If one account is compromised, attackers can use those same credentials to try and access other systems using similar techniques (Microsoft, 2023).

Social engineering is not limited to emails and can also happen through direct interaction. For example, an attacker might pretend to be from the IT team and contact an employee by phone to request login details. In situations like this, the attack relies more on trust and communication skills than technical ability.

Insider-related incidents are also a source of security risk. Employees may accidentally share sensitive information with the wrong person or use devices that are not properly secured. Many reports highlight how human error continues to play a significant role in these types of incidents.

Impact of Human Error on Security

Human error can have a major impact on cyber security. Mistakes made by users can lead to data leaks, financial loss, and unauthorised access to sensitive information.

For example, a user might open a malicious link in an email without realising the risk. This can install malware on their device, allowing attackers to move through the system, gain higher levels of access, and eventually reach critical areas. What seems like a small action can quickly lead to serious damage.

Research shows that cyber security incidents caused by human error can be highly costly and damaging for organisations (IBM Security, 2023).

Mitigation Strategies

While human error may not be entirely avoidable, organisations can take steps to reduce how often it occurs and limit the damage it can cause. One of the main approaches is regular security awareness training, which helps users better understand common threats such as phishing. Over time, this encourages safer behaviour in everyday tasks.

Multi-factor authentication (MFA) is another important control. Even if a password is stolen, the extra verification step makes it much harder for attackers to gain access (National Institute of Standards and Technology, 2017). Password managers can also help users create and manage strong, unique passwords for different accounts or systems.

System design also plays a key role in reducing user error. For example, applying the principle of least privilege ensures that users only have access to what they need to perform their role. Automated updates and built-in security controls further reduce the chances of mistakes by limiting the need for user decisions.

Finally, building a strong security culture within an organisation helps reinforce these measures. When employees treat security as part of their everyday work, they are more likely to stay aware and respond appropriately to potential threats.

Conclusion

Human error remains one of the most significant vulnerabilities in modern cyber security. Despite ongoing advancements in technology, attackers continue to succeed by targeting people rather than systems (Verizon, 2024).

This highlights the need for a balanced approach that combines strong technical controls with an understanding of human behaviour. By improving awareness, applying effective

security measures, and designing systems that account for human limitations, organisations can reduce their exposure to cyber threats.

Ultimately, cyber security is not just about protecting systems, but about ensuring people can use them safely and responsibly in real-world situations.

References (APA 7th Edition)

Verizon. (2024). *2024 Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

IBM Security. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/reports/data-breach

National Institute of Standards and Technology. (2017). *Digital identity guidelines (NIST SP 800-63B)*. https://pages.nist.gov/800-63-3/sp800-63b.html

Australian Cyber Security Centre. (2023). *ACSC annual cyber threat report 2022–2023*. https://www.cyber.gov.au

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu

Proofpoint. (2023). *State of the phish report 2023*. https://www.proofpoint.com

Microsoft. (2023). *Microsoft digital defense report*. https://www.microsoft.com/security