JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Human Factors in Cyber security: Understanding and Mitigating User Risks

Ashish Uday Shivalkar
Co-Founder, HACKANICS
Mumbai, Maharashtra

Abstract- Cybersecurity is not inherently a technology problem—it is also a human one. As threats become more sophisticated and large-scale, human error is a chronic and primary risk. This research paper explores the human factors contributing to cybersecurity risk, including cognitive overload, unawareness, social engineering susceptibility, and ineffective training. Based on cross-disciplinary research in psychology, information security, and human-computer interaction, the present study explains common behavioral patterns resulting in security violations. The study also examines the efficacy of various mitigation measures, viz., user-centric security design, behavioral training programs, and real-time decision aiding systems. The study concludes with a proposed framework for the integration of human factor assessment into organizational cybersecurity practice, ultimately promoting a global approach towards balancing technological defense with man-centered solutions.

Keywords— *Human Factors, Cybersecurity Awareness, Social Engineering, Phishing Attacks, Cognitive Bias, Insider Threats, Security Culture, Behavioral Cybersecurity, Security Awareness Training (SAT), Human Error, Deepfakes, AI-Driven Attacks, Synthetic Identity Fraud, Zero Trust Security, Multi-Factor Authentication (MFA), Psychological Manipulation, Security Fatigue, Organizational Policy, Adversarial AI Attacks, Federated Identity Validation*

INTRODUCTION

As the internet gets more networked, safeguarding information takes more than the deployment of the newest technology. It's also a function of the way people act on a daily basis. Of course, technologies like firewalls and encryption get better, but people can be a good defense or a bad weak link. Just like security compromise is a function of careless errors—like the use of weak passwords, opening phishing messages, accidentally sharing sensitive documents, or misconfiguring devices.

That is why it is necessary to know how humans act. Organizations really have to contend with these human threats for their cybersecurity to be effective. Cyberthieves prefer to exploit people's psychology against them, employing deceptions such as social pressure or distraction to bypass even the most secure security. That leaves anybody employees, contractors, or partners vulnerable, and they're most likely the easiest to take advantage of. Successful cybersecurity policy must combine good technology with ongoing user education, good guidelines, and positive reinforcement to enable safer decisions. This paper addresses the interface of psychology and social behavior with work behavior and provides practical guidance on reducing risk from people and on creating a culture in which security is always the top priority.

COMMON HUMAN-RELATED CYBERSECURITY THREATS

Human cybersecurity attacks are created by people either mistakes, carelessness, social-engineering trickery, or outright misuse of systems. They are the biggest cause of security issues across all industries, no matter how secure an organization makes its technology. To secure digital systems, good technology is needed along with making users display the right behavior, policies, and procedures.

1. **Phishing**
   Phishing is a prevalent cyber assault in which attackers pretend to be trusted sources or institutions. They forge messages or emails to trick users into revealing sensitive information, like passwords, credit card numbers, or login information.

Tools (Kali/Linux/Industry):

- Gophish
- Social-Engineer Toolkit (SET)
- Evilginx2
- King Phisher

Real-Life Incident Example:

Google and Facebook were defrauded of over $100 million between 2013 and 2015 by the phishing emails containing fake invoices by a gang that posed as a hardware supplier.

Impact:

It is capable of stealing login credentials, distributing ransomware, and resulting in enormous financial loss, wiping out company networks and customer trust.

1. Social Engineering

Social engineering is a technique for tricking people into sharing secret information or into taking security-compromising actions. Rather than attacking systems, the attackers attack people's actions to overcome technical defenses.

Tools (Kali/Linux/Industry): -

-Maltego

-SET

-Sherlock

- Recon-ng

Real-Life Incident Example: - Young hackers in 2020 concocted a fairly elaborate plan by convincing Twitter employees to give them access to the company's internal networks. They were able to hijack big accounts, including those of Elon Musk and Barack Obama, to pitch a bogus cryptocurrency scam.

Tactics:

- **Impersonation:** They impersonated a trusted individual, for example, a manager or tech support.
- **Pretexting:** They fashioned false narratives just to have individuals share confidential information.
- **Baiting:** They enticed victims with complimentary products, like a USB drive, that made them perform dangerous activities.
- **Tailgating:** They gained access to secure areas by following behind a person, exploiting social norms like leaving a door open.

2. Credential Misuse

Misuse of Credentials is when the attackers gain access to the usernames and passwords. This is typically the case since users have weak passwords, use them across different websites, or have them stolen in data breaches. With this access, unauthorized folks can log in and see sensitive information.

Tools (Kali/Linux/Industry): -

- Hydra
- Hashcat
- John the Ripper
- Medusa

Real-Life Incident Example: - In 2012, Dropbox was hard hit when 68 million user passwords were hacked. Dropbox was tricked by the hackers through stolen login credentials from an earlier LinkedIn breach. Dropbox did not have multi-factor authentication (MFA) at that time, which left it even more exposed.

Threats: - When credentials are utilized for malicious intents, they lead to brute-force attacks, credential stuffing, system unauthorized access, and data breaches. All these attacks lead to significant security breaches and compliance violations.

3. Insider Threats

This is a cybersecurity risk that comes from inside an organization. It can involve employees, contractors, or trusted individuals who either intentionally or accidentally misuse their access, which can result in data breaches or other security issues. These insiders might act on purpose, be careless, or have their accounts hacked by outside attackers.

Tools (Kali/Linux/Industry): -

- OSSEC
- Wazuh
- Auditd
- ELK Stack
- Splunk

Real-Life Incident Example: - In 2013, Edward Snowden, a contractor with the NSA, released a pile of classified information through his access. This is one of the most well-known examples of an insider causing trouble.

Types:

- **Malicious Insiders**: Malicious Insiders These individuals specifically go out of their way to hurt the company. They might be disgruntled employees, individuals wishing to make money, or individuals who hold a grudge against the company. Their actions can include stealing data, sabotaging the company's systems, or committing fraud.
- **Negligent Insiders**: Such users make mistakes that, by default, expose them to attacks. Some examples include the use of weak passwords, failure to follow security protocols, or sharing sensitive information with the wrong individuals inadvertently.
- **Compromised Insiders**: These people have their credentials or access compromised by third parties. Phishing attacks, malware, or any other form of takeover can be used by attackers to hijack an insider's account. This allows them to see systems and data as the legitimate user.

4. Lack of Cybersecurity Awareness

Unless security is trained into the users, they may not have the training and experience needed to recognize and defend themselves against cyber-attacks. This might make them vulnerable to being exploited through the use of techniques such as phishing, malware, and social engineering, all of which may result in serious security problems.

Tools (Kali/Linux/Industry): -

- KnowBe4
- LUCY Security
- Security Shepherd
- PhishMe

Real-Life Incident Example: - Sony Pictures was attacked hard in 2014 when its employees accidentally clicked on emails that were phishing. The result of this was the leakage of sensitive information, such as private files and emails. It was later discovered that the attack was conducted by a group affiliated with North Korea.

Impact: - Lack of awareness of security matters may cause one to lose data, damage a company's reputation, and allow unauthorized individuals to access internal systems. Therefore, it's advisable for companies to invest time and resources in frequent training of employees.

5. Shadow IT

Shadow IT occurs when staff utilize software, applications, or equipment that has not been sanctioned by the IT department. These unauthorized tools pose security threats as they do not adhere to the standard policies, and it becomes easier for breaches of data or cyberattacks to occur.

Tools (Kali/Linux/Industry): -

- Wireshark
- Netdiscover
- Nmap
- Tenable Nessus
- OpenVAS

Real-Life Incident Example: In 2013, Target experienced a major data breach when hackers accessed the internal network through a third-party HVAC vendor that had an unauthorized connection. This breach allowed them to steal information from over 40 million payment cards.

Risk: - Shadow IT can bypass security measures, create unwatched attack surfaces, and make it difficult for IT teams to monitor and secure systems properly.

6. Human Error

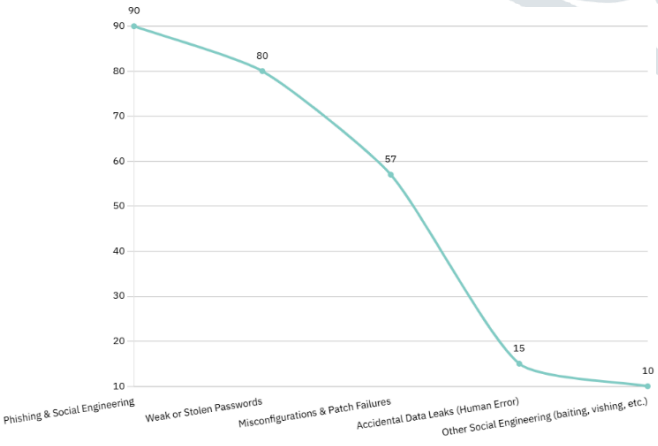
Human error in cybersecurity happens when users or admins make unintentional mistakes that can compromise security. This includes setting up systems incorrectly, mishandling sensitive information, or not installing important security updates. These mistakes can raise the risk of cyberattacks or data breaches.

Tools (Kali/Linux/Industry): -

- Ansible (automation)
- Lynis
- OpenVAS
- Bash scripts (audit configs)
- CIS-CAT

Real-Life Incident Example: - In 2019, Capital One had a big security problem when a mistake with a firewall in their AWS cloud setup let a former employee get into over 100 million customer records. This incident showed how even small setup errors can lead to serious data leaks.

Impact: - Human mistakes can cause problems with systems, lead to data leaks, and create issues with meeting security rules. That's why it's important to use automated tools, have clear steps in place, and conduct regular checks to lower these risks.



PSYCHOLOGICAL ASPECTS INFLUENCING USER BEHAVIOR IN CYBERSECURITY

Getting a grip on how people think and act is really important for keeping cybersecurity strong. A lot of security issues arise not from tech failures, but from how users understand information, make decisions, and respond in everyday work situations. These behaviors are shaped by human psychology, which can either boost security or lead to big risks. Here are some key psychological factors that affect how users behave and influence an organization's security.

1. Cognitive Biases

These are the mental shortcuts people use to save time and energy when making decisions. In cybersecurity, though, these shortcuts can be a huge liability. For example, someone might see a suspicious email and think, “Eh, it’s probably nothing,” and click on it anyway. That’s a bias at work—making people ignore risks or skip proper checks. These psychological factors are a big deal: they shape user behavior and can either strengthen an organization’s security or leave massive holes for threats to walk right through.

- **Authority Bias**: People can follow a superficial request just because it seems to come from someone important, as a manager. This makes phishing attempts that pretend to be the high -ranking team particularly risky.
- **Urgency Bias**: If a message creates a sense of urgency, such as saying that an account will be blocked in 10 minutes, users can run to act without thinking. This increases the likelihood of falling for a scam
- **Confirmation Bias**: Folks tend to trust messages that line up with what they already think or believe. So, they might overlook warning signs if the content seems familiar or believable.

Impact: These biases can make it tougher for users to make smart, security-conscious choices, which makes it easier for attackers to take advantage of this behavior and get around technical protections.

2. Habituation

The habit occurs when people keep watching the same security alerts such as pop-up warnings, indicating reminders or software updates to change the password. After repeatedly looking at these messages, users can start ignoring them, known as "alert fatigue". This can cause problems over time, as users can actually allow or ignore without thinking about risks as they are used for alerts. When people stop paying attention to the warning, it weakens the safety of the organization, which is more likely that a person will accidentally miss the signals of malware, phishing, or forget to update his software.

Impact: Habit makes users less attentive, which can make the best security systems less effective if people keep ignoring or rejecting significant alerts.

3. Social Influence

Social impact is a great factor that how people work in relation to cyber security. In the workplace, employees often see their colleagues to find out what is normal. If they see others ignoring safety rules or sharing passwords, they may feel willing to do so, even if they know that it is wrong. This behavior is shaped by workplace culture, which can either promote good safety practices or encourage risky behavior. If

no one is following the rules, users may feel less motivated to stick to cyber security policies.

Impact: A weak security culture, which is inspired by poor colleague effects, can cause widespread rules, which can make the organizations spread threats to strengthen their defense and spread the dangers.

4.*Overconfidence*

Extreme confidence occurs when users feel that they know more about cyber security, as they actually do. This false sense of safety may motivate them to take unnecessary risk or ignore important security steps. For example, one can leave the necessary safety training, turn off the antivirus software, or assumes that they can always see a phishing email, even when they can still be at risk. These actions can result in a result of security mistakes, even realizing it. This mentality is particularly risky because confident users cannot help, update or advice, thinking that they already know everything. Finally, it can create safety gaps in the organization.

Impact: Extreme confidence reduces awareness about risks, leads to more rules, and may be bad options, leading to the organization more weakened for cyber threats.

Emotional Triggers

Emotional trigger are strong feelings such as fear, stress, curiosity or excitement that can actually affect how people think and work. They can motivate people to make quick decisions without thinking about the risks involved. Cyber attackers know this and often use these emotions in their misleading messages. For example, they offer fake jobs, threats about legal issues, or messages that they see to someone you care to careful. The purpose of these strategies is to click on the link, open attachment or share personal information. When emotions are over, people can leave security steps, ignore warnings, and fall to social engineering scams. This type of manipulation works as it urges to work faster during emotional moments.

Impact: Emotional trigger can play with decision making, which can cause risky behavior, and make people more vulnerable to phishing, scams and malware.

5. Mental Workload and Distraction

When employees are busy or distracted, they struggle to follow safety procedures. This condition is known as a high cognitive load - when one is juggling a lot of tasks at once, it becomes difficult to focus or make a safe option. In these cases, users can ignore vital steps, click on the shady link, or disregard safety alerts to save time. This is especially common in a fast -paced jobs where people feel quick or overwhelmed. The attackers often take advantage of this by sending phishing emails during extreme work hours or by preparing immediate messages, to find out that users are more likely to make their decisions.

Impact: High mental charge means that users pay less attention, which increases the possibility of mistakes and weakens safety compliance..

Impact of Human Error on Cybersecurity Incidents

Human error is still one of the biggest reasons behind cyber security violations in various industries. Even though organizations use advanced equipment such as firewalls and encryption, many attacks are successful due to simple mistakes. These errors can come from employees, contractors or system admins and can also get the strongest defense. Common mistakes include clicking on phishing email, wronging safety settings, sending information to the wrong person, or forgetting to update the software. These errors are usually inadvertently, but data leaks, system breeches or financial hits may result in results.

Impact: Human errors can seriously harm an organization's ability to keep information safe and reliable. To cut down on these risks, companies should mix tech with clear guidelines, regular training, and automated tools that catch and fix mistakes before they cause trouble.

TYPES OF HUMAN ERROR IN CYBERSECURITY

Human errors come in many shapes and forms, often caused by overlooking something, a lack of awareness, or just going through the motions. These slip-ups can create real security issues for an organization. Here are some common types:

1. Misconfigurations

If servers, firewalls, or cloud settings aren't set up right, they can leak sensitive info or let unauthorized people into internal systems. This usually happens because things are done too quickly or the person setting them up doesn't have the right know-how.

Impact: - Misconfigurations can result in data leaks, issues with compliance, and potential system problems

Phishing Clicks

A lot of people accidentally click on links or open attachments in phishing emails. These emails look genuine and can trick users into downloading harmful software or giving up their login info. Impact: This can lead to identity theft, ransomware, and unauthorized access to company networks

Impact: This can lead to identity theft, ransomware, and unauthorized access to company networks. Weak or Reused Passwords

2. Weak or Reused Passwords

Using easy-to-guess passwords or the same password for different accounts makes it simpler for attackers to break in using brute-force methods or by taking advantage of leaked data from other breaches.

Impact: Weak passwords can give hackers full access to systems without triggering any security alerts.

3. Unpatched Systems

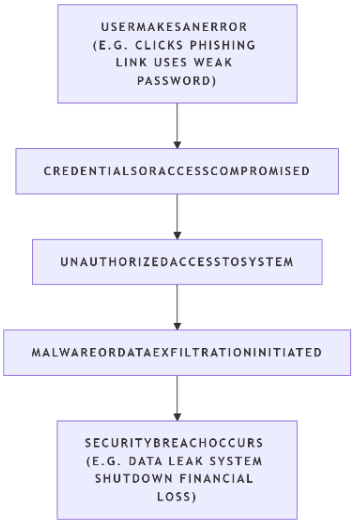
Not keeping software updated or failing to install security patches leaves known security holes open. Attackers often search for outdated systems to exploit.

Impact: Unpatched systems are a common target in big cyberattacks.

4. Accidental Data Sharing

Sometimes users send private files to the wrong person or upload sensitive documents to unsafe places, such as public cloud storage or shared folders without proper security.

Impact: This can cause data leaks, fines from regulators and loss of trust from customers.



SOCIAL ENGINEERING A N D

PHISHING TECHNIQUES

Cyberattacks do not usually start with cracking computers; they start with messing with people first. Little tricks like social engineering and phishing are how cyberthieves manipulate human nature and not technology. These attacks are easy to perform and effective because they rely on trust, emotions, and tricks to trick people into divulging sensitive information, clicking on bogus links, or giving access without permission. By messing with people, attackers can usually get past even strong security controls easily.

Social Engineering: - Social engineering is a method of cybercrime that uses psychological manipulation to influence individuals. Instead of attacking systems, they manipulate individuals into sharing personal details or by doing dangerous actions like disabling security measures or revealing confidential details. They tend to rely on trust, fear, urgency, or curiosity to guide the victims' decisions.

Phishing: - Phishing is a very common social engineering attack. Phishing scammers send fraudulent emails, messages, or texts pretending to be from a familiar source. They try to make you click on a malicious link, download a malicious attachment, or reveal personal information such as usernames, passwords, or credit card numbers. Because these messages can appear very authentic, phishing can easily deceive users and bypass technical security controls

TYPES OF SOCIAL ENGINEERING ATTACKS

ATTACK TYPE	DESCRIPTION
PHISHING	Sending fake emails or messages that make you look real to look real to click on a malicious link or to give sensitive information like password or account number.
SPEAR PHISHING	A more targeted form of phishing, where the attacker adapters the message to a specific person or organization using individual details.
WHALING	A type of phishing attack aimed at the purpose of high-level officers (e.g CEO or CFO) to steal confidential commercial data or authorize fraud.
VISHING	Voice phishing—fraudulent phone calls pretending to be from banks, IT support, or government agencies to get you to share personal or financial details
SMISHING	SMS phishing—sending fake text messages that try to trick you into clicking links, installing malware, or giving up private information.
PRETEXTING	To create a false story or identity (such as pretending to be an HR or seller) to create faith and to convince you to express personal or safe information.
BAITING	Offering some breathtaking (a free USB drive, music file, or like download) that includes malware or provides access to your system to the attacker.
TAILGATING	Getting physical access into a restricted field by closely following a writer-Z person without proper authentication done in workplaces.

HOW THESE ATTACKS WORK (PSYCHOLOGICAL TECHNIQUES)

Cyber aggressors usually manipulate human psychology to ignore logical thinking and make victims act without checking the facts. These tactics depend on emotional responses rather than rational decision-making. Here are the common psychological methods used:

Authority
concept: Attackers pretend to be someone in a position of power (e.g., company CEO, IT administrator).
Objective: To make the victim obey quickly without question.
Example: An email from a "boss" asking to transfer money urgently.

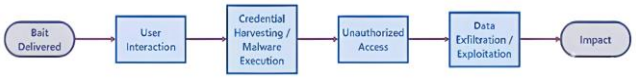
Urgency
concept: Creating a false sense of time pressure.
Objective: Prevent the victim from thinking carefully or verifying facts.
Example: "Your account will be blocked in 10 minutes unless you log in now."

Trust
Concept: Impersonating a trusted individual or organization.
Objective: Make the victim feel safe and lower their defenses.
Example: A phishing email that appears to be from a bank or a trusted coworker.

Fear
Concept: Using threats or alarming messages to pressure a quick reaction.
Objective: Intimidate the victim into compliance.
Example: "Your device has been hacked. If you do not pay within 24 hours, your data will be leaked."

How to Defend Against Social Engineering and Phishing

Protection Method	Why It Helps
Security Awareness Training	Educates employees on how to identify and avoid suspicious emails, links, and messages. It builds cybersecurity awareness and improves user vigilance.
Email Filtering and Sandboxing	Uses tools to automatically detect and block harmful emails. Suspicious attachments and links are tested in a safe, isolated environment before they reach the user.
Multi-Factor Authentication (MFA)	Adds an extra layer of protection. Even if your password is stolen, invaders need a second verification code (such as a text or application notification) to gain access.
Phishing Simulations	Simulated attacks sent to employees to test their ability to recognize phishing attempts. Helps identify training needs and improve response.
Zero Trust Security Model	Assumes no user or device is automatically trusted—even inside the network. **Every access request must be verified**, reducing the risk of internal or external threats.
Incident Response Plan	A clear, step-by-step plan that helps teams **respond quickly and effectively** when a cyberattack happens. Reduces damage and improves **recovery time**.



Cognitive Biases and Decision- MAKING FLAWS

Every day, we make a lot of decisions - some are simple, while others are difficult. All these options are not made with clear arguments. Cognitive bias is very low -minded errors that we can understand how to understand and decide things. These quick mental shortcuts, called heuristics, help us respond fast in daily life. But when it comes to cybersecurity, especially during stressful times, these biases can lead to bad choices that open the door to security issues. Attackers know how to exploit these weaknesses in our thinking to trick people and get past security measures.

Cognitive Bias: - It's basically a way our brains can process information that doesn't always lead to the right conclusions or choices. These biases can change how we focus, remember stuff, solve problems, and grasp what's going on. In cybersecurity, they can make users more likely to overlook risks, get caught in scams, or make errors that put security at risk.

Bias	Description
Confirmation Bias	Only focus on information that we already believe, while ignoring anything that contradicts it. This can lead to biased decision making and real danger
Anchoring Bias	Keeping a lot of importance on the first piece of information we see, even if better or new information is available. This can cause decision errors in assessment of danger.
Availability Heuristic	Making decisions based on events that are recent or easy to remember, rather than on actual data. This can distort risk perception and lead to overreaction or underestimation of threats.
Overconfidence Bias	Thinking we know more than we actually do, which can result in ignoring security advice or taking **unnecessary risks**.
Status Quo Bias	Preferring to keep things the same rather than making necessary changes, even when those changes improve **security posture**.
Bandwagon Effect	Just going along with what everyone else is doing without thinking about whether it's safe or makes sense in a security situation.
Framing Effect	To be affected by how information is presented instead of facts. For example, how to answer differently to a safety warning based on the word.
Sunk Cost Fallacy	A poor decision or sticking with the old system is just because time, money or effort has already been invested, even when switching will be safe or more efficient.

Impact on Decision-Making in Cybersecurity

Cognitive biases are a factor in cybersecurity that causes people to make decisions that raise risk, weaken security controls, and ultimately delay taking important actions. The impact of cognitive biases can include IT professionals all the way down to everyday users and can result in poor security choices.

For example,

- A system administrator may dismiss a legitimate alert due to confirmation bias, thinking that it is only another false sense of security, and could miss a critical threat.
- A user may fall for a phishing email due to the availability heuristic, because they can recall a similar email that did not appear to be malicious, resulting in credential theft or malware.
- A security team may rely on old processes or tools because of status quo bias. While mature processes and tools will become outdated, the team may avoid change out of fear it will affect the operation and it will turn out to be a better solution.

Impact: While there are many cognitive biases that have an impact on security, it is important for organizations to recognize cognitive biases and be able to address them through training and improved decision-making frameworks to assist in risk management, incident responding, and organizational security posture.

REAL-LIFE EXAMPLES: -

1). Aflac Data Breach (June 2025)

In June 2025, Aflac, an insurance company, suffered a cyberattack. This attack was not a typical ransomware type of attack. Rather, it was carried out using social engineering where employees were deceived into providing valuable information.

In this attack, it is believed that the attackers are part of a group called "Scattered Spider". The attackers impersonated trusted IT support people. The attackers called and messaged employees persuading them to surrender their login credentials or to click on malicious links. This is a good example of voice-phishing, or vishing.

Best security practices were followed, so Aflac's technical systems were safe, but the attackers used social engineering to circumvent those controls by confusing or deceiving people. They had gotten into Aflac through deception. Meanwhile it is suspected that personal data, possibly social security numbers, insurance information, and maybe even medical information, was exposed and put at risk.

Why it matters:

- Reminds us that cyberattacks are often all, or mostly, about people and not just machines.
- Exemplifies the importance of Security Awareness Training and verifying identity especially over the phone and chat.
- Reinforces the necessity for organizations to have strong incident response plans, to respond quickly, and to mitigate damage.

1). Marx and Spencer (M&S) Social Engineering Attack -

April 2025 in April 2025, the UK Retail Company Marx and Spencer (M&S) became a target of a cyber-attack, which did not include hacking its system directly. Instead, the attackers used social engineering to cheat workers in one of the third-party service providers of M&S.

What happened:

The cybercriminal contacted the employees of the company using fake phone calls and phishing emails. He pretended to be from M&S's internal team and assured the workers to reset passwords and reach important systems. This allowed the attackers to bypass technical rescue and enter the network using reliable credentials.

What was affected:

There were major problems in this attack, including online service disruption and delay. Personal data related to customers and employees may be theft. Estimated financial losses can reach £ 300 million due to lost trade and recovery costs.

why it matters:

This phenomenon suggests that even if the internal systems of a company are safe, the third-party risk and human error can still lead to major violations. This proves importance:

- Vendor Risk Management
- Security Awareness Training
- Strict access control policies
- Verification procedures for sensitive works

COGNITIVE BIAS IN SOCIAL ENGINEERING

Often, cybercriminals will exploit cognitive biases to develop accusations that could look like social engineering, as it is human seem to be constantly taking mental shortcuts that defines their reactivity--especially when emotions prevail, trust is extended, or we are under pressure. There are three biases we want to highlight and how they affect the victims of social engineering attacks: -

- **Authority Bias: -** Attackers will pretend to be someone of authority in the workplace. For instance, a manager, supervisor, or even IT support staff. Lots of times, people comply with direction from authorities without thinking. In these cases, attackers are by satisfying the victim's desire to stay under the radar and/or save the victim time.
- **Urgency Bias: -** Attackers will create urgency or time pressure. For instance, they may send the target the following message: "Your account will be disabled in 5 minutes". Offers for action that have been presented under time pressure lowers personal risk awareness, thus creating impulsiveness.
- **Reciprocity Bias: -** Finally, attackers will usually offer help, gifts, or a small service to the victim. Which leads to an attitude of it is acceptable (normal) to repay another like that. This social pressure tells the victim that they "owe" in some sense to reciprocate or repay the attacker in what ever form they wish.

Impact: - These cognitive tricks increase the effectiveness of an attacker delivering a social engineering attack when the victim is experiencing cognitive dissonance. Your goal should be to understand that the mental complications of the victim has increased significance for social engineering to be in your favor, creating some habits to protect against social engineering will greatly reduce your risk of exposure to all the psychological tricks your enemy would use in an attack.

How to Reduce Bias in Cybersecurity Decision-Making

Cognitive biases can lead to poor security decisions. The following strategies help reduce the influence of bias and improve risk awareness, critical thinking, and decision quality.

STRATEGY	HOW IT HELPS
Awareness and Training	Teaching employees about common **cognitive biases** helps them recognize and avoid **flawed thinking** in real-world security situations.
Checklists and SOPs	Using **checklists** and **standard operating procedures (SOPs)** supports **structured decision-making** and reduces the effect of emotion or pressure.
Red Team / Blue Team Exercises	These **simulated attack-and-defense exercises** help identify weaknesses from different angles and reduce **groupthink** by promoting **alternative viewpoints**.
Diverse Teams	Bringing people with different backgrounds and experiences together improves problems and leads to more balanced, purposeful decisions.

Data Driven Analysis	Instead of relying on the feelings or beliefs of the intestine, encourages the use of evidence-based insight, which helps in making accurate, rational decisions.
Time Buffers for Decisions	Permission for additional time for reviews and reflections reduces the decisions that are affected by stress or prejudice, improve the overall decision quality.

IMPACT OF HUMAN ERROR ON CYBERSECURITY INCIDENTS

Human error is one of the greatest reasons why cyber security violations happen around the world. Although organizations invest in strong security tools such as firewalls, cryptography and artificial intelligence (IA), they are usually the actions of people who create the greatest risks. Common errors include:

- Click on phishing and emails
- Incorrect security settings
- Do not report suspicious activities

These actions can give cybercriminals a path to systems, usually without having to break the technical defenses. Human errors in cyber security are usually divided into two main types:

- Skill -based errors:

They are small, usually automatic errors that occur during routine tasks. For example, sending an email to the wrong person or incorrectly configuring a server or firewall. They are usually caused by distraction, fatigue or multitasking.

- Decision -based errors:

This occurs when someone makes a bad judgment or incorrect decision, usually due to lack of knowledge, training or being deceived. For example, falling in love with a phishing blow by sharing confidential files without checking or ignoring a security alert.

ALARMING STATISTICS HIGHLIGHTING HUMAN ERROR IN CYBERSECURITY

Recent data clearly shows that **human error is a leading cause of cybersecurity incidents**, across all industries and organization sizes. Despite advanced technologies, people still play a major role in how cyber threats succeed.

- In 2024, approximately 95% of data violations included some forms of human fault. This includes clicking on phishing email, using weak or stolen passwords, making configuration errors, or insider mistakes.
- Several cyber security reports and annual research found that 68% to 74% of security violations involved the human element, showing that technology alone is not enough without addressing behavior and awareness.
- According to Mimecast, only 8% of employees account for about 80% of security incidents reported in some organizations. The average cost of insider -related data leaks is estimated at about $ 13.9 million per incident.
- In cloud environments, 44% of violations were linked to incorrect configurations a direct result of human supervision or lack of proper training during system configuration.

CASE STUDIES: REAL INCIDENTS INVOLVING HUMAN ERROR

1. CHANGE HEALTHCARE RANSOMWARE ATTACK (2024)

In 2024, a major American healthcare technology company, Healthcare Change Healthcare, faced ransomware attack after an employee clicking on the phishing email. The attacker stole login credentials, which was then used to achieve unauthorized access throughout the network. This caused major disruption in healthcare services and patient billing systems.

Key Factor: Phishing and credential theft

Effect: massive network compromise, service outage and reputed damage

2. CYBERATTACKS ON INDIAN EDUCATIONAL INSTITUTIONS (2025)

The Indian educational institutions recorded average cyberattacks each week of 8,400, nearly double the average on a worldwide basis in 2025. Many of these attacks were due to user vulnerabilities: phishing emails, bad passwords, and no training of staff and students on cyber security.

Key Factor: User mistakes and poor security awareness

Impact: Massive data leakage, learning disruptions, and unintended expenses from increased operations.

3.LONG ISLAND SCHOOL DISTRICT DATA COMPROMISE (2025)

Long Island, USA, there was reporting by several school districts that they had experienced a compromise in 2025. Investigation findings suggested that almost half of these attacks had come from phishing emails or other online ads that were either malicious or deceptive to human behavior, aka, curiosity, trust, etc.

Key Factor: Social Engineering and user manipulation

Impact: Exposed student- or user-data, downtime, and other costs associated with recovery from the breach.

CONSEQUENCES OF HUMAN ERROR IN CYBER INCIDENTS

Human mistakes in cybersecurity can have serious and wide-ranging effects on organizations. These impacts go beyond just technical damage—they affect finances, operations, reputation, and future risk.

IMPACT AREA	DETAILS & EXPLANATION
Financial Loss	Data breaches costs vary by industry but average between $4.2 and $4.9 million dollars. Insider threat breaches (from employees or contractors) are even higher at an average of $13.9 million.
Time to Detect/Contain	Typically, it takes about 204 days to detect a breach and between 73 and 280 days to contain. This delay allows attackers more time to steal data or cause further damage, increasing overall risk.

Operational Disruption	Human error-related breaches can **shut down services**—from **schools and hospitals to grocery stores**—causing serious **downtime**, delays, and financial setbacks.
Reputational Damage	After a breach, about **33% to 60% of customers lose trust** and may stop doing business with the affected organization. This leads to long-term **brand damage** and **loss of customer loyalty**.
Insider Risk	Around 66% of cybersecurity professionals expect an increase in insider-related breaches in the coming years. These are often the hardest to detect because they involve trusted users misusing their access.

Human-Driven Attack Vectors in Cybersecurity

A lot of cyberattacks do not start with advanced hacking, but instead with people making mistakes or taking risky actions. These human-driven attack vectors are tied into communication tools, human error, and human habits to bypass technical security measures.

- Phishing (e-mail, SMS, Voice)

Phishing is the most popular and dangerous form of attack vectors. Phishing encompasses deceptive messages sent through e-mail, text (SMS), and voice (vishing) were designed to trick users into clicking malicious links, providing login credentials, or downloading malware. **Statistic:** Up to 26% of employees click on phishing links regularly and put their organization at serious risk with everything from ransomware, credential theft, or network compromise.

- Misconfiguration

This is when systems, state-of-the-art cloud services, or firewalls are improperly configured usually due to human error. Examples of misconfiguration include not restricting users, leaving databases open to the public.

Statistic: The improper configuration is responsible for nearly 50% of all cloud-related security breaches, one of leading human-related vulnerabilities.

- **Data Misdelivery:**

Employees sometimes mistakenly send emails to the wrong recipient, or upload sensitive files to unsecured platforms. This is quite common, particularly when performing under pressure, or working with large amounts of data.

Statistic: MisaddressedEmails represent 17% to 49% of all incidences of data breaches reported, depending on the industry.

- **Collaboration Tools (ex. Slack, Microsoft Teams)**

Organized with collaboration tool customizations, attackers are increasing targeting business communications channels. Collaboration Tools can share phishing messages, push malware, and harvest info from nudging users.

Statistic: 44% to 79%, of organizations reported an increase in cyber-attack using collaboration tools like Slack and Teams.

PSYCHOLOGICAL & OPERATIONAL DRIVERS OF HUMAN ERROR IN CYBERSECURITY

Cybersecurity incidents are driven not only by technical failures, but also by psychological stressors, behavioral tendencies, and organizational circumstances. Ultimately, these human and organizational factors can compromise even the most secure systems.

- **Security Fatigue & Security Overconfidence**

People may stop following security measures when they are inundated with security alerts or simply believe they can identify threats. This is called security fatigue, and it may result in people failing to heed warnings, or reusing passwords, or ignoring processes.

Impact: Users that become overconfident in their own knowledge may turn off security tools, or say they will not fall for phishing tactics, increasing chances of becoming exploited.

- **Insufficient Security Training**

Users without education to identify advanced cyber threats simply cannot recognize sophisticated attacks. While some employees get training for cybersecurity, most receive minimal or outdated education—if they receive any education at all.

Statistic: Approximately 70% of employees cannot recognize sophisticated phishing attacks, and therefore fall for basic social engineering attacks.

- **Policy Friction**

Unreasonable security policy, such as complex password requirements or more than one-step login processes, irritates users, reduces productivity, and compromises labor. Users are more prone to taking shortcuts with complex security policies that detract from work productivity.

Statistic: As reported by Gartner there are 69% of employees that will knowingly bypass a security measure, when they believe their company's security policy slows down their job.

MITIGATION STRATEGIES FOR REDUCING HUMAN ERROR IN CYBERSECURITY

Strategy	Effectiveness
Security Awareness Training	Regular training and quarterly phishing simulations help users learn how to identify suspicious emails. Using gamification—like quizzes or points—makes learning more engaging and improves long-term knowledge retention.
Human Risk Scoring	On average, it takes about 204 days to detect a breach and 73 to 280 days to fully contain it. This delay allows attackers more time to steal data or cause further damage, increasing overall risk. This approach uses data to identify employees who are most likely to make **security mistakes**. It allows security teams to focus training and monitoring on the **highest-risk users**, since research shows **8% of users cause 80% of incidents**.
Zero Trust & Least Privilege	No one is trusted automatically in a Zero Trust model, not even if that individual is an insider of an organization. This is also a function of the principle of Least Privilege Access, which allowed limited access to users limited to what they needed, which also reduces the damage if the user's credentials have been exposed.

Multi-Factor Authentication (MFA)	MFA is a second step in logging in (a text message with a code or approval in an app), and would block many phishing and credential-based attacks, yet many organizations do not use this approach widely.
AI & LLM Collaboration	Artificial Intelligence (AI) and **Large Language Models (LLMs)** help detect suspicious behavior faster and reduce **false positives** in alerts, allowing security teams to focus on real threats.
Cultural & Policy Alignment	Creating policies **with employee input** increases **buy-in** and **compliance**. When users feel involved in shaping rules, they're more likely to follow them and support the organization's **security goals**.

SECURITY AWARENESS TRAINING IS ESSENTIAL

It is no longer possible to remain indifferent towards Security Awareness Training (SAT) in today's unpredictable threat landscape; SAT is not an option but a necessity in a strategy. The reality of the current cyber threat landscape is complex because technology has challenged our beliefs about security safeguards. There are technical safeguards (firewalls, endpoint protection software, and encryption) we could implement, but unfortunately, they rarely handle the weakest link in any security system, which is always the human component. Many industry reports suggest over 90% of successful cyberattacks come from some action taken by a user (clicking on a phishing link or being coerced by social engineering tactics) as opposed to a system error. This truth emphasizes the importance of ongoing user training as a baseline strategy for any comprehensive cybersecurity program.

WHY IS SECURITY AWARENESS TRAINING ESSENTIAL?

Reduces User Error

Along with giving employees an opportunity to understand their role in the organization's cybersecurity strategy, Security Awareness Training (SAT) helps employees understand the difference between a good and bad practice or making a cybersecurity mistake such as clicking on a suspicious link, using a weak password, or inappropriately breaking confidentiality of a secure file. SAT can also incorporate real-life situations (i.e. data breach) and cyberattack simulations to build the user's ability to think critically, make decisions, and respond to the everyday threats the user faces in the workplace.

Supports Compliance and Regulatory Mandates

Compliance regulations such as GDPR, HIPAA, PCI DSS, and ISO/IEC 27001 require ongoing employee security training. SAT assists organizations to meet these regulations, avoid costly penalties, and demonstrate a proactive approach to data security

Enhances Threat Detection and Incident Reporting

Trained personnel are more likely to notice unusual activity and report it promptly. Early detection leads to faster response to incidents, limiting potential damage and developing organizational resilience to cyber-attacks.

Delivers Cost-Effective Risk Mitigation

SAT is a financially sound investment compared to the reputational and financial cost of a data breach. Studies have shown that for every dollar spent on security awareness, a large amount of money can be saved, especially if layered defenses are utilized

BEHAVIORAL CHANGE REQUIRES SIMULATION

The creation of significant and lasting behavioral changes in cyber security goes beyond static politics or traditional lectures. In order to effectively reduce the risk associated with humans, organizations must use simulation -based learning. This approach provides practical experience, real world context and active commitment, and helps users understand and respond to threats more effectively. Educational and psychological research shows that people maintain information longer and are more likely to change their behavior when they actively practice realistic scenarios.

1. **Phishing simulations build the readiness of the real world**

Phishing is one of the most common and dangerous attack methods, usually using urgency, authority or emotional triggers to deceive users. Simulated phishing exercises expose employees to realistic threats in a controlled environment, helping them develop instinctive answers to suspicious emails. These simulations allow security teams: -

- Identify users or departments at higher risk,
- Monitor behavioral improvement over time,
- Adapted training to address the user's actual responses.

2. **Gamified learning increases engagement and retention**

Gamification adds digits, challenges, progress tracking and award for safety training. This approach makes learning more interactive and enjoyable; user enhances inspiration and participation. As a result, the organizations see: -

- The rate of completion of high training,
- Improvement in long -term knowledge retention,
- A strong sense of responsibility for safety.

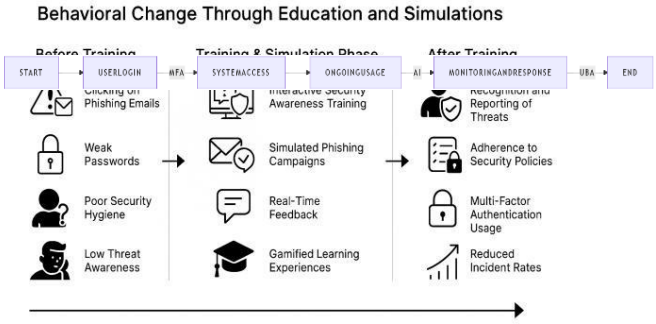
The study of Knowbe4 and Cyvent shows that gamified training leads to less mistakes than traditional slide-based learning.

3. **Interactive landscape strengthens decision making skills**

Practical cybersecurity exercises-like hands-on labs, roll-playing, and accidental reaction drill-help users create confidence in making quick, informed decision making during real threats. This simulation cover:

- Social engineering attacks,
- System misconfiguration,
- Insider the danger detection,
- Safe data handling and reaction phase.

This type of experienced learning improves user confidence and reaction speed, both are important to reduce the effects of safety phenomena.



TECHNOLOGY SHOULD AID, NOT HINDER

Technology plays an important role in defense against cyber threats, but it should be designed to not obstruct users. When the safety tool is difficult to use or control is very strict, the users may be disappointed, ignoring policies, or finding work - round. This can increase mistakes and weaken the overall security currency of the organization. Effective safety solutions should be balanced with protection with purposeful to encourage compliance and reduce risk.

1. Proponible vs. security: striking on the right balance. When safety devices are very complex or obstruct the daily work, they can have the opposite effect. Strict materials such as filters, long login phase, or vague alert can cause disappointment. As a result, users can avoid safe tools or find unsafe work -round - a behavior known as "safety friction". A report by 2025 Gartner found that 69% of the employees would deliberately bypass security control if those measures slow down their productivity. This highlights the need for user -friendly safety solutions that support both safety and efficiency.

2. Human-focused design in cyber security

Modern cyber security focuses on human-focused design manufacturing equipment that people think and work align with it. It also includes:

Simple, easily used interfaces,

- Smart safety signs that only appear when needed,
- Minimum impact on daily workflows,
- Role-based access and automation to reduce unnecessary decisions.

When safety solutions are designed keeping in mind the user, they increase compliance, reduce errors, and strengthen overall security.

3.**Intelligent technologies must support, not overload**

Advanced tools, such as detection of threats to AI, behavioral Analytical and automated answers work better when helping users, do not replace them or overloaded. These technologies can:

- Cut into fake alarms,
- Provide clear and useful information without technical language,
- Adjust based on user behavior and specific work risk.

By facilitating the understanding of complex data allows for smart tools to make better safety decisions, improve efficiency and protection without requiring deep technical skills.

4. **Aligning safety with workflow and culture**

Security tools should fit naturally into the way people work and match the organization of the organization. The integration of safety features with platforms such as Slack, Microsoft Teams and CRM Systems helps ensure that protection is part of daily tasks, not an interruption. When safety seems perfect and favorable, users are more likely to follow best practices and remain involved with cyber security protocols.

LEADERSHIP SHAPES SECURITY CULTURE

Strong leadership is important for building a successful cybersecurity culture. While tools and training are important, it is the actions and attitudes of leaders, leaders and team leaders who shape how serious security are taken over the organization. When leaders are actively involved and lead an example, security becomes a shared mindset - not just a list of rules to follow.

1. Leadership and shared accountability

A strong cyber security culture begins with leadership. When leaders and managers demonstrate safe behavior, actively support security efforts and take responsibility for their actions, employees are more likely to follow. This visible obligation builds trust and shows that cyber security is a shared responsibility, not just an IT problem. According to a Gartner study in 2025, organizations with engaged management saw 42% higher compliance with security policy and 60% fewer insider-related incidents compared to those without strong performing involvement.

2. Inclusive policy development and open communication

Effective managers involve employees in creating security policy, and ensuring that the rules are practical, relevant and easier to follow. When staff feel heard and included, they are more likely to understand the guidelines and follow them. Modern leadership also promotes open, fearless communication around cyber security. Instead of using scare tactics, strong leaders create a culture of psychological Security-that restores employees to report errors, suspicious behavior or almost missed without fear of guilt. This approach builds trust, improves early threat detection and strengthens the organization's ability to respond quickly to events.

3. Embedding Security into Business Strategy

Security administrators consider cybersecurity as a essential part of normal business goals, not just technical concerns. By coordinating cybersecurity with strategic planning, risk management and operation measurements, they ensure that they receive proper credit, employees and support. This approach helps all sections to understand that safety is important for success in business, not a barrier or late reflection. It also promotes improvement and constant investment in people who focus on people, such as awareness training, behavioral surveillance and flexible security policy.

4. Leadership in Cyber Crisis and Recovery

During a cyber event, strong leadership is important. Leaders who remain calm, act quickly and communicate help reduce injuries, maintain self -confidence and guide the organization through improvement. Its role is crucial to coordinating response efforts, s and lessons are learned to avoid future events.

IBM Cyber Resilience Report 2024 found that organizations with executive active involvement in incident response recycled 42% faster and reduced costs by almost 30% compared to those without engaged management.

As cyber threats become more advanced, organizations need more than just technical defenses- they need a human focused approach. This means projecting security systems, policies and processes that are not only safe by design, but also easy to use, practical and aligned with real -world workflows. When tools are excessively complex or disturbing, users can avoid them or find alternative solutions, which can lead to new safety risks. By making safety effective and for the user, organizations can reduce errors and strengthen overall protection.

1). Security Should Fit How People Work

Many traditional security controls do not consider how people behave under real-world-like conditions, tight deadlines or fatigue. When security tools are very strict or difficult to use, such as complex password rules or confused logins, users usually ignore them only to stay productive. This not only weakens the defenses of the organization, but also reduces confidence in security policies. According to a 2025 Gartner study, 69% of employees admitted that he would intentionally ignore security measures if these measures diminished them.

2**). Designing Security That's Easy to use**

The man -centered security design focuses on protecting Easy and practical for users without reducing safety standards. The main features include:

- Simple login options such as biometrics or password access,
- Intelligent access controls that fit the user -based function or level of risk,
- Useful and non -discriminated security promotes,
- Standard settings that protect users without an extra effort.

These friendly designs reduce frustration, improve compliance, and make behavior safe natural choice, helping users to remain safe without diminishing work.

1. **Reducing Risk Through User Collaboration**

involving employees in the project and security resources testing leads to stronger adoption and more practical policies. When users understand the reason behind security controls - and know that their comments have been considered - they are more likely to follow the procedures and report problems in advance.

This approach is part of cyber security informed by behavior, which combines psychology, usability testing, and risk analysis to create safety solutions that support people rather than working against them.

2. **Empower Users with Supportive Technology, Not Surveillance**

Man -centered security avoids heavy monitoring or surveillance, which can create fear and resistance. Instead, modern organizations use real-time safety support technologies, functions-based panels and tools driven AI-What guide users without adding pressure.

1. **AI-Driven Deepfake Attacks**

This technology uses AI to mimic sounds, images or moving pictures therefore people use deepfake by AI software And it can produce ultra-realistic false audio and video in addition to phoney photographs Cyber criminals are using this new twist to impersonate the CEO (or anyone else in a position of authority) during online voice- or video calls.

Real-World impact:

- In one major incident, attackers employed a deepfake of a company's CFO to authorise a $25 million transfer.
- **Scalable threat**: These attacks are also automated so that they can send out thousands of individual scam calls and messages. This makes detection difficult.
- **Economic risk:** By 2027, the US could face losses of up to $40 billion from deepfake-related fraud, according to experts.

Deepfakes have become a serious cyber threat, particularly in social engineering., fraud and executive impersonation scenarios

2. **AI-Driven Phishing and Automated Cyber Attacks**

Cyber criminals now use generative AI to craft highly self-wicked phishing emails, fake chat bots that answer queries with broken English; smart software plus adaptable malware that changes the way in which it conducts operation depending on what is happening before its eyes.

- **Targeted Phishing:** Attackers use personal information obtained from social media networks to craft messages that appear genuine but lead to malicious links
- **Adaptive Malware is a Sea of Change:** - Today's malware changes in response to what has gone before; it learns, evolves and mutates, and is no longer limited to just trying different signatures (as its ancestors were).
- **Easy to Use Tools: -** AI-based hacking tools like FraudGPT are now available in the daily online shopping cart, making sophisticated attacks easier than ever—even for less talented attackers.

This new breed of AI-based threats is strengthening cyberdefenses for all industries and businesses.

3. **AI-Enhanced Crime and Nation-State Cyber Operations**

AI is increasingly used to increase organized cyber crime and state -sponsored attacks, as highlighted by Europol. Criminal groups and hostile nations are leveraging AI to:

- Launch more accurate and automated cyber operations, including fraud, misinformation and cyber-espionage.
- Perform hybrid attacks that combine traditional hackers with influence campaigns to destabilize targets.

This triggered a digital arms race, where defenders should constantly adapt to the faster, smarter, and more difficult to detect threats.

4. Synthetic Identity Fraud ("Repeaters")

The invaders are now using AI -generated false identities, called "repeaters" to ignore identity verification systems such as KYC (meet your client) and biometric checks.

- These false profiles are changed only a little at a time, allowing them to undergo unique traditional safety checks.
- They are used to test and investigate various platforms, looking for weaknesses before launching real attacks.
- Detects them requires collaborative identity validation, where organizations share signals to identify patterns between systems.

5. Attacks Targeting AI Systems Themselves

Now, cyber criminals are targeting the A.I. systems that companies use to block spam, render images and detect malware.

- **Adversarial manipulation:** This includes planting hidden backdoors in A.I. models or in the training data used to teach them, that enable attackers to sneak past systems such as deepfake detectors.
- **Biometric deepfakes** may deceive facial recognition or voice authentication systems by imitating legitimate users.
- AI supply chains pour malware on fraudulent (or fraudulent-looking) training data, skewing the logic or goals of AI models from within.

These threats serve to demonstrate that AI itself is gradually becoming a target, and a real one at that (not just a weapon), which in turn suggests an emerging need for more extensive and esoteric modes of validation, transparency and security with how models are constructed and trained.

IMPLICATIONS & DEFENSIVE IMPERATIVES

Only by evolving to new and shared solutions will organizations be able to respond to AI-enabled threats such as deepfakes and synthetic fraud:

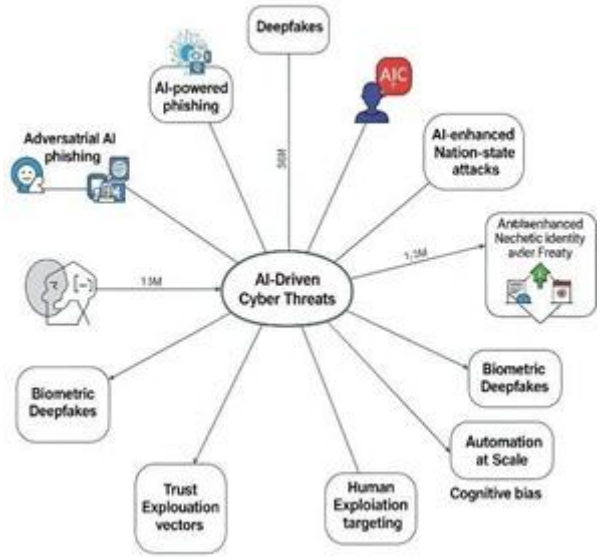
Multi-Modal Detection: Use audio, visual, and metadata to better detect deepfakes and manipulated media.

AI + Human Collaboration: Let AI tools flag suspicious activity, while giving cybersecurity teams the power to check and confirm threats. This strikes a balance between automation and expert insight.

Federated Identity Sharing: - Pass KYC (Know Your Customer) data between trusted groups to spot fake identities used over and over in fraud.

Secure AI Governance: - Guard AI systems by locking down training data, adding digital watermarks, and running tests to find weak spots in the models.

Policy and Regulation: Make use of new laws such as the U.S. "TAKE IT DOWN Act" and the EU AI Act to steer the ethical and secure use of AI. However, keep in mind that worldwide teamwork is crucial to fill in the gaps in rules and regulations



REFERENCES

1) https://navvia.com/blog/exploring-the-human-factors-in-cyber- security
2) https://securityscorecard.com/blog/the-human-factor-in- cybersecurity/
3) https://www.mdpi.com/2624-800X/2/3/29
4) https://easychair.org/publications/preprint/kPcK/open
5) https://medium.com/%40binijoann/strengthening-cybersecurity- why-people-are-the-key-factor-bc0d34962d7a?utm_source=chatgpt.com
6) http://paper.ijcsns.org/07_book/202210/20221036.pdf
7) https://www.upguard.com/blog/human-factors-in-cybersecurity
8) https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1019645

4

9) https://medium.com/%40binijoann/strengthening-cybersecurity- why-people-are-the-key-factor-bc0d34962d7a
10) https://deepstrike.io/blog/cyber-crime-statistics-2025
11) https://www.infosecurity-magazine.com/news/data-breaches- human-error/
12) https://www.wsj.com/business/c-suite/crowdstrike-ceo-doj- official-and-executives-take-the-stage-at-wsj-tech-live-cybersecurity-e6e6e0a6
13) https://timesofindia.indiatimes.com/technology/tech- news/indian-schools-hit-by-8000-plus-cyberattacks-per-week-report/articleshow/121912099.cms
14) https://www.scworld.com/news/95-of-data-breaches-involve- human-error-report-reveals
15) https://en.wikipedia.org/wiki/Security_awareness
16) https://gitnux.org/security-awareness-training-statistics/
17) https://www.cyvent.com/post/cybersecurity-statistics-2025
18) https://www.businessinsider.com/bank-account-scam- deepfakes-ai-voice-generator-crime-fraud-2025-5
19) https://apnews.com/article/846847536f6feb2bbb423943fd96e1f

1

20) https://www.techradar.com/pro/security/cybercriminals-are- deploying-deepfake-sentinels-to-test-detection-systems-of- businesses-heres-what-you-need-to-know
21) https://www.thehackacademy.com/feature/emerging-ai-driven- threat-trends-what-to-watch-in-cybersecurity-for-2025/
22) https://smartaidaily.com/deepfake/deepfake-evolution-2025- from-historical-origins-to-future-threats-countermeasures/
23) https://itbrief.com.au/story/from-deepfakes-to-ransomware-the- key-trends-which-will-shape-it-security-in-2025
24) https://arxiv.org/abs/2002.12749
25) https://www.reddit.com/r/AIFUstock/comments/1ja5hpt
26) https://en.wikipedia.org/wiki/TAKE_IT_DOWN_Act
27) https://www.researchgate.net/publication/385685188_Human-Centric_Cybersecurity_Understanding_and_Mitigating_the_Role_of_Human_Error_in_Cyber_Incidents
28) https://www.researchgate.net/publication/377473406_Human_factors_in_cybersecurity_an_in_depth_analysis_of_user_centric_studies
29) https://www.researchgate.net/publication/386747842_Human_Factor_in_Cybersecurity_Behavioral_Insights_into_Phishing_and_Social_Engineering_Attacks
30) https://link.springer.com/article/10.1007/s10207-025-01032-0?
31) https://zagrebsecurityforum.com/Portals/0/SecurityScienceJournal/SSJ%202_2_4%20HUMAN%20FACTORS%20IN%20CYBERSECURITY%20RISKS%20AND%20IMPACTS.PDF?
32) https://pmc.ncbi.nlm.nih.gov/articles/PMC8195225/
33) https://arxiv.org/abs/1506.07167
34) https://posthumanism.co.uk/jp/article/view/1242
35) https://www.proofpoint.com/us/resources/threat-reports/human- factor-social-engineering