H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-07

Human Factor in Cybersecurity: Strengthening the Weakest Link

Overview

Humans: The Weakest Link

The recent cyberattack on Qantas Airlines, allegedly by the Scattered Spider group, exposed the personal data of nearly 6 million customers. This incident echoes a growing trend: cybercriminals now prefer exploiting humans over breaking firewalls. Why? Because people are easier to manipulate than machines. The Scattered Spider group is known for impersonating IT personnel, tricking help desks and bypassing multi-factor authentication (MFA) through social engineering. Major companies like Marks & Spencer, Co-op, and Harrods have all fallen victim costing them months of business disruption and severe reputational damage.

Based on cybersecurity expert's analysis, the biggest vulnerability in any digital infrastructure isn't software or hardware but human behavior. Just like the fall of Troy due to the Trojan Horse, a symbol of trust and deception, modern organizations often fall not from brute force but from emotional manipulation and human error.

The top human-related cyber risks are:

1. Phishing & Social Engineering - emotion-driven emails trick users into opening malicious links or attachments.

2. Credential Theft & Misuse - weak or reused passwords are easy targets for hackers.

3. Human Error - Sending the wrong file, misconfiguring systems, or clicking unsafe links.

4. Malicious Insiders - disgruntled employees or coerced staff intentionally violating policies.

Recommendations

How to fortify the human firewall:

For Organizations:

1. Conduct phishing simulations & awareness training.
2. Enforce Multi-Factor Authentication (MFA) across all systems.
3. Establish a strong internal security culture.
4. Monitor for unusual behavior & maintain reporting mechanisms.

For Individuals:

1. Think before you click, be skeptical of unsolicited emails.
2. Use strong, unique passwords and password managers.
3. Always double-check recipient addresses before sending emails.
4. Report suspicious behavior, security is everyone's responsibility.

Conclusion

The battleground of cybersecurity requires vigilance and consciousness. Our strongest defenses can fail if trust is misused. As tech advances, so must our skills and awareness. Remember: "The gate of Troy didn't fall from force, but from trust. Cyber attackers today exploit the same flaw."

Stay alert. Stay updated. Stay secure. Cyber resilience starts with you.

References:

a. https://www.weforum.org/stories/2025/07/hackers-employees-cybersupport-and-other-cybersecurity-news/
b. *https://thebftonline.com/2025/02/05/humans-often-considered-the-weakest-link-in-cybersecurity/*
c. *https://www.renewableuk.com/news-and-resources/blog/cyber-security-and-human-risk-are-humans-the-weakest-link/*