

4 Minute Read | Cybersecurity & Society



You Are Easier to Hack Than Everything

By: R A M Milanes

Cybersecurity threats are no longer confined to firewalls, encryption, or sophisticated malware. The weakest link, time and again, is human. As the now-famous cybersecurity maxim goes: *“You are easier to hack than your computer.”* Social engineering which is the art of human hacking has long been here to exploits trust, curiosity, and authority to gain access where technical attacks fail. This feature takes a closer look at how criminals manipulate people, why it works so well, and what organizations can do to defend themselves.

“A hacker doesn’t need to break your firewall—just your trust.”

The Human Vulnerability: What Is Social Engineering?

Unlike technical exploits that target code, social engineering targets cognition. Attackers manipulate people into revealing passwords, granting access, or clicking malicious links.

Psychology rather than technology becomes the battleground. And because humans are naturally trusting, cooperative, and prone to error, they remain the most lucrative entry point for attackers.

Psychological Levers: How Hackers Manipulate Us

First is **authority**, people comply with perceived senior figures. An email “from the CEO” often prompts quick, unquestioned action. Capitalizing on **urgency & fear**, deadlines and threats rush people into compliance without verifying requests. We will not forget the most common **curiosity & greed**, a “Salary Update” or “Bonus Announcement” or a “Winning Raffle Entry” subject lines exploit natural impulses. Finally, for a country that is known to be so hospitable, **politeness & trust** no explanation needed.

Did You Know?

- Over **90% of data breaches** world-wide involve human error.
 - The National average of **reported** Personal Data Breaches in the Philippines is **over 70%**
- Hackers can now clone a voice with as little as **3 seconds of audio**.
- The average cost of a phishing attack on a mid-size company: **\$1.6 million**.

Real-World Cases of Human Hacking

Qantas Data Breach – One Phone Call Too Many (2025)

Hackers posed as contractors and tricked a call center into handing over access credentials, bypassing multi-factor authentication. The attack exposed the data of up to six million passengers. It was not a flaw in the system, but in human trust.

The Twitter Hack (2020)

Attackers spear-phished Twitter employees by phone, compromising internal tools. High-profile accounts—including Elon Musk and Barack Obama were hijacked to post cryptocurrency scams. Technology was intact; human defenses failed.

Google and Facebook Phishing Scam (2017)

A fraudster impersonated a hardware supplier and sent fake invoices. Both tech giants paid them, losing over \$100 million. The criminals didn’t need to code just to convince.

Sony Pictures Hack (2014)

What began with phishing emails to assistants and contractors spiraled into a devastating breach, leaking unreleased films and private communications. The breach proved that one compromised individual can topple an empire.

Everyday Examples

Baiting is where USB drives labeled “Executive Payroll” left in offices. Employees plug them in, unleashing malware while **Tailgating** is executed by an intruder in a courier uniform slips behind employees into secure zones without a badge scan.

“One careless click can undo millions of dollars in cybersecurity investment.”

Cybercriminals exploit emotions that override logic. Fear trumps policy. Trust overrides caution. Curiosity beats training. In every case, social engineering bypasses technology by exploiting humanity.

Building Human-Centered Defenses

- **Security Awareness Training**, we must teach staff to recognize phishing, vishing, and pretexting.
- **Simulated Attacks**, mock exercises keep employees alert.
- **Policies & Verification Protocols** require callbacks or secondary confirmation for sensitive requests.
- **Multi-Factor Authentication & Zero-Trust** reduce damage even if credentials are exposed.
- **AI Detection Tools** we can counter AI-powered scams with AI-driven defenses.
- **Leadership Involvement** where boards and executives own cybersecurity and not just IT.

4 Tips to Outsmart Social Engineers

1. **Pause before clicking:** Verify links and email senders.
2. **Question authority:** Always confirm high-pressure requests—even from “executives.”
3. **Protect personal data:** Don’t overshare on social media.
4. **Report suspicious behavior:** Early alerts can save entire organizations.

Cybersecurity is no longer only about securing machines it includes safeguarding minds. The greatest firewall is awareness, **“In cybersecurity, the brain is both the biggest weakness and the best defense.”**