

Topics

1. What is social engineering?

How does it impact your business?

2. Types of Social Engineering Attacks

3. Impact of Social Engineering: Key Statistics on Businesses

The mind is the weakest link

The numbers don't lie—and they're ugly

Social engineering bleeds businesses dry

They're coming for the unsuspecting

Why social engineering works (and works well)

Training is your best defense

Tech alone won't save you

A full-court defense is the only play

The bottom line: If you're not ready, you're next

4. How to prevent social engineering attacks

Share



Impact of Social Engineering: Key Statistics on Businesses

Published: **May 23, 2025**

By:  **Lizzie Danielson**

Key Takeaways:

- Humans are the weakest link. Social engineering preys on psychology, not technology.
- Businesses suffer huge losses. In 2024, the average data breach cost hit \$4.88 million, and 60% of small businesses shut down within six months of a major breach.
- Non-technical staff are prime targets. CEOs face 57 phishing attacks per year, compared to 40 for IT staff.
- Tech alone can't stop attacks. 68% of cyberattacks exploit human error. Firewalls and antivirus aren't enough.

Forget the Hollywood movies that portray hackers as geniuses in dark basements pounding away at keyboards. The biggest threat to your business isn't a brilliant coder who can hack their way out of the Matrix—it's good old-fashioned manipulation. [Social engineering](#) is the digital-age version of a con artist swindling their mark. Instead of convincing you to invest in a Ponzi scheme or marry them without a prenup, they're tricking employees into handing over passwords, sensitive data, and access to critical systems. And it works—big time.

Read on for some social engineering statistics that prove just how effective these attacks are, why they're on the rise, and what your business can do to stop taking the bait.

[Try Huntress for Free](#)
[Get a Free Demo](#)

The mind is the weakest link

Cyber defenses? Firewalls? AI-powered security? None of that matters if an attacker can convince an employee to hand them the keys to the kingdom.

[Social engineering](#) preys on human psychology—trust, fear, urgency—to bypass all that expensive security tech. The harsh truth? The biggest vulnerability in any company isn't a software bug—it's the people behind the screens. [74% of data breaches are tied to human error or manipulation.](#) [Huntress Managed Security Awareness Training](#) gives your team the skills to spot and fight back against these threats.

The numbers don't lie—and they're ugly

Social engineering statistics paint a grim picture:

- ✓ [98% of cyberattacks rely on social engineering](#)
- ✓ [Ransomware hits businesses every 11 seconds](#)
- ✓ In 2024 alone, [59% of organizations world](#)wide became victims.

The good news? [97% of companies manage to recover their data after an attack](#) thanks to solid backup strategies. If your company hasn't been hit yet, it's not because you're doing something right—it's a matter of time.

Social engineering bleeds businesses dry

A social engineering attack doesn't just hit your reputation—it ransacks your bank account. The average cost of a data breach in 2024? A staggering [\\$4.88 million](#). And if you're a small business, brace yourself: [60% of small businesses shut down within six months](#) of a major breach.

A single email scam can turn an entrepreneur's dream into a nightmare overnight. The clock's ticking—it takes just [21 seconds to click on a malicious link after opening an email, and only another 28 seconds to hand over your data](#). Phishing is the king of the attack methods.

They're coming for the unsuspecting

You'd think IT teams and security pros would be the main targets. Wrong.

Recent social engineering data shows that cybercriminals are refining their tactics, targeting non-technical employees like administrative assistants, HR reps, and finance teams—anyone with access to sensitive data is a target.

A Barracuda report states that [an average CEO receives 57 targeted phishing attacks in a year](#) due to the sensitive nature of their correspondence. In comparison, IT staff account for only 5% of total phishing attacks, with each employee [targeted by an average of 40 phishing emails per year](#). Executive accounts are attractive due to their sensitive data, while IT accounts are targeted due to access to critical systems. Regardless of the reason behind the target, attackers are relentless in their attempts to breach.

Why social engineering works (and works well)

Threat actors aren't breaking in—they're being let in, using psychological tricks that have worked for centuries. One of the most alarming social engineering facts is authority-based scams, where the attacker pretends to be a well-known brand or service to trick victims into clicking on a phishing link. These make up [49% of all socially engineered threats](#). It's no surprise that [43% of phishing attacks impersonate Microsoft brands](#).

Want to see how attackers refine their tactics? Check out our video [Hacker Trends in Social Engineering](#).

Training is your best defense

Most employees take [less than a minute](#) to fall for a phishing email. The best way to fight social engineering is to teach employees to spot the hustle. Run simulated phishing tests and invest in regular [security awareness training](#). It's like self-defense for the digital world—when people know the tricks, they're way harder to fool.

Tech alone won't save you

Think antivirus software and firewalls have you covered? Think again. [68% of cyberattacks involve a human element](#). That means if you're relying solely on technical defenses, you're exposed. The only real security comes from a combo of tech, training, and vigilance.

A full-court defense is the only play

If you're serious about stopping social engineering, you need a full strategy—because one weak link is all it takes. That means:

- ✓ [Security awareness training](#) so employees recognize scams before they fall for them.
- ✓ Clear reporting procedures so staff know exactly what to do if they suspect an attack.
- ✓ A security-first culture where employees feel empowered (not scared) to question suspicious emails or requests.

Regular testing with [simulated attacks](#) keeps everyone on their toes.

The bottom line: If you're not ready, you're next

Social engineering isn't some niche threat—it's the main event. And it's not just targeting the big corporations. It's coming for every business, big or small. The best defense? Stay skeptical, stay educated, and never hand over the keys to your digital kingdom just because someone asks nicely. Threat actors don't break in anymore. They walk right through the front door.

Check out [Huntress Security Awareness Training](#) to protect your business from the con artists of the digital world.



Lizzie Danielson

[Read More >](#)

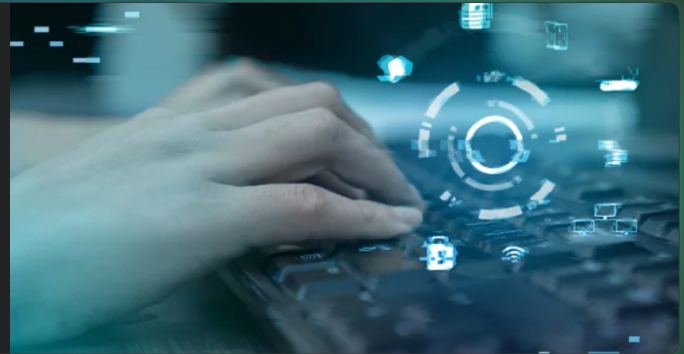
[Continue Reading](#)

[How to prevent social engineering attacks >](#)

Protect What Matters

Secure endpoints, email, and employees with the power of our 24/7 SOC. Try Huntress for free and deploy in minutes to start fighting threats.

[Try Huntress for Free](#)



Platform

Huntress Managed Security Platform
Managed EDR
Managed EDR for macOS
Managed ITDR
Managed SIEM
Managed Security Awareness Training
Book A Demo

Solutions

Phishing
Compliance
Business Email Compromise
Education
Finance
Healthcare
Manufacturing
State & Local Government

Why Huntress?

Managed Service Providers
Value Added Resellers
Business & IT Teams
24/7 SOC
Case Studies

Resources

Resource Center
Blog
Upcoming Events
Support Documentation

About

Our Company
Leadership
News & Press
Careers
Contact Us



© 2025 Huntress All Rights Reserved.
[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)

[Free Trial](#)