

Topics

1. What is social engineering? How does it impact your business?

The confidence game: what is social engineering?

The four types of social engineering scams

Why do these scams work? The psychology behind social engineering

The true cost of getting played

How to beat the hustlers: social engineering prevention

Want to see social engineering in action?

Stay smart, stay secure

2. Types of Social Engineering Attacks

3. Impact of Social Engineering: Key Statistics on Businesses

4. How to prevent social engineering attacks

Share    

What is social engineering? How does it impact your business?

Published: **May 23, 2025**

By:  **Lizzie Danielson**

Key Takeaways:

- Social engineering is a psychological con, not a technical hack.
- Common scams exploit human nature. Phishing, tailgating, watering hole attacks, and baiting all rely on deception.
- The impact of social engineering attacks goes beyond financial loss to reputational damage, legal consequences, and loss of customer trust.
- Prevention starts with awareness. Try the [Huntress Managed Security Awareness Training](#).

In cybersecurity, threat actors aren't always hiding behind lines of code. Sometimes, they're sliding into your inbox, charming you over the phone, or walking straight into your office with a fake badge. This is social engineering: the art of manipulating people into giving up their secrets. Unlike brute force hacks, social engineering plays the long con, using psychology over technology to crack security wide open. Let's cover the basics of social engineering.

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

The confidence game: what is social engineering?

To understand how social engineering works, it's important to recognize that these attacks exploit human psychology rather than technical vulnerabilities.

[Social engineering](#) is the digital world's equivalent of a con artist working a crowded street. Instead of picking your pocket, these attackers trick you into handing over the goods willingly—passwords, financial info, and access credentials. It's less about breaking firewalls and more about breaking human instincts.

Ready to see our Managed EDR in action? [Start your free trial of Huntress Managed EDR](#) and experience firsthand how our expert-led platform turns the tables on cyberattackers.

The four types of social engineering scams

Social engineering scams come in many forms, but most social engineering examples follow a

similar playbook—manipulating human emotions like trust, fear, or curiosity to deceive victims into revealing sensitive information. Cybercriminals don't need fancy code to slip past security. They exploit trust, fear, curiosity, and urgency, turning everyday interactions into security nightmares. Here's how they pull it off:

1. Phishing: The digital bait-and-switch

Imagine getting an email from your bank claiming your account is locked. Panic sets in, and before you think twice, you've clicked the link, entered your login, and—boom—your credentials are in a scammer's hands.

Common phishing tactics:

- ✓ Urgent language ("Your account is in danger!")
- ✓ Spoofed sender addresses (it looks legit)
- ✓ Fake login pages (a pixel-perfect trap)

2. Tailgating: The door-to-door con

Sometimes, the easiest way into a system is literally through the physical front door. Tailgating happens when an attacker follows an employee into a restricted area by pretending to belong there.

How they pull it off:

- ✓ Pretending to be a delivery driver
- ✓ Carrying fake credentials
- ✓ Flashing a convincing smile

3. Business email compromise: The costly deception

Imagine your CEO sending you an urgent email asking for an updated vendor payment or a wire transfer. It appears legit—the right name, business logo, even the tone is recognizable. The catch is that it's a scam.

Business email compromise (BEC) is a highly targeted type of cyber fraud where threat actors pose as trusted people like partners, executives, or vendors. BEC scams are carefully crafted, often using stolen credentials to bypass traditional security measures, making them different from [phishing attacks](#), which cast a wider net.

How it works:

1. Find the target: Attackers research company executives, LinkedIn profiles, and press releases to identify who has access to sensitive data.
2. Set the trap: They either spoof an executive's email address or gain access to a real email account through phishing, credential misuse, or malware.
3. Begin the manipulation: Once inside, they craft convincing messages that exploit urgency or authority, like impersonating the CEO requesting a wire transfer.
4. Convince the employee: The employee believes the request is legit, and complies by sending the money. Once fraud is detected, it's too late, as funds have already been laundered through multiple accounts.

4. Baiting: The too-good-to-be-true-trick

Have you ever picked up a free USB drive from a trade show? How do you know it wasn't planted by an attacker? Baiting lures victims with promises of free gadgets and downloads, exclusive deals, or enticing software, all laced with malware.

Examples of baiting:

- ✓ Download this free e-book (ignore the malware hiding behind the curtain).
- ✓ Stream movies for free!
- ✓ Just install this software first...

Why do these scams work? The

psychology behind social engineering

Humans are wired to trust, help, and act quickly when faced with urgency. Threat actors take advantage of that using psychological tricks:

- ✓ Authority bias: If it sounds official, people listen.
- ✓ Scarcity principle: Limited-time offers make us act fast.
- ✓ Reciprocity: If someone does us a favor, we feel the need to reciprocate.

Social proof: If everyone else is doing it, we assume it's safe.

The true cost of getting played

If you think falling for a social engineering attack is just a small mistake, think again.

- ✓ Financial fallout: The average [social engineering breach cost businesses \\$4.88 million in 2024](#). [98% of cyberattacks rely on social engineering techniques](#).
- ✓ Reputation damage: Customers lose trust. Brands take years to rebuild credibility.
- ✓ Legal nightmares: Compliance violations lead to fines, lawsuits, and headaches.

Find more [statistics on social engineering scams here](#).

How to beat the hustlers: social engineering prevention

A strong defense isn't just about firewalls. It's about making sure your people don't get played. Here's how:

Security awareness training: Your best weapon

Your employees are your first line of defense. Regular training helps them recognize scams. Try these for starters:

- ✓ Simulated phishing attacks
- ✓ Real-world case studies
- ✓ Interactive learning (because boring training gets ignored)

Lock down the tech: No easy open doors

Even the best-trained team needs solid tech to back them up. Implement these:

- ✓ Advanced email filtering: Flags shady messages before they land in inboxes.
- ✓ Multi-factor authentication (MFA): Makes stolen credentials useless.

Make cybersecurity a culture, not a checkbox

Security isn't a one-time thing. It's a mindset. Build a workplace where employees:

- ✓ Question unusual requests
- ✓ Report suspicious emails and calls
- ✓ Know who to call when something feels off

Use threat detection driven by humans

Threat actors evolve, and so should your defenses. While AI-powered monitoring can help detect unusual patterns, the real advantage comes when it's combined with 24/7 human expertise. Your best line of defense against threats is a security team that understands context, looks into anomalies, and responds proactively.

Want to see social engineering in action?

Threat actors have stepped up their game, leaving behind the haphazard scams of the past in favor of slick, sophisticated phishing tactics designed to fool even the sharpest eyes. Today's attacks are crafted with precision, using better grammar, more believable lures, and tactics that adapt. [Watch this video](#) to see just how easy it is to get hooked.

Stay smart, stay secure

- ✓ Social engineering isn't about hacking tech. It's about hacking people.
- ✓ If it feels off, it probably is. Question everything.
- ✓ Education is your strongest defense. The more you know, the harder you are to fool.
- ✓ Cybersecurity isn't just IT's job—it's everyone's job.

The best way to avoid getting scammed? Think like a scammer and see for yourself how [Huntress identifies threats, exposes deception, and keeps you ahead of the game](#). Our [Managed Security Awareness Training](#) can help teams recognize and block attacks before they happen, and our [Endpoint Detection and Response \(EDR\) solution](#) catches malicious activity before it spreads, stopping attackers before they can do real damage.



Lizzie Danielson

[Read More >](#)

[Continue Reading](#)

[Types of 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](#)