OUCH! May 2025

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

How Cybercriminals Exploit Your Emotions

A Costly Text Message

Emma had just left the grocery store, arms full of bags, when her phone buzzed with a text message from her daughter.

"Mom, I lost my phone! I'm using a friend's. I need money for a new one. Please send $800 right away—I'll explain later!"

Her heart skipped a beat. Her daughter, Angie, was away at college, and she knew how important her phone was for school, work, and staying in touch. The thought of her stranded without a phone made her anxious. She quickly replied,

"Are you okay? What happened?"

A response came almost immediately.

"I'm fine, but I can't talk. Borrowing a friend's phone. Can you send the money now? I need to get a replacement ASAP. I'll call you tonight. Love you!"

Emma hesitated for a moment. Something felt off, but her worry overruled her doubts. She pulled up her banking app and transferred the $800 to the phone number provided in the text message. She didn't even question why it wasn't going directly to her daughter's account—maybe Angie couldn't access it without her phone.

Later that evening, she called Angie's real number, expecting to hear relief in her voice. Instead, she answered normally.

"Hey, Mom! What's up?"

Emma froze.

"Did you get the money?"

Angie sounded confused.

"What money?"

Emma's stomach dropped. She opened the text messages again, reading them with fresh eyes. The urgent tone, the lack of specifics, the insistence on immediate payment—it all suddenly screamed **scam**. A scammer pretended to be her daughter, knowing that a panicked mother wouldn't stop to verify.

Unfortunately, she wasn't alone. Every day, cybercriminals manipulate emotions to trick people into making costly mistakes. Here are five common emotional triggers they exploit—and how to spot them before it's too late.

1. Urgency – "Act Now, or Lose Something"

Scammers create artificial time pressure to rush you into making mistakes.

How It Works:

"Your bank account has been compromised! Verify your identity within two hours, or your funds will be frozen."

- *"Your payment has been completed." (when you know you never bought the item)*
- *"Your password is about to expire! Update it immediately here."*

How to Spot It:

- Contact the company directly using official contact info, such as calling on a trusted phone number or using the company's mobile app.
- Look for vague details in the message—legitimate companies provide specifics, not threats.

2. Fear – "Something Bad Will Happen"

Cybercriminals use fear to create panic, pushing victims to act without thinking.

How It Works:

- *"This is the government. You owe back taxes and must pay immediately, or you'll be arrested."*
- *"A virus has been detected on your device! Call this number for support."*
- *"If you don't pay this ransom, your private photos will be leaked."*

How to Spot It:

- Government agencies don't threaten via text or email.
- Tech companies won't reach out to fix your computer.

3. Curiosity – "You Won't Believe This!"

Scammers exploit curiosity by using shocking or enticing messages.

How It Works:

- *"Is this a video of you? 😳" (with a malicious link)*
- *"Breaking news! Huge celebrity scandal—click here to see."*
- *"Your friend tagged you in a crazy post!"*

How to Spot It:

- Be skeptical of sensational messages.
- Verify with the sender before clicking anything.

4. Trust & Authority – "This is Someone You Know"

Cybercriminals pretend to be trusted figures—bosses, banks, or even loved ones.

How It Works:

- *"Hi Mom, it's me! I lost my phone. Can you send money?"*
- *"This is your boss. I need you to purchase gift cards for an office event."*
- *"We detected suspicious activity in your account. Click to secure it now."*

How to Spot It:

- Create a secret passphrase with family members to verify each other's identity.
- Look for vague details—scammers often don't know your name or mailing address.
- Be wary of unusual requests—especially those involving money or sensitive info.

5. Excitement & Greed – "You've Won Something Amazing!"

Too-good-to-be-true scams prey on people's desire for rewards or attention.

How It Works:

- *"Congratulations! You've won a free iPhone—claim it now!"*
- *"You seem like a wonderful person, tell me more about yourself."*
- *"You've been selected for an exclusive investment opportunity."*

How to Spot It:

- If you didn't enter, you didn't win. Legitimate companies don't ask for fees to claim prizes.
- Be wary of strangers who persistently push something "too good to be true" or express romantic feelings too quickly.
- Be skeptical of "exclusive" offers sent randomly.

The next time you get an urgent text or phone call, stop, think, and verify before taking action. Don't let emotions be your weakness!

Guest Editor

Teressa Gehrke is the founder of PopCykol, an online safety and security awareness company. She has over 10 years of industry experience consulting as a technical writer, UX designer, and project manager. She's a board member of WiCyS Colorado. Teressa is an award-winning musician. Linktree

Resources

Romance Fueled Investment Scams: https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Defend Against Voice Cloning Attacks: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Text Messaging Attacks: A Smishing Saga: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/