WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 12 · WEEK OF SEP 21, 2026

FEATURE

Nigerian Princes, Free iPads, and the Evolution of Social Engineering

"I wonder when my free iPad's going to get here. I paid for the shipping fee." This seems more like a punchline than something that could happen to us. It would require the victim to be gullible. Technically illiterate. There was an attempt to be convincing, but who could possibly fall for that?

But a lot of people did. In fact, it was a serious problem during the rise of social media in the early 2010s. The 50-dollar inconvenience seems a lot less consequential than, let's say, identity theft. But that happened with 'Free iPad' victims too. The Nigerian Prince joke works the same way. A pop culture joke that bled people dry.

Social engineering is, simply put, manipulation. It exploits human vulnerabilities before digital ones. When 98% of cybersecurity incidents involve social engineering, it's essential to understand what forms it can take.

Which leads back to what this looks like for you. It still comes in the form of suspicious emails, but the phishing emails are written by AI, using personalized information about your company. Instead of claiming to be a Nigerian Prince, it's a phone call claiming to be your IT department. In an age where people can have entire meetings with deepfaked versions of their colleagues before wiring 25 million dollars, relying on classic tells such as grammar errors, far-fetched claims, and mismatched URLs won't work.

THE OLD TELLS

01 Typos & Grammar Errors
Attackers use AI to distribute emails en masse written flawlessly, regardless of their native language.

02 Email Address Typos
It's still good to check where it's coming from, but spoofing lets attackers fake the sender name and address entirely.

03 Hovering Over URLs
Bad actors can redirect domains to a completely different site. Hovering only shows the first hop or destination.

04 Direct Phone Calls
Voice cloning technology uses AI to take a snippet of your colleague's voice from a voicemail greeting. Once a sample is obtained, they can have full-fledged conversations with victims using a familiar voice.

05 Generic Greetings
AI can personalize communications easily by scraping the web for your name, location, and workplace. An old scam would start with, "Dear Customer." Now it's "Dear Ben, hope things are going well at RADICL."

06 Amateurish Website Designs
A poorly designed site impersonating Microsoft's login page could now be a picture-perfect replica using site cloning.

Conventional wisdom still has a place, but social engineering is a lot more convincing than it once was. So maybe the question isn't, "Does this look like a scam?" AI is making that question harder to answer.

The better question might be simpler:

Do I have to do that?

Usually, the answer is no. If you needed to download an attachment or click on a link, you'd probably be aware of it independent of an email.

Consider context. **Why do I have to log in again to view this file? Why do I have to wire finances within the next two hours? Why is IT calling me to reset my password over a phone call?**

That pause is important because social engineering depends on getting you to act before you think. The technology can make an email look legitimate, a website look familiar, and a voice sound like someone you know. But none of that changes whether the request itself makes sense.

MEET THE ANALYST

Maya Douglas

SOC ANALYST 2

Maya is a SOC Analyst 2 at RADICL Defense. Her security career began during her undergraduate CS program at CU Boulder and has spanned such roles as contracting at Microsoft and being cybersecurity lead for MSPs. She spent four years writing for Her Campus, which means she came into security already knowing how to tell a story.

> **Catching one bad login stops an incident. Catching that it's the same campaign hitting five clients across five industries turns it into an early warning for everyone else: that's the actual force multiplier of threat intel.**
>
> MAYA DOUGLAS, SOC ANALYST 2 · vSOC

ASK A SOC ANALYST

"What was the most convincing social engineering you've seen?"

SARAH MENNE

"While I was job hunting, I got this email from a recruiter using a name and company that matched a LinkedIn profile. The details didn't add up but it definitely made me pause."

MAYA DOUGLAS

"I met someone in person at a cybersecurity convention who told me about a tool and gave me his Discord. He sent me the GitHub repository there, and I started getting weird pop-up ads after I cloned it."

BRENDAN DEWYSE

"A 'mother' with a crying baby recording. I've seen it on a video. You could always go with the neon vest strat: throw on a safety vest, carry a clipboard, and walk right into a restricted area."

EYE ON THE THREATSCAPE

01 Iranian state-sponsored actors target journalists, dissidents using CHOSENBRICK

Social engineering is used to establish trust before sending CHOSENBRICK malware. Once it's downloaded, it poses as a legitimate app such as Pictory, KeePass, or Adobe Flash Player. Infected computers are connected to a Telegram bot to exfiltrate data.

02 This malware lets four AI models vote on its next move

Cisco Talos found CLOSEDQUORUM, a Windows implant with no human operator. It asks DeepSeek, Qwen, Mistral, and Gemini what to do, takes the majority vote, then steals passwords and crypto wallets.

03 The FBI boarded two hacked oil ships at sea

Two ships carrying crude oil to Texas were reportedly compromised mid-trip. The Coast Guard and FBI stated there were "no reports of operational disruptions, vessel instability, physical danger to crews, or environmental impacts."

THIS WEEK IN CYBER HISTORY

Sep 18, 2022. Grand Theft Auto VI was leaked on GTAForums.com. Rockstar Games issued a statement confirming an "unauthorized network intrusion" that prematurely revealed the settings and protagonists of the game. The content itself was in early development, but the final product should be available pretty soon.