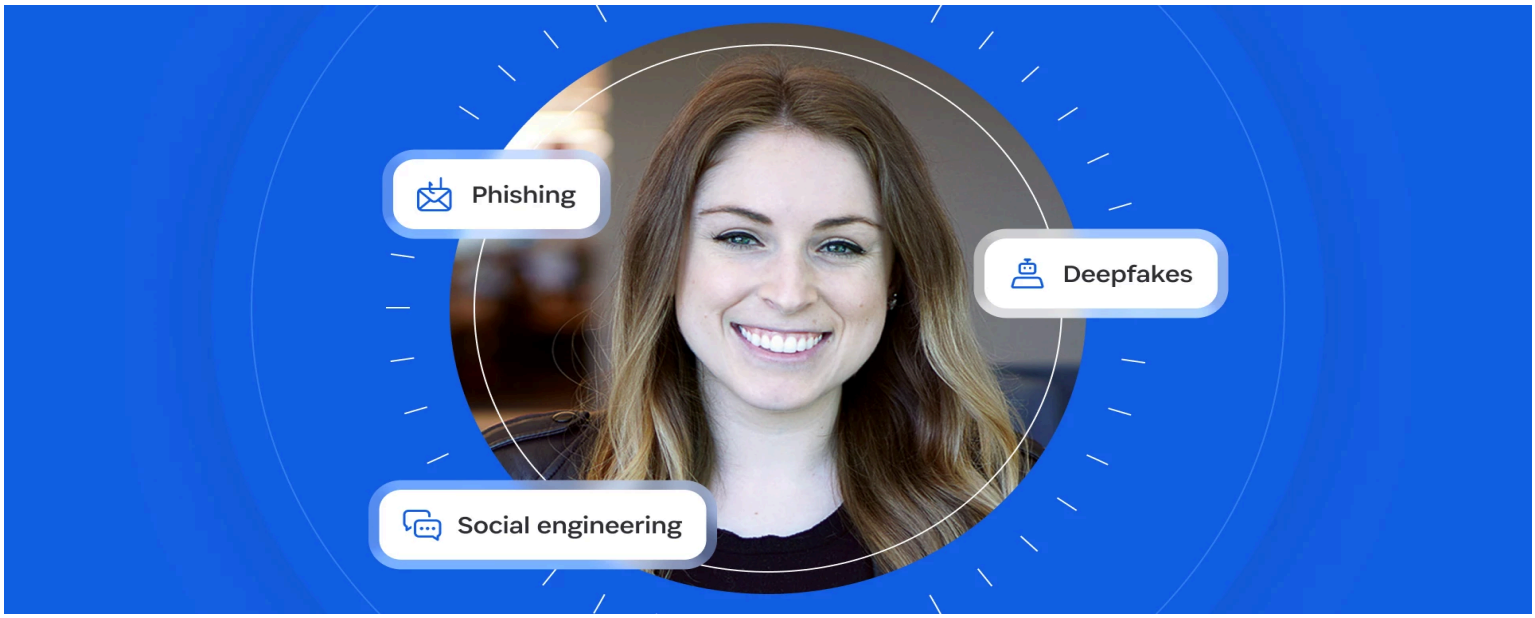
1P_jess
1Password Employee • 1 year ago

AI-powered social engineering attacks have arrived. Here's how to spot one.

Last edited: 4 months ago



Social engineering is a common tactic used by scammers to trick unsuspecting individuals into sharing sensitive information or access to confidential apps and systems. With the rise of AI, social engineering techniques have become even more sophisticated, making it harder than ever to know what to believe.

Thankfully, as social engineering has advanced, so have the strategies to keep yourself (and your data) safe. In the latest Random but Memorable episode, Rachel Tobac – an ethical [illegible] CEO of Social Proof Security – shares how to stay alert in a time of deepfakes and ChatGPT.

Chat

Can't see this video? ***Watch on YouTube***

How AI has made social engineering more sophisticated

One of the most useful aspects of AI is how it can handle tedious tasks and help us get our work done faster. However, that same ability to automate effort is exactly what can make AI so dangerous. Attackers can delegate the manual work of trying to gain access to sensitive information to AI agents. That allows them to target people in a shorter spaces of time, and increase the likelihood of successfully tricking *someone*.

> *"[AI] allows attackers to programmatically send all of those phone calls using AI agents without any intervention from the human. [The AI agents can] go out and collect all of those credentials and report back to the person who is managing the AI."*

Toback explains, "[Attackers] know how to choose the right target and they know how to spoof a phone call or make it look like they're emailing from the right email address. But what AI does is it scales that. It allows them to programmatically send all of those phone calls using AI agents without any intervention from the human. [The AI agents can] go out and collect all of those credentials and report back to the person who is managing the AI".

AI isn't just helping attackers scale their efforts; it's also making those exploits harder to detect. One example is how easy it has become to imitate someone's writing style, which has traditionally been a reliable way to spot impersonation attempts. Let's say you get an email from the HR department at work. If you've gotten similar emails before, you likely have a sense of HR's writing style. This can make legitimate company emails more recognizable, and, thankfully, it can also make unconvincing phishing attacks more obvious, too.

But thanks to AI-powered tools, Tobac explains that attackers can more accurately emulate a specific style of writing. They do this by referencing existing writing samples, like a leaked internal document, or prompting tools like ChatGPT to write in a more corporate tone. This can make the written impersonation far more convincing – and sometimes even indistinguishable from the author's own writing. As a result, it can elevate what would have been an obvious scam email to a convincing imitation with only a small amount of effort.

It's not just written content that's become easier to spoof. Both voice and video have become more imitable, meaning that being in a phone call with someone – or even a video call – may not guarantee you're actually speaking to that person.

> *"I can pop into a live Zoom or Teams call looking and sounding like the person that I'm trying to look and sound like. And that's quite scary."*

As Tobac describes, "It's definitely something that's more up and coming for attackers to try and do a live video deep fake... it's something that I can create usually in a few minutes with a machine that I have... I can pop into a live Zoom or Teams call looking and sounding like the person that I'm trying to look and sound like. And that's quite scary."

How to spot an AI-powered social engineering attack

Tobac recommends several strategies to stay diligent and safe against AI-supported social engineering threats.

Latency as an indicator of AI-powered tools

Listening for latency – or a delay – in a person's responses can help you recognize a deepfake in video and audio calls (in 2025, at least). If you're speaking to someone and notice a pause – about 800ms – before they start speaking, this could be an indicator that there's a tool being used to generate a response. (Tobak demonstrates what this delay typically sounds like in her Random but Memorable episode to help our listeners recognize it better.)

Movement in video calls to check for overlays

In video calls specifically, asking the person to move their hand in front of their face or move their head up and down, or side to side, is another technique to see if a tool is being used to mask an impersonator's actual appearance. Many tools can't yet seamlessly handle this movement, although this will likely change in the future.

Verify the person through another communication method

Tobac also suggests applying a “politely paranoid protocol” when it comes to conversations involving sensitive information. Specifically, she recommends taking steps to confirm the person you’re speaking to is actually who they claim to be – even if you’re on a call with them.

> *“It is the organization's job to make sure that their team understands when, where, and how to verify identity. So, somebody falling for this is not that individual's fault, even though it really does feel that way.”*

“Use a second method of communication to verify that person is who they say they are. [If] you get a call, reach out to them on Signal, Slack, email, any other method of communication. You get an email, you want to make sure there's not some sort of business email compromise or vendor email compromise. Pick up the phone, give them a call to the other method of communication you have on file.” Think of this like applying multi-factor authentication principles to the person you’re about to share sensitive information with; finding additional ways to double-check the person you’re communicating with is who they say they are can help you continue your conversation worry-free.

She notes that this should become part of the standard protocol for internal communications for businesses. “It is the organization's job to make sure that their team understands when, where, and how to verify identity. So, somebody falling for this is not that individual's fault, even though it really does feel that way.”

Don't forget the basics

While attackers continue to expand their social engineering toolkits, the fundamentals of online security still go a long way. Use a password manager, don’t reuse passwords, and turn on multi-factor authentication for all account logins. These simple steps remain some of the most effective ways to keep you and your data safe.

Interested in how AI impacts social engineering trends? Join us in this episode’s Community forum thread. Share your own approach to staying safe online and any of the more advanced AI-powered attacks you’ve seen.

Like Reply Follow Share

Leave a reply...

Was this helpful?

Related topics

August 2026 at 1Password: Smarter sign ins, secure AI agents, and safer developer secrets
Announcements

Developer newsletter: August 2025
Developers blog

How geopolitical hackers target and take down public infrastructure
Industry perspectives

1Password CISO Jacob DePriest explains how to build a strong security team
Industry perspectives

1Password's Abe Ankumah explains how businesses can securely adopt AI agents
Industry perspectives

Pricing

Downloads

Features

Autofill

Password sharing

Two-factor authentication

Passkeys

Solutions

Passwordless

Device Security

Compliance and Cyber Insurance

What's new

Community blog

Events

Developers

Discussions

Documentation

Integrations

Slack

Bug bounty

Resources

Guides and toolkits

Help and documentation

1Password blog

1Password Marketplace

Random but Memorable

Community guidelines

Company

About

We're hiring!

1Password

Terms of Service

Your Privacy Choices

Cookie Policy

Privacy Policy

Accessibility

©2026 1Password. All rights reserved.
4711 Yonge St, 10th Floor, Toronto Ontario, M2N 6K8, Canada