# AI-Generated Social Media Scams

Think that friend request or invite to connect came from a real person? Before you accept, here are 12 things to consider.

1

AI usage is increasing, along with the tactics of cybercriminals.

2

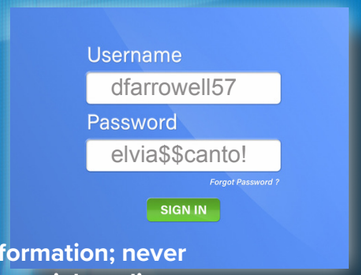
Cybercriminals use artificial intelligence to create realistic personas that can deceive users into sharing sensitive information.

3

AI-generated personas can mimic real people, complete with photos, bios, and relatable posts.

4

AI generated personas often engage in conversations to build trust before launching scams.




5

You might receive friend requests from AI generated contacts who seem to share your interests or appear to be thought leaders in your profession.

6

After friendly exchanges, scammers may ask for help with financial issues or request sensitive information about your organization.

9

Be cautious with personal and professional information; never share details with someone you've just met on social media.

10

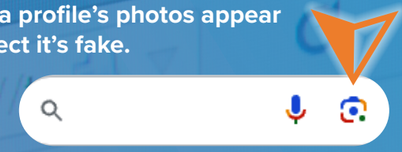
Watch for red flags, such as profiles with few friends, lack of personal posts, or generic bios, which may indicate a fake account.

8

Always verify profiles before interacting. Look for inconsistencies in photos, posts, and friends lists. Be a healthy skeptic.

11

Use reverse image search to check if a profile's photos appear elsewhere on the internet if you suspect it's fake.



7

Falling for these scams can lead to severe personal or professional consequences.

12

Report suspicious profiles to the platform immediately to help protect others from scams.

Barracuda