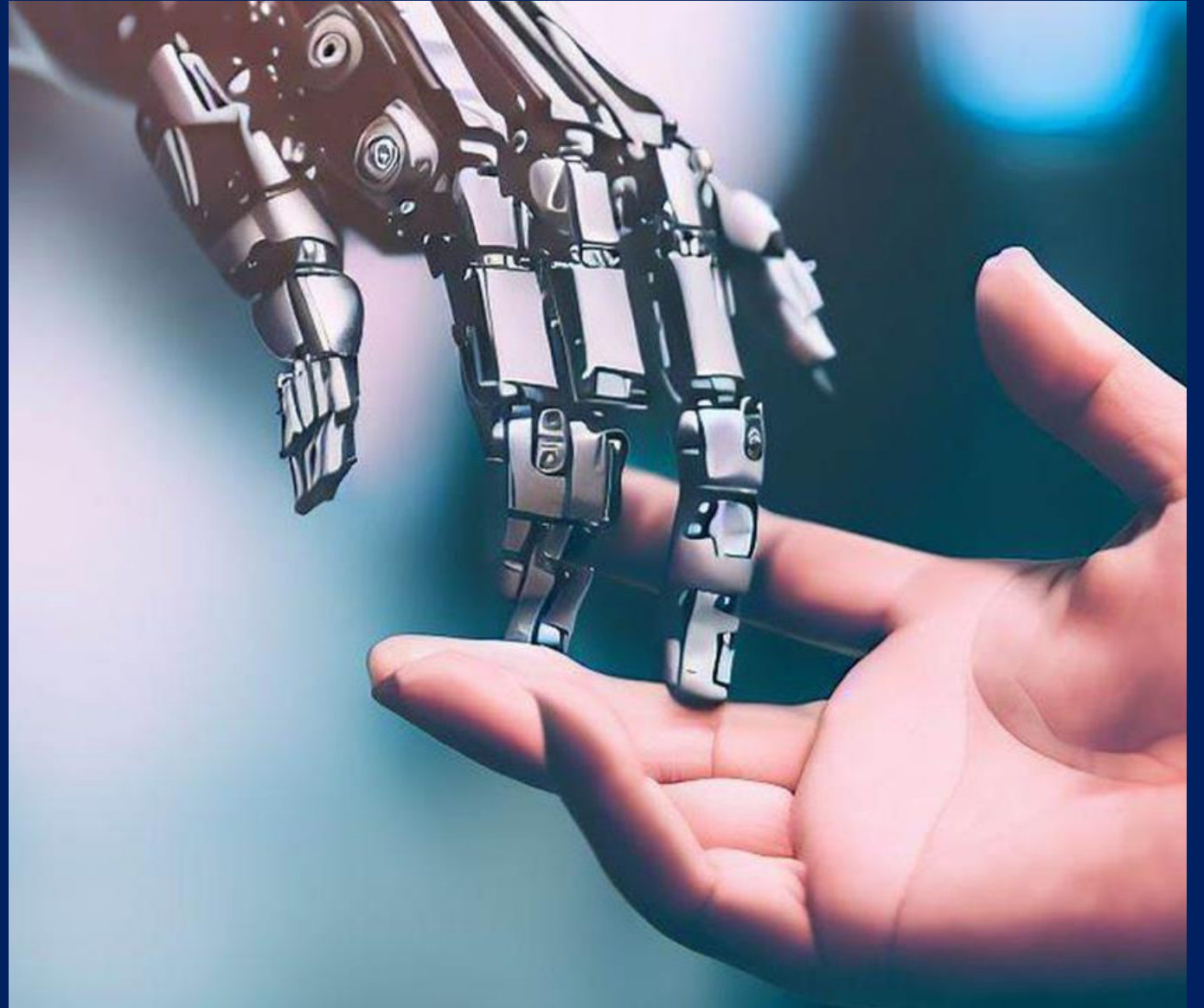


AI is here...

The increasing
use of artificial
intelligence in
frauds and
scams



What is Artificial Intelligence?

- Called AI for short
- It is a machine learning system producing a simulation of human intelligence
- It is the first new technology that can create rather than simply produce for a human creator
- It can analyze and use logic to make decisions
- It can do things humans can't do – interpret vast amounts of information, mimic voices, fake videos
- It is rapidly evolving in ways tech people do not understand

Why are scammers using AI?

- They can run their scams faster
- They can run their scams more convincingly
 - They'll know a lot about you from your social media
- They can run thousands and thousands of scams at once
 - They can use a chat bot for the grooming/love bombing stage and then deal with you directly when it's time to go for the money

Deep Fake Scams

- Deepfake technology uses AI to manipulate or create videos, voices, or images that appear genuine but are entirely fake.
- Scammers can create deepfake phone calls and videos impersonating individuals, including relatives, celebrities or high-ranking officials, to spread misinformation or orchestrate financial scams.
- Deepfake voice technology can be used to mimic someone's voice, leading to voice-based identity theft and fraudulent activities.



GMIA
→

What can you do to protect yourself?

- When you receive a call from your child or grandchild- they're in jail through no fault of their own! – it feels like you have to move fast.
- You don't.
- Tip offs that it's a scam –
 - what kind of payment they want – gift cards or bitcoin because they are untraceable. Or they will come to your house for cash.
 - They won't let you off the phone and DO NOT want you to call the police station or relatives
- A handy way to verify who you are talking to: a code word or phrase that all the family knows but is not written down or posted about. Make it random and simple, like "Bacon."

A celebrity wants to be friends or more!



What can you do to protect yourself?

- This one is easy! When a 'celebrity' contacts you, DO NOT RESPOND.
- If you have proceeded anyway, you may be able to confirm the scam by asking for a video call. (But maybe not.)
- You could ask to make the initial correspondence by US Mail (It would be hard to do and it is a Federal crime.)
- Ask the tech person in your life to run the photos to locate their initial source
- Never, ever, I mean never, believe they need money because all their millions are tied up.

Voices AND Faces



What can you do to protect yourself?

- Involve your friends and family
- Ask for a video chat, rather than a one-sided recording
- Remind yourself that seeing is NOT believing
- Step away and think about what you would say to a friend in this situation
- Remind yourself that, so far, no real celebrity has been documented fishing around Facebook looking for new friends
- Set your social media to private!

Phishing Attacks Enhanced by AI:

- Scammers use AI algorithms to create highly convincing and personalized phishing emails, messages, or websites.
- AI analyzes vast amounts of data about potential victims, such as social media posts, online behavior, and personal information, to craft targeted messages.
- Phishing emails may appear to come from trusted sources, such as banks or reputable companies, making it challenging for recipients to identify them as fraudulent.
- Phishing is not just in your email anymore but on social media such as LinkedIn, Indeed, Instagram, Facebook, Telegram, Discord, Twitter and other social media apps

Chatbot Scams

- AI-powered chatbots are designed to engage in realistic conversations with users.
- Scammers may use these chatbots to mimic customer support agents, providing a false sense of legitimacy.
- Victims may unknowingly disclose sensitive information or fall for fraudulent offers presented by these chatbots.



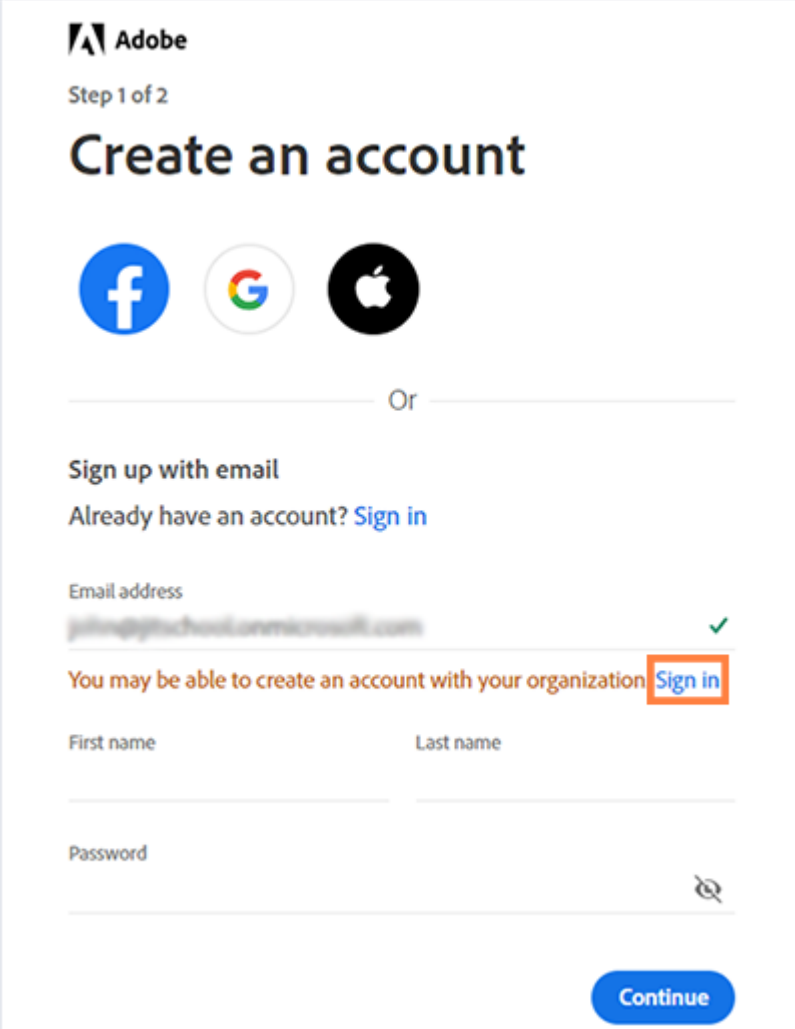
Social Engineering

- AI can analyze vast amounts of publicly available data to create detailed profiles of potential victims.
- Scammers use this information to craft targeted social engineering attacks, gaining the trust of victims and extracting sensitive data or financial resources.



Automatic Account Creation

- AI can be used to automate the creation of fake accounts on social media or other platforms.
- These accounts may then be used to propagate misinformation, promote scams, or conduct social engineering attacks.



The screenshot shows the Adobe account creation interface. At the top left is the Adobe logo. Below it, it says "Step 1 of 2" and "Create an account". There are three social media icons: Facebook, Google, and Apple. Below these is an "Or" separator. The main heading is "Sign up with email". Below that, it says "Already have an account? Sign in". There is an "Email address" field with a checkmark on the right. Below the email field, there is a message: "You may be able to create an account with your organization" followed by a "Sign in" button. Below this are fields for "First name" and "Last name", and a "Password" field with a visibility icon. At the bottom right is a blue "Continue" button.

What can you do to protect yourself?

- You will never be able to memorize all the different types of scams—there are too many and new ones all the time.
- Your radar should go up when:
 1. It involves money
 2. It requires personal information or clicking a link or QR code
 3. It is a hurry
 4. You are not allowed to hang up and call back
 5. The news is surprising! Your account is locked, your grandson is in jail, your power is about to be shut off, there is an arrest warrant

When the news is surprising & unexpected

- VERIFY – set up a code word in your family. For businesses, hang up and call the main number.
- Most of all – STOP, PAUSE, DELAY, CHECK
- GIVE YOURSELF TIME – to think logically about next steps.
 - Grandson is kidnapped? You are not Rambo – call their mom or the police.
 - Power is about to be shut off? Hang up and call the main number.
 - About to be arrested? The police do not inform fugitives that they are coming.
 - Crypto/gold/coins/foreign currency seems like a great investment? Hang up and talk to a financial advisor. Don't be that guy that bought Iraqi dinar.
 - The President, a politician, or a newscaster is in a video of ****shocking**** news? If it's true, *every* news network will report it.

We do not know where all this is going SO...

- Make the decision today that you believe NOTHING from a surprise contact. Rather than trying to assess whether something is a scam, decide ahead of time that it is.
- If it is a company, look up their web address or phone number and contact them directly.
- The IRS and Medicare will NEVER contact you to ask for personal information
- If your nephew is suddenly in jail, call his mom or call the police
- If Brad Pitt suddenly turns up on your Facebook Messenger and says, “Hey, baby girl” ...RUN.

These scams are so difficult to detect because...

- We believe in our eyes and ears. The old saying “I’ll have to see it to believe it” needs to be changed to:

“I’ll believe it after I’ve checked it out ten ways to Sunday.”

You always have time, and time is on your side.

After all that bad news...

- The Fraud and Scam Reduction Act passed in 2021 prioritizes scams against older Americans and will educate financial institutions, wire transfer companies, retailers on how to spot scams.
- If you have been scammed, throw embarrassment out the window and reach out for help to the Police, Dept of Aging, The PA Link, Crime Victim's Center, and the National Elder Fraud Hotline.
- Remember that there ARE still good people in the world.

Need help with programs and services?

Call the Link!

1-800-753-8827



Contact Information

- The PA Link: 800-753-8827
- National Elder Fraud Hotline: 833-372-8311
- Crime Victims Center:
 - Bucks 800-322-4472
 - Chester 610-692-7420
 - Montgomery 888-521-0983
- Dept of Aging:
 - Bucks: 267-880-5700
 - Chester: 610-344-6350
 - Montgomery: 610-278-3601