JPMorganChase

Cyber Safety for Good

SENIOR CITIZENS

REQUEST A SESSION

Keeping yourself safe on the internet and in the digital world around you doesn't have to be hard! Here are some helpful tips to stay safe and secure online.

DEVICES

- When using smart home devices and digital assistants, remember that they are only as secure as you make them!
- Regularly back up the data on your devices (cell phones/computers/tablets) preferably to an external source.

PASSWORDS

- Make each password a phrase and as unique as possible.
- When choosing a password, remember: the longer the better!
- If you need help keeping track of all your unique passwords, you can use a password manager.

SOCIAL MEDIA

- When posting on social media, never share sensitive information like location or vacation plans.
- Stay skeptical of what you see online, on social media or in ads – ask a friend or family member before acting.
- Everything you post online will stay online **forever** so think twice before you hit send/post.

SCAMS

- Scams can come in many forms, from emails saying you've won a prize to calls from fake government agencies.
- If you fall victim to a scam, stay calm, change your passwords, gather as much information as possible, and contact your financial institutions and law enforcement.

DEFENDING YOURSELF

- To help defend your technology from malware attacks, get anti-virus protection and keep it updated regularly.
- Set up automatic updates for your operating system, internet browser, software/apps and anti-virus protection to keep yourself secure!
- When using your credit/debit card online, verify that you're on a reputable and valid website – whether shopping, donating or anything else.

ARTIFICIAL INTELLIGENCE

- AI refers to technology/computers programmed to do tasks that humans typically do.
- When using generative AI tools, avoid using the email account you use for banking, work, social media, etc.
- Be discreet and diligent by giving AI chatbots parameters instead of personal information.
- Voice deepfakes are an emerging threat – establish a safe word to determine if an urgent phone request is coming from a family member in distress – ***pause before taking action***.

PHISHING

- Beware of phishing attacks - they can come in multiple forms: phone calls, text messages and email!
- Practice safe email habits by never following links/instructions from unknown sources.
- Always question what you see and never send sensitive information if you're unsure about a request.