Warning: Beware of AI Voice Phishing Scams

In recent times, there has been a rise in sophisticated voice phishing (vishing) scams leveraging artificial intelligence (Al) technology. These scams involve the use of Al-generated voices that convincingly mimic real individuals or authoritative figures to deceive victims. Here's a crucial warning to help you stay vigilant:

- Unsolicited Calls:
 - Be cautious of unexpected calls, especially if the caller claims to represent a trusted institution, government agency, or financial organization. Al-generated voices may sound remarkably genuine, making it challenging to distinguish from real calls.
- Verify Caller Identity:
 Before providing any sensitive information or following instructions, verify the caller's identity independently. Use official contact details obtained from legitimate sources, such as the organization's official website or customer service hotline.
- Avoid Immediate Actions:

 Scammers often pressure victims into taking immediate actions, such as sharing personal information, passwords, or making urgent financial transactions. Take your time to assess the legitimacy of the call and avoid making impulsive decisions.
- Personal Information Protection:
 Refrain from sharing sensitive personal information, such as social security numbers, passwords, or financial details, over the phone unless you can verify the authenticity of the call.
- Be Skeptical of Threats:

 Scammers may use threats or urgent scenarios to manipulate victims. Be skeptical of calls claiming legal actions, account suspensions, or other emergencies. Verify such claims independently before taking any action
- Educate Others:

 Share this warning with friends, family, and colleagues to raise awareness. The more informed individuals are, the better equipped they are to recognize and avoid falling victim to AI voice phishing scams.



Remember, scammers are continually evolving their tactics, and AI voice phishing is a concerning development. Stay vigilant, trust your instincts, and verify the authenticity of any unexpected calls to protect yourself and your personal information. If you suspect a scam, report it to relevant authorities or your local consumer protection agency.

The most effective course of action when receiving a call from an unrecognized number or name, claiming to represent a significant state or federal agency, is to exercise caution and verify the caller. Politely request the caller's name, title, department, and a return phone number. If possible, independently verify the caller's identity by reaching out to the respective state or federal agency through a different phone number or email.

New York State Regional Information Centers Data Privacy and Security Service

