Scam Type	How you are targeted	Examples	What to do
Phishing Scams	• emails • Text messages • Phone calls • Phone messages	An email from your bank asking you to verify your account details. A text message from the post office asking you to verify your personal details. A phone call or message from the tax office saying that you owe money and to call a number.	Always check the sender's email address, or phone number. Never click on links or download attachments. Report suspicious emails, text messages and phone calls to the company.
AI Chatbots	• Social media • Websites	A chatbot on social media promising to help you find a job if you provide personal details. A message request after commenting on a business's social media page.	Check the legitimacy of the service (Google the exact phrase, then add Scam). Use official websites or trusted sources. Avoid sharing personal information.
Job Scams	• Job search sites • Social Media • Text messages	A job listing asking for a fee to access training materials for a position that seems too easy.	Never pay for job or training. Check the company's official website for job listings. Report suspicious job postings.
Online Shopping Scams	• Fake websites	A website selling product or gadgets at a fraction of the market price, but they don't deliver after payment.	Shop only from trusted websites. Look at customer reviews. Use secure payment methods.

Scam Type	How you are targeted	Examples	What to do
Tech Support Scams	• Your computer • I-pad/tablet • phone	Calls or pop-ups claiming your computer has a virus. A pop-up message saying, "Your computer is infected! Call this number for support." A call from Microsoft saying there is a problem with your computer.	Don't give remote access to your computer. Contact trusted tech support directly if you suspect issues. Hang up on unsolicited calls.
Romance Catfishing	• Dating App • Dating Websites	Very attractive and professional looking pictures Messages at odd hours Over the top attention and compliments Asking for money or gift vouchers	Reverse image search suspect pictures Report and block NEVER share personal details NEVER send money, gift vouchers or crypto currency
Investment Scams	• Social Media • Ads on web pages	Promises of high returns on AI/Crypto-related investments. An ad claiming you can double your money by investing in a new AI/Crypto technology.	Research thoroughly before investing. Be careful of offers that seem too good to be true. Consult with trusted friends or financial advisors.
Lottery/Prize Scams	• emails • Text messages	Messages claiming you've won a prize or lottery. A text message saying you've won a $10,000 lottery but need to pay a fee to claim it.	Do not respond or provide personal information. Verify any claims through official sources. Report scams to local authorities.