Grandparent scam

- Scammers prey on grandparents, who may not always be up to date with what their grandchild is doing.
- Scammers call, pretending the grandchild has gotten into some trouble and needs cash quickly.
- Scammers will stress the importance of sending cash through the mail or sending money through a wire transfer.
- Scammers use scare tactics to intimidate grandparents into paying quickly. They might imply that the grandchild is in physical danger or living in bad conditions in a jail overseas.
- Scammers do their homework on your family, checking social media profiles and other online sources to learn grandchildren's names, and sometimes even their travel plans.

To decrease the likelihood of becoming a victim, look for these possible indicators:

- If you ever get a call from or about a grandchild or any other relative in danger or trouble, and the immediate request is for cash, you need to pause and calm yourself.
- Ask the caller for their contact information then consult another family member first.
- Also contact your grandchild to confirm they are okay.
- If you can not make contact with your grandchild to confirm this is a scam, call the police.

Virtual Kidnapping Scams

- Scammers call you from an unknown number and the person on the phone tells you he has your adult daughter held captive.
- Prior to calling you, he has already called your adult daughter, forcing her to make statements, like, "Dad, help me". The scammer tells your daughter he will hurt you if she doesn't make these statements and if she tells you about this call.
- The scammers will play this statement in the background of the call, reinforcing the scam indicating he has your daughter held captive.
- The scammer will direct you to immediately wire a certain amount of money to a specific account.
- The scammer will state that if you hang up the phone before the money is wired, they will hurt your daughter.

To decrease the likelihood of becoming a victim, look for these possible indicators:

- Incoming calls come from an outside area code.
- Calls do not come from the kidnapped victim's phone
- Callers go to great lengths to keep you on the phone
- Callers prevent you from calling or locating the "kidnapped" victim
- Ransom money is only accepted via wire transfer service
- A red flag should be raised anytime a wire transfer is requested.

Support Tech Scams

- Scammers call you directly on your phone and pretend to be representatives of a software company, like Dell or Microsoft.
- Scammers will spoof the caller ID so that it displays a legitimate support phone number from a trusted company.
- Scammers may have you check your computer for specific file names that every computer has, then says the file is a virus.
- Scammers will ask you to install applications that give them remote access to your device.
- Using remote access, these experienced scammers can misrepresent normal system output as signs of problems.
- These fake error messages aim to trick you into calling an indicated technical support hotline.
- When you engage with the scammers, they can offer fake solutions for your "problems" and ask for payment in the form of a one-time fee or subscription to a purported support service

To decrease the likelihood of becoming a victim, look for these possible indicators:

- Microsoft does not send unsolicited email messages or make unsolicited phone calls to request personal or financial information, or to provide technical support to fix your computer.
- Microsoft will never know there is an issue with your computer unless you tell them. Therefore, any communication with Microsoft has to be initiated by you.
- You should only call phone numbers that you find through an independent source such as a phone book or online search
- If a notification appears with a phone number, don't call the number. Error and warning messages from Microsoft never include a phone number.

Lottery Scam

- Scammers will contact you via mail, telephone, social media, or email notifying you that you have won a lot of money or a fantastic prize in a competition, lottery or sweepstake that you don't remember entering.
- The winning notification you receive will ask you to respond quickly or risk missing out.
- To claim your prize, you will be asked to pay a fee. Scammers will often say these fees are for insurance costs, government taxes, bank fees or courier charges.
- The scammers make money by continually collecting these fees from you and stalling the payment of your winnings.
- The scammer may also urge you to keep your winnings private or confidential, to 'maintain security' or stop other people from getting your prize by mistake.
- Scammers do this to prevent you from seeking further information or advice from independent sources.

To decrease the likelihood of becoming a victim, look for these possible indicators:

- If you haven't entered a lottery or competition, you can't win it.
- Verify the identity of the contact by calling the relevant organization directly – find them through an independent source such as a phone book or online search. Do **not** use the contact details provided in the message sent to you.
- Do an internet search on any of the details of the competition – many scams can be identified this way.
- Never send money or give credit card, online account details, or copies of important personal documents to anyone you don't know or trust.

Overall Protection from Scams

47

- Be cautious about what you share on social media and consider only connecting with people you already know.
- Be sure to use privacy settings on all social media and online accounts. Imposters often get information about their targets from their online interactions and can make themselves sound like a friend or family member because they know so much about you.
- Never send money to someone you have never met face-to-face.
- Never share personally identifiable information, such as banking and credit card information, your date of birth, and Social Security number.
- Don't be pressured to act immediately**.** Scammers typically try to make you think something is scarce or a limited time offer.
- Scammers weigh heavily in on the sense of urgency for you to act.