SCAM NAME	HOW IT WORKS
AMAZON IMPOSTER	An Amazon imposter seeks to convince targets that significant and questionable charges have appeared on their account. The scam often leads to the criminal gaining account access, or even gaining access to the target's device to install key logging malware.
Amazon doesn't work this way. Any communication from the giant that induces worry should be a red flag. Check your account yourself on the website or app.	
BAIL MONEY–ARREST ACTIVITY	A criminal sends a social media direct message, SMS text or places a direct phone call stating that a loved one has been arrested and requires bail money.
Do not respond to the person contacting you. Disengage and call the loved one or someone closely associated with the person to validate that no problem exists.	
BENEFITS APPLICATIONS	Victims are contacted at random and advised that a recent government benefits application has been delayed due to a paperwork problem. The criminal may ask the victim to photograph and send their government-issued ID via SMS text.
Refrain from speaking with or providing information or images to an unknown party. Government IDs should be reported as stolen if provided to a criminal via SMS text or other method.	
CRYPTOCURRENCY	Cryptocurrency is often a major component of various scams because it is easily liquidated and virtually untraceable. Criminals pressure victims into withdrawing cash so that it can later be deposited into a criminally-controlled cryptocurrency account.
Do not deposit cash into an ATM that converts it into a cryptocurrency account or sends it to a digital wallet.	

FAKE JOB SCAMS	Scammers pretend to be hiring managers in order to steal personal information from people who have posted their resumes on various job seeking websites; criminals may also attempt to ask for funds to pay for hiring fees or equipment.
Job seekers receiving questionable contact about work opportunities should call the HR department of the company in question to validate the contact and to confirm any associated hiring expenses.	
GIFT CARDS	Criminals treat gift cards like portable currency. Victims are instructed to provide the card and activation codes via SMS text or voice calls so that the criminal can quickly drain the available funds.
There is no legitimate reason a gift card is required to pay for anything – especially during an emergency situation. Disengage and personally verify all claims.	
HUGE RETAIL BARGAINS	Cybercriminals often create websites that offer outrageous bargains that lure innocent shoppers. The same websites are often full of harmful malware in addition to collecting personal information during a transaction for goods that do not exist.
Purchase from reputable merchants that offer dependable guarantees and a safe payment space.	
LOTTERY	Lottery scams are very common. Victims, who may not have even played the lotto, are convinced to send money and information to claim a nonexistent prize by criminal imposters.
Lotteries and similar contests do not require any payment to participate or receive winnings. Anyone suggesting otherwise is lying.	
MEDICAL	Criminal imposters often request personal information and payments related to medical care. Most medical scams are randomized and target victims via email, phone calls and SMS text messages.
Do not provide personal details or payments to an out-of-the blue contact; only share sensitive information with trusted healthcare providers.	
PEER-TO-PEER (P2P)	Peer-to-peer payments are legitimate and convenient ways for consumers to rapidly send funds to friends and family. Criminals often convince victims to send funds for nonexistent bills and sometimes they take over the P2P account to perform unauthorized payments.
Never provide P2P account login and password information to anyone. Never send funds to unknown persons or agree to transfer funds on behalf of unknown persons.	

REAL ESTATE

Real estate scams are abundant. Criminals target victims by monitoring "for sale" listings and public information websites so that they can pose as a closing attorney requesting settlement fees be re-directed to an account controlled by the criminal.

Never wire or send funds to a receiver in advance of a real estate closing transaction. Further verification can be obtained by contacting the settlement attorney directly.

RENTAL

Criminals impersonate government or nonprofit employees and request personal info and money up front for fake rental assistance programs.

Consumers need to verify that they are using a legitimate government or nonprofit agency. Report fraud directly to the Consumer Financial Protection Bureau at https://www.consumerfinance.gov/

ONLINE ROMANCE

Older adults are often more vulnerable to romance scams when they are socially isolated or experiencing troubled family relationships. Cybercriminals seize upon vulnerable adults by appealing to their need for validation and interaction. The losses associated with romance scams can be devastating if left undetected.

Beware of romantic interests who lavish attention and praise almost immediately upon contact. Talk about your new acquaintance with friends or family to balance your perceptions.

TAX DEBT

Imposter scams are legion today because criminals know that law-abiding citizens are threatened by news that they suddenly owe a debt to the government for taxes. Criminals make every attempt possible to convince their victims to send rapid payments before the victim realizes that they do not actually owe any pressing tax debts.

Hang up on calls and ignore all other forms of contact pertaining to tax debt especially if they are threatening or coercive. U.S. consumers should contact the IRS or equivalent state agency directly to verify claims regarding unpaid tax debts.

VIRTUAL PHONE OR TEXT SERVICE

Criminals sometimes find fraud victims by responding to an online "for sale" ad by posing as an interested buyer of a high value item like an automobile. The criminal asks the seller to verify his or her identity before sending a payment for the item and advises the seller that a verification code will be sent to their mobile device to confirm their identity. The criminal, in this scenario, is actually using the victim's mobile device number and name to open a virtual phone or text service that will be later used in other fraud schemes. The verification code generated and sent to the victim's device is actually a verification code used to establish the fraudulent account. Once the fraudulent account is opened, the criminal simply tells the victim that they no longer wish to purchase the item.

Never share verification codes with anyone. Disengage from communication as soon as a request is made to read back a verification code.

VIRUS & MALWARE

Scams leveraging the threat of costly malware and virus mitigation are often called "tech support scams". Cyber criminals often contact victims unexpectedly using a variety of communication methods. When victims accept assistance from tech support scammers they are often victimized by numerous requests for money and they may also lose control of other sensitive financial accounts that reside on the device that is taken over by the criminal under the pretense of helping the victim remotely.

Do not give remote access to personal devices to unknown parties. Never respond to pop-up virus alerts, links, or call numbers that appear within the pop-up windows. Remember: Caller ID is not a reliable method for determining the identity of a caller since this information can be manipulated.