The Addison Police Department frequently receives reports regarding various frauds and scams, including some instances where people impersonate Village employees. Below is a list of known frauds and scams reported to the Addison Police Department. Please note that this is not an exhaustive list of all frauds and scams; *it is crucial for Addison residents to remain vigilant*. In an effort to keep our residents informed, and thus reduce the number of victims, the Addison Police Department is alerting residents to the following:

Phishing: What is it?

Phishing, as the term suggests, refers to the practice of "fishing for victims." Scammers impersonate legitimate organizations or companies, sending emails or making phone calls that appear official in order to solicit sensitive information from unsuspecting individuals.

If you receive an email or pop-up requesting personal or financial information, it is crucial that you do not respond or engage. Avoid clicking on any links or pop-ups, and refrain from providing personal information over the phone unless you have initiated the call and are certain of the recipient’s identity.

What You Can Do:

1. **Verify Requests:** Reputable companies will never request sensitive information via email or phone. If in doubt, contact the organization directly using a phone number you know to be legitimate.
2. **Protect Your Information:** Never disclose information such as bank account details, passwords, or Social Security numbers to unknown parties.
3. **Stay Updated:** Ensure that your computer's antivirus and anti-spyware software are current to help protect against phishing attacks.

By staying vigilant and informed, you can better safeguard your personal and financial information from phishing attempts.

Fake Warrant Scam

In this scam, Victims may receive phone calls, emails, or text messages claiming that an arrest warrants have been issued in their names. Potential victims are instructed to call a specific number or follow a specific link that has been provided in order to arrange to avoid arrest. The scammer will then pose as a law

enforcement official (often times it's a "Sheriff") these fraudsters may request that a settlement be paid via wire transfer, money order, or prepaid/gift card.

In an attempt to deceive the victim and prove "legitimacy", fake warrants are crafted to appear official, often featuring logos of an unspecified "United States District Court," a case number, and various charges. Common allegations include offenses such as missed jury duty, unpaid taxes or unpaid bills of sorts.

Important Reminder: A legitimate arrest warrant is always served in person by a U.S. Marshal or another law enforcement officer. Importantly, law enforcement will never request payment over the phone.

What Can I Do?

- **Phone Calls:** If you receive a suspicious phone call, hang up immediately. Block and delete the number to prevent further contact.
- **Emails:** If you receive an email related to this scam, delete it without engaging, and do not click on any provided links.
- **Text Messages:** If you receive a text message from a suspected scammer, block the number and delete the message. Again, do not follow any links included in the text.

Gift Card Scams

In this scam, criminals deceive people to purchase gift/prepaid cards as a form of payment for utilities, taxes, computer problems, medical expenses or to "clear" a warrant, amongst other things. Once the gift/prepaid card is purchased, the scammer will ask for the numbers on the back of the card. Once you provide the numbers, your money is gone.

What Can I Do?

- **Understand Gift Card Usage:** Gift cards are intended for personal gifts, not as a form of payment. If someone demands payment via gift cards, it is a clear indication of a scam. No legitimate government agency, utility company, or business will ever request payment in this manner.
- **What can I do?:**
    - **Phone Calls:** If you receive a call instructing you to make a payment with gift cards, hang up immediately and block the number.
    - **Emails:** If you receive an email requesting payment via gift cards, delete it without engaging. Do not click on any links included in the email or text message.

Additional Precautions:

- **Verify Legitimacy:** If you have any doubts about the authenticity of a call or email, contact the company directly. Do not rely on the caller ID displayed on your phone or call back any number provided in a voice message.
- **Independent Research:** Look up the company's official contact information online and initiate the call or email yourself. This ensures you are communicating with the legitimate organization.

Amazon Impersonation Scam

In this scam, the victim receives a phone call, email or text from "Amazon" notifying them of an unauthorized purchase or suspicious activity on their account. The victim could be instructed to download an app to rectify the error, press a number to speak to a “customer service representative” or follow a link to submit a refund request. In these scenarios, the fake "Amazon" could ask for your account details looking to steal your personal information. Or the fake "Amazon" might “accidentally” give a larger refund and advise the victim to buy gift cards to “pay back” Amazon for the overpayment. If an app is downloaded or link is followed by the victim, the offender could get access to their banking information and apps to commit more fraud.

What Can I Do?

1. **Avoid Unrecognized Numbers:** Do not call back any number that you do not recognize. Instead, use the contact information available on the official website of the company in question.
2. **Verify Communication Sources:** Always rely on known contact details rather than any numbers provided in unexpected emails or text messages.
3. **No Gift Card Payments:** Never agree to pay for goods or services using gift cards. Legitimate businesses will not request payment in this manner.
4. **Protect Your Devices:** Do not grant remote access to your device or share personal, banking, or account information with anyone who contacts you unexpectedly.

Home Repair/Improvement Scams

Key Reminder: These scams often times relate to ***driveway seal coating*** or ***roofing repair/replacement***. The scams are more prevalent after a bad storm or weather event.

In this scam, the scammer will often times wear “construction type clothing” and drive a pickup or a van in order to appear like a reputable construction company. The pickup/van will have no or non-descriptive lettering on the side of the vehicle. The scammer will often say that they are in the neighborhood doing work on some of the neighbors’ houses and they have extra material left over or since they are already in the area, they are willing to reduce their prices in order to obtain additional projects. The scammer will often times say “today only” or “working in your area this week only” in order to create a sense of urgency. The scammer will additionally advise that the project costs a certain amount of money but then provide a significantly lower “cash only” discount if the victim pays upfront.

What Can I Do?

1. **Check Local Regulations:** Soliciting door-to-door is illegal in most towns. Be cautious of anyone engaging in this practice.
2. **Look for Identifiable Vehicles:** Beware of contractors who do not have their trucks clearly marked with company branding. This can be a red flag.
3. **Trust Your Instincts:** If a deal sounds too good to be true, it likely is. Be wary of offers that seem unusually advantageous.
4. **Request References:** Always ask for references and specific addresses of previous work. Insist that they return after you’ve had a chance to verify these details in person.
5. **Payment Method:** If a contractor insists on cash payments or requests that checks made out to "cash," proceed with caution. Never write a check to “cash.” A reputable contractor will always request payment made out to the business name.
6. **Verify Credentials:** If you have any doubts, ask for their contractor's license number, driver's license, and certificates of insurance. If they only provide information verbally, tell them to return the next business day after you have had time to verify their credentials.

Overpayment/Fake Check Scam

In this scam, a victim lists an item for sale on an online platform (such as Facebook Marketplace or Craigslist). The buyer then pays more than the agreed

selling price, either by sending a counterfeit check or making an overpayment through a digital wallet like PayPal or Cash App. The buyer requests a refund for the "overpayment," often asking the seller to send the excess amount to a third party via Zelle or another online payment app, claiming it was an error or that they need to cover shipping costs.

Unfortunately, once the seller complies, the seller later discovers that the deposited check has bounced or the buyer's payment has been reversed, resulting in the seller losing both the money refunded and the item sold.

What Can I Do?

1. **Verify Payment Legitimacy:** Never ship an item before confirming that the payment is valid and has cleared.
2. **Be Wary of Overpayments:** Offers that involve overpayment should raise immediate red flags. Trust your instincts—if it seems too good to be true, it likely is.
3. **Report Suspicious Activity:** If you encounter dishonest buyers or sellers, report them to the online marketplace to help protect others from falling victim to similar scams.

Tollway Scam

In this scam, you may receive a text message claiming that your Illinois toll account has been overdrawn. The message typically urges you to follow a link to add funds to your account to avoid potential fines.

What Can I Do?

1. **Do Not Click the Link:** Avoid clicking on any links provided in the message, as they may lead to phishing websites designed to steal your personal information.
2. **Verify the Claim:** If you have concerns about your toll account, visit the official Illinois tollway website directly or contact their customer service using verified contact information.

Romance/Sweetheart Scam

In this type of scam, a con artist pretends to be romantically interested in their victim, often exploiting emotions to gain trust and ultimately steal money. While these scams can occur in person, they predominantly take place online, targeting individuals, particularly lonely seniors or those who are widowed or divorced. The

scammer may foster a deceptive relationship, sometimes waiting months before soliciting funds, all while convincing the victim of a deep and committed bond.

What Can I Do?

Sweetheart scammers are adept manipulators, and it is crucial to remain vigilant for warning signs that may indicate the relationship is fraudulent:

1. **Avoiding Privacy:** If the scammer is eager to leave the dating platform's messaging system for phone calls or email, this could be a red flag.
2. **Excuses to Avoid Meeting:** Be wary if the person continually provides excuses to avoid in-person meetings.
3. **Repeated Financial Requests:** A sudden request for a “loan” that evolves into ongoing pleas for money related to family expenses, housing issues, medical problems, or failed business ventures should raise concerns.

Trust Your Instincts: If something feels off, trust your intuition. Protect yourself by being cautious and seeking advice from trusted friends or family members. Awareness is key to avoiding sweetheart/romance scams.

Arrest Scam

In this scam, the caller informs you that your loved one has been arrested and requests bond money for their release from jail. A similar scam involves a caller claiming to be a relative or friend, who asks you to send payment to get them out of jail.

What can I Do? If someone calls informing you that a loved one needs to be bonded out of jail, find out which jurisdiction the individual is in and call that agency directly to confirm that the person has, in fact, been arrested. Ask questions.

Grandparent Scam

The Grandparent Scam involves scammers contacting older adults and impersonating their grandchildren. The conversation typically begins with a phrase like, “Hi Grandma/Grandpa, it’s me!” This prompts the grandparent to respond with the name of their grandchild, providing the scammer with personal information.

*Additional personal information may have been obtained via social media.

Once the scammer has established this identity and gained a certain level of trust, they often create a sense of urgency by claiming they are in a difficult situation, such as being involved in a car accident, facing arrest, or having a stolen wallet and are in need of money. They may assert that they are out of the country and request money be sent via Western Union or MoneyGram. The scammer will often ask the grandparent to keep the matter secret, suggesting that other family members would be upset if they found out.

In some cases, the scam may involve the scammer impersonating a police officer, adding an illusion of credibility. The scam can also occur through email rather than a phone call.

*This scam usually appears more during holidays and school break seasons especially during high travel season *Spring break, summer break, winter break, Memorial day, Independence day etc.

What Can I Do?

1. **Avoid Acting Hastily:** Resist the urge to respond immediately to the call or email. Scammers thrive on creating panic and urgency.
2. **Verify the Information:** Contact your grandchild or other family members to confirm the details before taking any action. Hang up the phone call and call the family member in question, or call other family members who would be able to contact the
3. **Do Not Send Money:** Never send money based solely on information provided in a phone call or email. Always verify the situation first.

IRS Telephone Scam

In this scam, potential victims are often told they are entitled to large refunds or that they owe money that must be paid immediately to the IRS. If the scammer is unsuccessful in their initial attempt, they may call back with a different approach. This type of scam frequently targets immigrants, who may be threatened with deportation, arrest, utility shut-off, or revocation of their driver’s licenses. Scammers may also resort to insulting victims to instill fear and manipulate them.

What Can I Do?

1. **Official IRS Communication:** The IRS will always send a written notification of any tax due via U.S. mail. If you receive a phone call claiming you owe money, it is likely a scam.
2. **No Payment Requests Over the Phone:** The IRS never asks for credit card, debit card, or prepaid card information over the telephone. Any such request should raise immediate suspicions.
3. **Report Scams:** For more information or to report a scam, visit www.irs.gov and enter "scam" in the search box.

Utility Scam

In this scam, an individual posing as a representative from the local utility company visits during a power outage, claiming they can reconnect the victim's service for a cash payment. The victim may find the situation suspicious but rationalizes the request, thinking that since the power is out, the company might be unable to process payments through their systems. The impersonator appears legitimate, and the victim, desperate for service restoration, pays the requested amount.

However, hours later, the victim finds that their utilities remain disconnected, and the scammer is nowhere to be found. Ultimately, the utility company restores service independently, not the fraudulent representative.

Key Reminder:

Local utility companies, including the Village of Addison electric and water utility, will **never** send someone door-to-door during an outage to request cash payments for service restoration.

What Can I Do?

- **Verify Identity:** Do not engage with individuals asking for cash payments at your door. Contact your utility company directly using official contact information to confirm any requests.
- **Report Suspicious Activity:** If you suspect a scam, report it to local authorities or your utility company immediately.

"Can You Hear Me?" Scam

In this scam, a caller will typically ask, "Can you hear me?" as soon as you pick up the phone, trying to elicit a "yes" response. They may fumble their words or

claim issues with their headset to create confusion and encourage you to reply. According to the Better Business Bureau, scammers can use your affirmative response to falsely claim that you authorized major purchases, such as vacation packages, cruises, warranties, and other high-value items.

What Can I Do?

1. **Do Not Respond with "Yes":** If you receive a call from an unfamiliar number and the caller asks if you can hear them, do not answer "yes." Instead, simply hang up.
2. **Stay Alert to Other Tactics:** Scammers frequently change their strategies as awareness increases. Be cautious of any other questions designed to elicit a simple "yes" answer.
3. **Do Not Answer Unknown numbers:** If you do not recognize the phone number, do not answer. Let the call go to voicemail.

Lottery Scams

In this scam, the fraudster pretends to have won a local lottery but claims they are ineligible to collect the winnings due to various reasons, such as age or immigration status. The scammer presents a fake or fraudulent lottery ticket and proposes to split the winnings with the victim. They typically ask for an amount far lower than the ticket's purported value, creating a sense of urgency and making the offer seem like a "good deal."

The scammer may pressure the victim by claiming they are under a tight deadline, encouraging them to go to an ATM or bank to withdraw cash. Once the victim has withdrawn the money, the scammer hands over the fraudulent ticket. Later, the victim discovers that the ticket is worthless.

What Can I Do?

1. **Skepticism Towards Lottery Wins:** Be wary of anyone claiming to have won a lottery, especially if they ask for your help to claim the winnings.
2. **Avoid High-Pressure Situations:** If someone is pushing you to act quickly, it's a major red flag. Legitimate lottery claims do not involve such urgency.
3. **Verify Authenticity:** Always verify the legitimacy of any lottery ticket before making any financial commitments. Contact the lottery organization directly if necessary.

Foreign Lotteries or Sweepstakes

In this scam, victims receive notifications via email, phone, or postal mail claiming they have won a lottery. To claim their prize money, they are instructed to send a check to cover fees, taxes, or insurance. Scammers may even send a check for the “alleged” lottery winnings. While the check may initially appear to clear in the victim’s bank account, it is soon discovered to be fraudulent after the victim has sent the required "fees."

In a variation of this scam, a check is mailed to the recipient, accompanied by a request to cash the check and wire back funds to cover “taxes, fees, or insurance” in order to claim the prize. However, the original check is ultimately worthless.

What Can I Do?

1. **Illegal Participation:** It is illegal for U.S. citizens to enter foreign sweepstakes or lotteries.
2. **Red Flags:** If you are asked to send money to claim a prize, especially if you have received a check, it is a significant red flag.

Jewelry Scam

In this scam,

Tech Support Scam

In this scam, individuals posing as representatives from a high-profile tech company contact victims, claiming that their computers are either infected with computer virus’ or “malware” or at risk of infection. The scammers often create a sense of urgency, suggesting that the virus or malware could cause significant damage to the computer and their personal information., The scammer will then pressure victims to grant them remote access to troubleshoot and resolve the supposed issues.

By allowing remote access, victims enable scammers to manipulate their systems, install malware and virus’, create errors, and potentially access personal and financial information. Additionally, the scammers may then charge for unnecessary repair services.

Key Reminders:

1. **Never Grant Remote Access:** Do not allow anyone to take remote control of your computer, especially if they contacted you unsolicited.

2. **Professional Help:** If you need computer assistance, hire a reputable local repair service rather than relying on unsolicited offers.
3. **Do Not Answer Unknown numbers:** If you do not recognize the phone number, do not answer. Let the call go to voicemail.

Collection Agency Scam

In this scam, perpetrators impersonate representatives from a collection agency and make cold calls to victims, threatening lawsuits or embarrassing confrontations at their workplaces unless they start making payments. The scammers typically request payment through non-returnable methods, such as MoneyGram, Western Union, or wire transfer. In some cases, they may even possess information about a legitimate outstanding loan, making their claims seem more credible. Victims may face ongoing harassment for months.

What Can I Do?

1. **Verify the Collection Agency:** If you believe you have a bad debt, do your homework to confirm the legitimacy of the collection agency contacting you. Look up their official contact information and reach out directly.
2. **Ignore Suspicious Calls:** If you receive calls from unknown collection agencies that you cannot verify, consider blocking those numbers.
3. **Know Your Rights:** Familiarize yourself with your rights as a consumer regarding debt collection. The Fair Debt Collection Practices Act (FDCPA) protects you from harassment and deceptive practices.

Obituary Scam

In this scam, fraudsters target the surviving spouse by reading the obituary columns and presenting fake bills, claiming that these were owed by the deceased. In some cases, scammers may even deliver packages, asserting that they are items the deceased ordered and for which payment is now due.

What can I Do?

1. **Verify Outstanding Bills:** Always check with the relevant company or business to confirm any outstanding bills purportedly owed by the deceased. Do not accept invoices at face value.
2. **Reject Unordered Packages:** If you receive packages that you did not personally order, do not accept them. Contact the sender or relevant authorities to report the situation.