



## ELDRIDGE POLICE DEPARTMENT

**Joseph Sisler**

Chief of Police

### CRIME PREVENTION / SAFETY TIPS

*The following are crime prevention tips the Eldridge Police Department encourages its citizens and visitors to utilize to prevent themselves and their property from being targets of crime. While no method is perfect, there are steps that people can take to protect themselves and reduce the risk that they will be victimized.*

#### INTERNET AND ONLINE SAFETY

*Today, people use the internet for many things daily. Below are some tips we'd like to share with you to help make your use of the internet safer for you and your children*

##### **Online Safety Tips for Parents**

- *Keep the computer in a common area, such as the family or living room. This helps you monitor your child's computer use.*
- *Spend time with your child online and talk to them about their internet use. Ask to see their profile page(s). Many children have more than one profile. Google your child's name.*
- *Snapchat is the most commonly used social media app by teenagers and adolescents, mostly because content (messages, photos, or videos) automatically deletes after they are opened. This has made Snapchat the primary means of 'sexting' between teenagers as well as adults. Please use discretion when deciding if you will allow your child to install Snapchat on their phone.*
- *Know your child's screen names and passwords. Ask your child to add you as a "friend" on his/her profile page.*
- *Limit the information allowed in online profiles and make sure profiles and post settings are set to private.*
- *Control access to chat rooms and Instant Messaging. Monitor the sites they are visiting by clicking the internet browser's History button.*
- *Teach children to avoid risky behavior, such as accepting friend/message requests from strangers, flirting, or discussing sex online with people they do not know in person, posting sexually suggestive material, or being rude or mean to someone online.*
- *Remind children that computer use is not confidential.*
- *Keep the lines of communication open.*

305 North 3rd Street, Eldridge, Iowa 52748

Phone (563) 285-9822 • Fax (563) 285-9835 • [police@cityofeldridgeia.org](mailto:police@cityofeldridgeia.org)

- *Make agreements about computer use, such as:*
  - *Approved websites they are allowed to visit*
  - *Length of time they can be online*
  - *Basic safety rules*
    - *Never give out personal information (name, age, address, phone) or use a credit card online without permission*
    - *Never share passwords with anyone, including friends.*
    - *Never arrange to meet in person someone they met online.*
    - *Never reply to a bully or any other uncomfortable messages they receive online.*
    - *Agree upon the consequences for not following the rules or breaking the agreement. It can be helpful to write down the rules and agreements in the form of a contract.*

### *Online Safety Tips for Kids*

- *Don't share your password – even with your best friend.*
- *Know who your friends are! Make sure you have met someone in person before you accept a friend/message request.*
- *Don't post anything you wouldn't want your grandmother to see.*
- *What you post online stays online FOREVER (even if you think it's deleted), so think before you post.*
- *Pay attention to how you are communicating. Don't say anything online you wouldn't say in person. Don't be rude online.*
- *Protect your privacy and your friend's privacy too...get their permission before posting something about them.*
- *Check what your friends are posting or saying about you. Even if you are careful, they may be putting you at risk.*
- *Don't take, keep, or send nude or partially nude pictures of yourself or others. You could be prosecuted for creating or distributing child pornography if you possess or send nude or partially nude pictures of someone under the age of 18.*
- *Tell a trusted adult if someone does or says something online that makes you feel uncomfortable.*
- *Unless you're prepared to attach your Facebook page to your college/job/internship/scholarship or sports team application, don't post it publicly!*
- *Don't become an addict. The key to becoming a well-rounded adult is to find a balance between your online experience and your in-person social encounters.*

### *Online Shopping*

- *Don't give your personal information unless you are absolutely sure that it is safe.*
- *Create strong passwords, especially those associated with your bank or credit card information.*
  - *Use a combination of letters, numbers, and at least one capital letter and special character (@#\$%^&\*)*

- *This means where possible, not giving out your full name, your address, your phone number, your credit card number, your social security number, or information about your family and friends.*
- *If you have to give a name to register or login to a forum or for some other online purpose, use a nickname or alias where possible.*
- *Sometimes you'll want to give personal details, including your credit card number, for online shopping. This is OK, as long as the online seller is reputable and has secure shopping facilities.*
- *Secure shopping means that they use secure servers which receive and store your personal information in encrypted form so that if anyone intercepts your transaction, they won't be able to decode the data and get your details.*
- *Secure site pages will have addresses starting with 'https' rather than 'http' (eg. You might browse around their site on unsecured pages, and then when you are ready to make a purchase, you'll be switched to secured pages).*

## **Residential Safety**

*In order to protect your home and property, the Eldridge Police Department encourages citizens to follow the tips below:*

- **Walk** around your home as though you were a burglar trying to look for ways to get inside. If you find vulnerable spots, take the necessary steps to secure those access points.
- **Always** lock your doors and windows. Exterior doors should be made from strong wood or metal and should be locked with a deadbolt. Install guards on windows that prevent them from being raised more than a few inches.
- **Leave** a light on (perhaps on a timer) when you go away, even for the evening. You may also leave a television or radio on as well.
- **Install** motion sensor lights outside your home and out of reach so burglars cannot unscrew the light. Also, buy variable light timers to activate lights in your home.
- If you live in an apartment building, **NEVER** prop open the door or let someone in behind you. If the building has a main entryway, make sure that security is enforced at the main door. Report residents who do this to your landlord.
- **Be vigilant** – If you suspect suspicious activity around your home, your neighbor's homes, or in your neighborhood, please report it to the police immediately by calling **911**.
- **Document** serial numbers of all electronics and tools and take pictures of all valuables. Keep this in a safe place to provide to the police in the event you are burglarized.

## **Scams & Fraud Prevention**

*While advances in technology have created ways to make our lives easier, they have also created new ways for scammers and thieves to prey on unsuspecting citizens. If you believe you may have been a victim of a scam or fraud, you are encouraged to contact your local law enforcement agency. Here are some of the more common types of scams, tips to identify scams, and how to avoid falling victim to fraud.*

## Phone Scams

Even though they may sound outdated, phone scams are still a frequently used method by scammers to defraud people. Senior citizens are especially vulnerable to these types of scams. These calls are always **unsolicited**, and the caller will try to get you to **send them money or provide your personal identifying information** (social security number, bank account numbers, login/passwords, etc.) The callers will prey on your emotions, specifically your fear, generosity, or greed. Here are some examples of common phone scams:

- **Advance fee/Windfall Scam**

- The caller claims you have won a sweepstake, or the lottery, or have inherited a large sum of money, but you must pay a “small fee” or “tax” to claim the money. Some scammers go as far as to mail the victim a check that appears to be real. However, these checks always return as non-sufficient funds, usually after the victim has already sent the caller the payment.
- Sometimes, the caller will request bank account or credit card information so they can “process” the money. Once they have your account information, they can empty your bank account.
- **Never send a check or wire money to someone who calls you.**
- **Never provide your bank account information to anyone over the phone or email.**
- **If it sounds too good to be true, it probably is.**

- **IRS/Tax Scam**

- The caller, claiming to be from the IRS, calls or leaves a voice message stating you owe back taxes and threatens that, unless funds are wired immediately, legal action will be taken, or you’ll be arrested (or they may say you have a refund waiting but need to verify personal info before sending).
- This scam is especially prevalent during and immediately after-tax season.
- **The IRS will never call you about matters like this; they send all notices via US Mail.**
- **If you are ever unsure, hang up the phone, find your local IRS branch’s phone number in the phone book or from an internet search, and call to verify.**

- **Tech Support**

- In this scenario, a scammer posing as a technical support representative calls to claim there is an issue with your computer – for example, that your software is outdated or that you need to confirm your identity – and asks for remote access to resolve the issue. Once you provide this access, the scammer may request payment for tech assistance, install malicious software, change settings to leave your computer vulnerable, and/or steal your financial information.
- These callers often use a lot of high-tech jargon or language in the hopes the victim will believe their story.

- Sometimes the caller can “spoof” their phone number, meaning your caller ID displays a different name or phone number.
  - **No real companies call you, especially unsolicited, to fix your computer or install updates.**
  - **Immediately turn off your computer if you believe you have given unauthorized access to someone.**
  - **Never give someone remote access to your computer.**
  - **Never provide your password or personal information to a caller asking to “confirm your identity”.**
- 
- **Charity Scam**
    - Many scammers will call you posing as a representative for a charity, asking for a donation. They often claim the donation is for cancer patients, police/firefighters, natural disaster victims, or some other group of people to tug at your heartstrings (and your purse/wallet strings).
    - Callers can even claim to work for a well-known charity (Red Cross, St. Jude’s, etc.).
    - They may ask for bank account information to “process your donation”.
    - **Ask for the caller’s full name and the name of the charity. Thoroughly research any charity before donating by visiting their website. If you decide to donate, only do so through a secure website, or by mailing a check directly to the organization’s headquarters.**
    - **Never give your bank account or personal identifying information to anyone over the phone.**
- 
- **Police/Law Enforcement Scam**
    - The caller claims to be a law enforcement officer, detective, federal agent, or other police agency from another country. They may tell you that you or a loved one is in some sort of legal trouble, and to avoid being arrested or having an arrest warrant issued, or to release a family member in jail, you must send or wire money.
    - They usually give generic names like “Officer Dan Smith” or “Agent Mark Johnson” or they may use an actual officer’s name.
    - **Ask for the officer’s full name, title, badge number, and agency/department, and write it down.**
    - **Tell the caller you want to verify who they are. Hang up, look up the agency/police department’s phone number online or in the phone book, call that number and ask to speak to the person who called you.**
    - **Police will NEVER call you and demand money/payment in order to avoid an arrest warrant or criminal charges.**

## Internet / E-mail Scams

The anonymity of the internet has made it a prime instrument to utilize to commit fraud. Many online scammers operate out of different states or even different countries, making it difficult to locate or prosecute them. This is why developing safe online habits is so important to avoid becoming a victim of fraud or identity theft. Here are some examples of online scams:

### ○ “Phishing” Scams

- “Phishing” is when a scammer sends an e-mail or text message purporting to be from a reputable company to induce individuals to reveal personal information, such as passwords or credit card numbers.
- These messages often contain a link to a website that appears legitimate but is not.
  - For example, PayPal’s actual website URL is <https://www.paypal.com>. An example phishing site URL may be <http://www.pay-pal1.me>. At first glance, it may look like PayPal’s website, but it is not. While it looks like you are logging in, you are actually sending the scammer your login information. They will then spend all the money in your account.
- Here you can see an example of an actual phishing text message. The sender is attempting to get the recipient’s Craigslist login information, using an out-of-area phone number. The link may also go to a website that installs malware or a virus on the victim’s phone, giving the sender access to sensitive data.
- **Never click a link sent to you in an unsolicited e-mail unless you are absolutely sure it is safe.**
- **If you do follow a link from a message asking you to log in, close the page and type in the website URL yourself to make sure you are on the real website.**

### ○ Craigslist / Marketplace Fraud

- In this scheme, if you have posted an item for sale on Craigslist or another online marketplace, you may receive an e-mail or text message from someone offering to pay you more money than you are asking for the item. Ultimately, the “buyer” sends a check or pays with PayPal and asks you to mail them the item.
- After you have sent the item, either the check will bounce or the PayPal charge will be disputed, leaving you out the money AND the item you were selling.

## Door-to-Door / In-Person Scams

Some bolder thieves will commit their scams in person. Like phone scammers, they frequently use high-pressure techniques or can be or become aggressive. Citizens should use EXTREME caution if an unknown person or solicitor asks to come inside their home. Burglars have been

known to use a rouse to get into a home, during which time they will “case” the home for valuables to determine if they can burglarize the residence later. Here are a couple of examples of door-to-door scams:

- **Door-to-Door Charity Scam**

- A person comes to your door, claiming to work for a charity, and asks for a donation. They usually state they can only accept cash, or a check was written to them (not in the name of the charity).
- **Never write a check made out to the solicitor’s name.**
- **Ask to see identification and ask lots of questions. While some scammers may have false credentials, they are likely to get scared away if questioned too much.**
- **Call the police if you are unsure the solicitor is legitimate. Most cities require a solicitor’s permit to go door-to-door. The police can more easily verify the person’s identity.**

- **Contractor Fraud**

- A “contractor” tells you they can do home repairs for you, often at a great discount. They will require full or partial payment upfront.
- Many of these scammers will solicit you (e.g. “I noticed your roof is in need of repairs” or “I have leftover supplies from another job and want to offer them to you at a great discount”).
- After doing minimal work, the “contractor” will never show up again, leaving the victim out the money they paid upfront.
- **Do your research before hiring a contractor. Only used a licensed contractor; they are certified and are highly knowledgeable about building codes and other legal/safety requirements.**
- **Ask about permits. If they say they don’t need permits, they are probably not licensed.**
- **Some legitimate contractors do require money upfront. Only pay a contractor upfront if you are certain, you can locate them again or you verified who they are in the event they stop showing up to do the job.**

## **Vehicle Burglary/Theft Prevention**

Motor vehicle burglaries/thefts have risen dramatically over the past few years. In most cases, the victim’s vehicle was left unlocked, or the garage door was left open. In the cases where entry was forced, valuables or other targeted items were often left in plain view. Discovering your vehicle has been burglarized can be a horrible feeling, the feeling of being violated. You don’t just lose your belongings; you lose your sense of security and privacy. These quick, easy steps can deter thieves from stealing your items:

1. **Always lock your car doors**
2. **Don't leave valuables in plain view**
3. **Park in well-lit areas**
4. **Report any suspicious activity to the police**

### *"Lock It Up" Initiative*

*Starting in 2016, the Quad Cities region began experiencing a spike in stolen vehicles. In 2016 and the first quarter of 2017, Quad Cities law enforcement agencies received reports of approximately 750 stolen vehicles. The Quad Cities law enforcement community has been working together in a collaborative effort of sharing information, strategies, and resources to combat this growing issue.*

*The vast majority of the reported car thefts have been crimes of opportunity, where vehicles are left **RUNNING UNATTENDED**, or **UNLOCKED WITH KEYS INSIDE (in the driveway, along the street, or open garage door)**. These thefts are not limited to certain cities or neighborhoods; they can/have occurred all over the Quad Cities. Many of the suspects are juveniles, some as young as 11 or 12 years of age. These stolen vehicles are being used to commit thefts, burglaries, shootings, and other crimes. Usually, the vehicles will flee from law enforcement, driving recklessly and putting the members of our community and their property in serious danger. Too often, these stolen cars end up involved in hit-and-run crashes.*

*There have been multiple items left unsecured in unlocked vehicles during these thefts/burglaries. Items such as guns (often used in shootings or used to commit serious crimes), money, computers, purses, and other valuables.*

*In order to combat this growing trend, the Eldridge Police Department wants to encourage citizens and visitors to take the following steps to deter these thefts and hopefully keep themselves from becoming a victim:*

- **Always lock your car doors.**
- **Do not leave your car keys in your car, even if it is locked.**
- **Do not leave valuables, especially guns or other weapons.**
- **Be aware of your surroundings and report any suspicious activity to the police.**
- **Do not, under ANY circumstances, leave your car running unattended. Most thefts take less than 10 seconds.**
  - **Even cars that require a key fob/push button start can be stolen if left running unattended.**
- **Do not leave your garage door open, especially if you leave your residence or during the evening hours.**

*Remember if it looks off or you see something that looks suspicious or is too good to be true contact the Eldridge Police Department or your local law enforcement agency for clarification before falling victim. Watch out for and educate your children and elderly family members as they are primary targets.*