North Reading Police Department
Community Alert: Tips to Protect

- Resist the pressure to act quickly. A scammer wants you to act quickly so you have less time to think and realize you are being scammed.
- Never give out personal identifiable information including what bank you use, account numbers, family names or birthdates.
- If contacted about a grandchild, contact your grandchild or another family member to determine whether or not the call is legitimate.
- Do not answer phone calls from unknown numbers.
- A government agency will never ask you to pay them using gift cards or crypto currencies such as Bitcoin or Dogecoin. A government agency or business will never send anyone to your house to pick up money.
- A government agency will never make threats when you do not comply with a request.
- Gift cards are never used as a way of payment to anyone.
- Never wire money based on a request made over the phone or in an e-mail, especially overseas.
- Make sure your computer's anti-virus and security software and malware protection is up to date.
- Never send anyone you don't know intimate or personal photographs.
- Communicating through an app such as WhatsApp or Words with Friends does not mean the person is legitimate.
- Never give remote access to anyone. If you feel that your computer has been compromised, shut it down and unplug and get it checked by a technology professional.

Common Scam Red Flags

- Asking for gift cards to be sent or to have gift card codes sent.
- Threats over the phone or e-mail threatening arrest or prosecution.
- Calls or emails saying you have a computer issue when you didn't initiate the help.
- Getting a panicked call from a "relative" saying they need money immediately.

When in doubt, call the North Reading Police Department at **978-664-3131 ext. 0** and speak with an officer BEFORE you send any money; the earlier you call, the better. Once money is sent, it is very hard to recover. Please share these tips and red flags with friends and family.