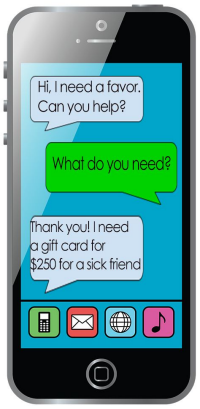


BEWARE:

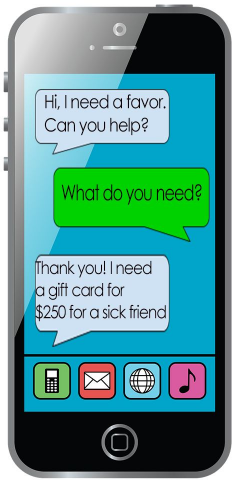
CYBER SCAMMERS' LATEST TEXT SCAMS TARGETING ADLA SCHOOLS AND PARISHES

"Smishing" (SMS phishing) is a type of fraudulent activity that involves using SMS or text messages to trick people into giving up personal information so that money can be fraudulently obtained. Perpetrators use various techniques to gain the trust of a victim and may provide specific instructions, which if followed, could result in monetary loss to the victim. Perpetrators may impersonate someone you know that is in some position of authority (a priest, teacher, manager, police, or government agency).

DO NOT BECOME A VICTIM. If you receive such texts do the following:

- Take time to consider your actions before responding to suspicious text messages.
- If in doubt, call the **published main number** of the parish, school or administrative office from whom the text claims to have been sent to authenticate the text message.
- Do not respond to the text message if you doubt its origin.

For more information, and to stay up to date about the latest cyber security threats impacting ADLA locations, visit the ADLA website or https://www.consumer.ftc.gov/features/scam-alerts



BEWARE:

CYBER SCAMMERS LATEST TEXT SCAMS TARGETING ADLA SCHOOLS AND PARISHES

"Smishing" (SMS phishing) is a type of fraudulent activity that involves using SMS or text messages to trick people into giving up personal or confidential information so that money can be fraudulently obtained. Perpetrators use various social engineering techniques to gain the trust of a victim and usually provide specific instructions, which if followed, usually result in some sort of monetary loss to the victim.

Smishing is very much like phishing (email-based scams). Perpetrators will impersonate someone you know that is in some position of authority (a priest, teacher, manager, police, or government agency) and will advise you of some emergency or crisis that requires your attention. They will ask (or demand) that you do something to resolve the situation (provide your passwords, click on a link that takes you to some web site or buy a gift card and text them the card information). They may even ask you to call them at the number they are texting from to "verify" that they are who they say they are.

DO NOT BECOME A VICTIM. If you receive such texts do the following:

- Take time to consider your actions before responding to suspicious text messages.
- Ask yourself if the sender, if genuine, would really contact you via text.
- If in doubt, call the **published main number** of the parish, school or administrative office from whom the text claims to have been sent to authenticate the text message.
- Remember that even if the text message seems to come from someone you trust, their number may have been hacked or spoofed. Look closely at the area code of the number. If it is not a local area code then the text may not be legitimate.
- Do not click on links in text messages unless you are 100% certain that they are genuine and well-intentioned.
- Do not respond to the text message if you doubt its origin. A response could be used as a verification that your number is responsive to text messages and you may be inundated with similar messages. Hackers build and sell lists of numbers to others for fraudulent purposes.

For more information, and to stay up to date about the latest cyber security threats impacting ADLA locations, visit the ADLA website or https://www.consumer.ftc.gov/features/scam-alerts