HAVE YOU GOTTEN A TEXT MESSAGE WITH AN OFFER THAT SOUNDS "TOO GOOD TO BE TRUE?"

THEN IT PROBABLY IS!

BE ON THE LOOKOUT FOR SMISHING TEXTS.

THEY ARE MORE COMMON THAN YOU MIGHT THINK... AND CAN POTENTIALLY CAUSE YOU MORE THAN JUST AGGRAVATION!

WHAT IS SMISHING?

Text message phishing or smishing is a form of social engineering using text messages - it is the act of attempting to acquire personal information such as passwords and details by masquerading as a trustworthy entity in a text message.

WHAT CAN YOU DO TO AVOID BECOMING A VICTIM?

Awareness is the key to protecting yourself from becoming the victim of a smishing scam. A text message may contain a piece of information that seems to be of a personal nature - which is designed to make the offer seem credible... a piece of info you may have inadvertntly posted on Social Media.

- Don't reply to the text message or call the number. Even if the text message says "text 'stop' to stop receiving messages," never reply.
- Do a web search of both the number and the message content. Type the number, message (or both) into Google search.
- If the smishing message is spoofing a company, call the company directly, and inquire about the message you received. If they confirm that it's not from them, delete it.
- Don't click on any links in the message. Often, scammers don't need you to give up personal info - all they need to do is pique your interest enough to get you to click on a link and download a virus to your phone.

WHAT SHOULD YOU LOOK OUT FOR?

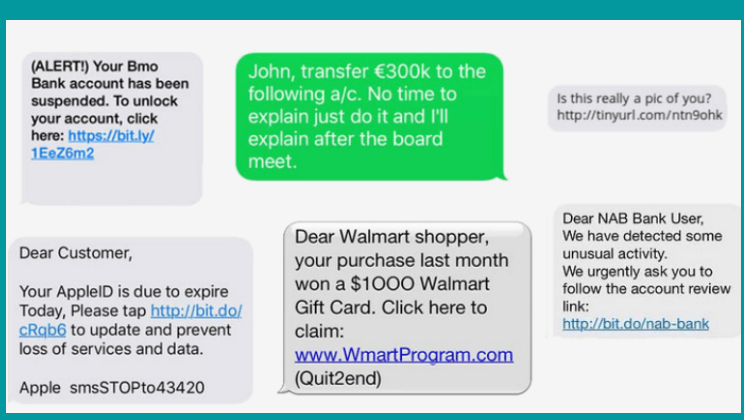
Overall, what smishers are usually looking for is the missing piece of the puzzle. That could be a social security number, pin number, password, or any other private detail that will help them access your accounts. It's easy to say "don't give it to them," yet many smishing scams are intricately designed to elicit a response, even if that response is just a tentative and short-lived click on a link.

Be weary of unusual text messages from people you don't know or companies offering free products.

Be careful that you don't post info on Social Media that could reveal any portion of your passwords.

Remember your best practices regarding passwords -
DO NOT tell anyone what your passwords are for ANY of your accounts
(not even if they say they are from your "IT" department!)

Here are just a few examples of common Smishing texts



DON'T HESITATE TO CHECK THESE RESOURCES FOR MORE INFORMATION

For more information regarding work use of home computers, visit these sites:

- Oneida Co. Acceptable Use Policy
- NYS Information Security Policy
- NYS Acceptable Use of Technology Resources Policy

Don't hesitate to contact the IT department if you need assistance with determining if a text message is a scam.

Better to be safe than sorry!

ONEIDA COUNTY
www.ocgov.net