WFG National Title

SAFE Tipsheet

Beware of Smishing! What's that?

December 2021

Are you planning a much-needed holiday vacation to somewhere sunny and warm or some winter wonderland? Nice!

Time away from the office with no more ringing phones, Zoom calls, no phishing emails with scary attachments and dangerous links to avoid can be a welcome treat. It's just you and your family, the open road, and your mobile phone.

However, there are many ways you can be phished other than traditional phishing and spear phishing using email. You can also be phished using your mobile phone - no email needed! It's called Smishing (SMS Phishing) and involves you and a text message. Hackers can send a text to try to trick you into believing that you have won something or that the text is from your bank or your credit card company with some issue that needs to be resolved quickly. Just like an email, they may ask you to enter your login information, or they may provide a link to confirm a charge or verify your SS number or other sensitive data about yourself. They may even provide a "secure" phone number for you to contact them instead.

NOTE!
Collecting your information by voice over the phone is called Vishing (Voice Phishing). But that's a whole other kettle of . . . Phish, to learn about later.

How do you avoid smishing while out and about with family and friends? In much the same way as you avoid email phishing:

- ☑ **Do** install a good antivirus app on your personal mobile phone (i.e., BitDefender or Norton).
- ☑ **Do** consider using a VPN on your mobile devices.
- ☑ **Do** a web search for the number and message content. You may find many others have received the same message confirming it is Smishing
- ☑ **Don't** click on links or attachments in an unfamiliar or unexpected text message. It's the easiest way for a hacker to get you to install malware on your phone or take you to a fake site that wants your login information.
- ☑ **Don't** reply to a text message from a number you do not know, even if it prompts you to "Text Stop" to stop further messages.
- ☑ **Don't** call a number provided in a text. If it says it's from a bank or other company, call their main number directly.

If you did happen to click on a link in an unknown text message, and you haven't installed antivirus yet, do it now and then scan your cell phone and follow the directions.

Take these easy-to-follow steps to keep this holiday season, and the rest of your year, worry-free from smishing.