TMC
SPOT SCAMS AND MALWARE

BE AWARE OF THE SIGNS TO AVOID RISKS

E-MAILS & TEXTS

HOW TO SPOT A PHISH OR SMISH

"**SMISHING** " is the text message version of a phishing email and can contain links to things like:

- MALICIOUS WEBSITES
- EMAIL ADDRESSES
- PHONE NUMBERS

that may automatically open a browser window or email message, download malware, or dial a number.

Spelling and Layout

Poor grammar and sentence structure, misspellings, using emojis, and inconsistent formatting are other indicators of possible phishing attempts.

Generic Greetings and Signature Blocks

"Dear Valued Customer" or "Sir/Madam" - and a lack of contact information are strong indicators of a phishing email.

Generic or Suspicious Sender Addresses

Cybercriminals imitate legitimate business email addresses by changing or removing a few letters.

NEVER reply to a suspected phishing email.

Suspicious Attachments

An unexpected email asking you to download/open an attachment is the most common way to become a victim of ransomware and other malware.

NEVER open attachments from an unknown sender or an email you are not expecting.

Spoofed hyperlinks and websites

ALWAYS hover your cursor over links in the body of the email and email addresses - the destination link may not match what it appears to be in the email
(e.g., .com vs. .org)
URLs (website address) can be shortened and hide the true destination of the link (e.g., bit.lyandtinyurl)

Sign up for *The Advisor* - TMC's monthly compliance newsletter and receive **Security Scout** monthly security awareness reminders!

TOTAL MEDICAL COMPLIANCE

www.totalmedicalcompliance.com
(888) 862-6742
service@totalmedicalcompliance.com