Online safety tips

Cybercriminals find information about who you trust and impersonate them when they contact you. Their goal is to solicit personally identifiable information (PII) from you when you select links in an email, answer the phone, or simply reply to a message. They then use your PII to commit more harmful crimes, or they sell your information to someone else. These attacks often reach you by email ("phishing"), phone call ("vishing"), or text ("smishing"). Typical phishing, vishing, and smishing messages often appear urgent and may even threaten or pressure you to take action. If you receive an offer that seems too good to be true, it probably is.

Think before you click

When you receive an email, hover over any links to reveal the URL and make sure the web address looks legitimate before you select the link. Look for other ways you can verify the sender and content, such as by the sender's email address and content that includes proper spelling and grammar. If you don't think an email is legitimate, then don't select any links.

For more online safety tips and information about protecting your TSP account, visit tsp.gov/security.