## T2025_01 Smishing: Text Messaging Scams - What You Need to Know (11th February 2025)

Smishing, a type of phishing attack delivered via text messages, tricks individuals into revealing personal or financial information or downloading malicious software. Scammers often use spoofed numbers to impersonate trusted sources like banks or delivery services and create a sense of urgency to prompt immediate action. They may send shortened links to conceal malicious websites or request sensitive details such as Social Security numbers or bank account information. To protect yourself, be cautious of unexpected texts, avoid clicking on suspicious links, verify any requests for personal data through official channels, use strong passwords with two-factor authentication, and report suspicious messages to your mobile carrier or the Federal Trade Commission (FTC). Staying vigilant can help safeguard your personal information from smishing scams.

## References

- Tip of the week. (n.d.). Retrieved from UTHSC. https://uthsc.edu/its/cybersecurity/tip-of-the-week.php