PROTECT YOURSELF FROM TEXT MESSAGE SCAMS

Think before you click.

Scammers are constantly evolving their tactics, using fake text messages to trick people into revealing sensitive information. Learning how to identify fraudulent texts can help protect your personal and financial information.

How Text Message Scams Work

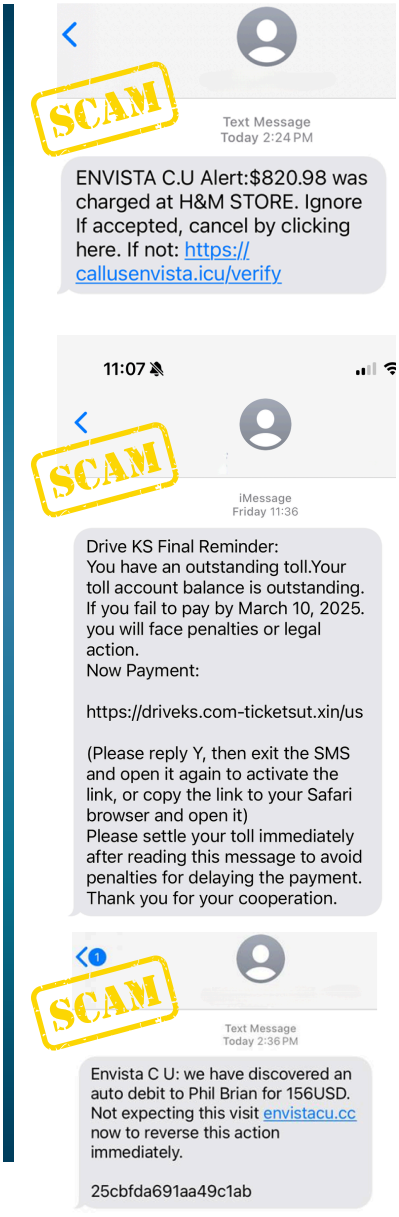
Scammers disguise harmful links in text messages to appear legitimate. Their fake texts often claim to be from your bank, a shipping service or a government agency, urging you to take immediate action. Clicking on these links may install malware on your device or lead to phishing sites designed to steal login credentials.

Key Warning Signs of Malicious Texts

Check the Domain: Does the end of the URL match the official source? Banks and legitimate companies use official domains like .com, .gov, or .org—not random letters or numbers.

Be Cautious of Shortened URLs: Scammers often use services like TinyURL or Bitly to hide fraudulent links. Avoid clicking if you can't see the full web address.

Hover to Reveal Hidden Links: Some scammers embed dangerous URLs behind legitimate-looking text. If possible, hover over links on your desktop to reveal the source.



HOW TO STAY SAFE

Do not click on links in unexpected texts. If you receive a text claiming to be from your bank or a business, visit their official website directly.

Verify with the source. If in doubt, call the organization using the phone number on their official website - not the one in the text.

Enable two-factor authentication (2FA). This adds an extra layer of protection to your accounts.

Scammers rely on urgency to trick you into acting without thinking. Stay vigilant and protect your personal information by always inspecting URLs carefully. Pause. Evaluate. And, when in doubt, reach out.

Envista

ENVISTAFRAUDDEFENSE.COM