DNC Registry and SCA. Under the Do Not Call Registry and the Spam Control Act you receive protection from marketing messages across phone calls, SMS, email, and instant messaging. The statement that these laws reduce telemarketing calls only is false.

Stopping messages after registration. Upon registering your phone number on the Do Not Call Registry, businesses have up to 21 days to stop sending marketing messages. The statement is true.

Knowing if a business has data protection practices. Businesses must make available their data protection policies, and you can also look for the Data Protection Trustmark logo. The statement that you will not know if a business has practices to safeguard your personal data is false.

Messages allowed after DNC registration. Businesses may send non marketing messages such as service or reminder messages unless you consent to marketing messages. The statement that businesses must stop sending any message is false.

Whether consent is always required. If you willingly provide your personal data for a purpose, you may allow its use where needed for the transaction. The statement that businesses must seek consent at all times is false.

Requesting an organisation to stop using personal data. You can opt out at any time by sending a request. Personal data may still be retained for business or legal needs. The statement is true.

Knowing if personal data has been leaked. Businesses must inform you when a data breach that puts you at risk occurs. The statement that you will not know if your personal data has been leaked is false.

Loan or gambling messages. SMS or calls about loans or online gambling from unknown senders relate to criminal offences and should be reported to the police. The statement is true.

Knowing why businesses want your personal data. You should know the purpose of collection to decide if it is reasonable. The statement that you do not have to know why businesses want your personal data is false.

Requesting changes to inaccurate personal data. You may access data held about you and request corrections if it is inaccurate. You may also check past year usage or disclosure. The statement is true.

Withdrawing consent. Before withdrawing consent for the use of your personal data, you should understand the consequences. The statement is true.

Sharing personal data without informing individuals. Businesses gen-

erally need consent to collect, use, or disclose your personal data. They may share it with partners when necessary for provided services. The statement that businesses can share your personal data with any other business without informing you is false.

What is considered personal data. Personal data includes any data that identifies you, even when combined with other data. Personal data is therefore data that identifies you.

Considerations when downloading apps or games. You should consider what personal data is being collected, why the requested personal data is being collected, and how the requested personal data may be used. All of the above must be considered.

Legitimate purposes for using personal data. Personal data may be used for research and development purposes, to improve or develop new products and services based on customer preferences, and for legitimate reasons such as the prevention or detection of fraud or ensuring security. All of the above are legitimate purposes.

Withdrawal of consent details. Withdrawal of consent for marketing messages via a channel applies only to that channel unless you specify otherwise. You may need to give notice, and your personal data may not be deleted and can be retained for business or legal needs. All of the above statements are relevant.

Tell tale signs of phishing emails. A request for your personal or sensitive information for no legitimate reasons is a tell tale sign of phishing. Phishing attempts may also include misspellings, threats, rewards, mismatched URLs, or suspicious attachments.

Reducing nuisance calls or messages. The ScamShield app blocks known scam callers and filters SMS from unknown senders. It can reduce nuisance calls or messages. ScamShield is therefore the correct method.

Stopping unsolicited telemarketing messages. To stop receiving unsolicited telemarketing messages and calls, you should register with the Do Not Call Registry. Registration is free.

Handling loan or gambling messages. If you receive SMS or calls about loans or online gambling from unknown sources, you should notify the police. Do not reply or interact.

Characteristics of strong passwords. Strong passwords should have a minimum of eight characters, include at least one alphabetical character, one numeric character, and one special character, and contain a mix of capital and small letters. All of the above describe strong passwords.

How websites collect personal data. Websites typically use cookies to collect personal data such as usage profiles. Websites must provide clear information about collected data and seek consent when required.