Banking & Payments Federation Ireland

core™ Research

The FraudSMART Social Engineering Survey

A measurement of the incidence and citizens response to scams.

t: +353 1 649 6433 1 WML, Dublin 2, D02 F206 https://onecore.ie/research/

The Central Mission

core™ Research

To measure the frequency of suspicious communications and explore the actions taken when people encounter suspicious content / scams.

National Survey

Who we Spoke to

Fieldwork dates:

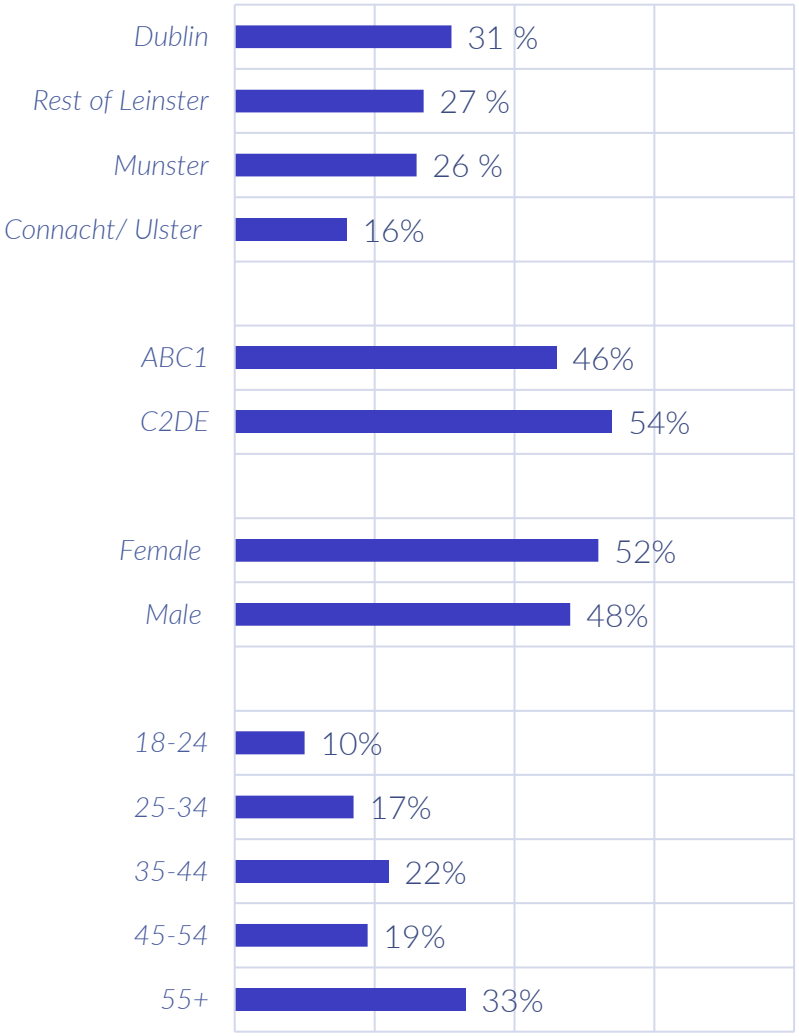
8th January – 17th January

Sample size:

An online survey of 1,000 adults 18+ in the Republic of Ireland.

Nationally representative of the population based on age, gender, region, and social class.

The sample has a margin of error of +/- 3% at a 95% confidence level.



The Executive Summary

core™ Research

Encountering suspicious activity is on the rise

Reflecting on the past year, 45% of people state that they have experienced more suspicious activity compared to this time last year.

This underscores the urgent need to bridge the gap in security measures and enhance public awareness of how to effectively protect against scams and suspicious activity.

Over 3 in 4 adults in Ireland encounter suspicious content or activity at least once a month.

Phone calls are the second most frequent channel for suspicious activity, with 3 in 4 adults receiving suspicious calls at least every six months, and 1 in 2 encountering them monthly.

Mobile phones are the primary channel for suspicious experiences. Text messages are the most common source, affecting a significant majority.

This highlights the pervasive nature of suspicious activity targeting mobile users in Ireland.

Blocking or ignoring are the most common responses to suspicious activity

….with 99% of people taking at least some action to protect themselves from scams. However, many are not consistently adopting protective measures.

While it's encouraging that a majority take proactive steps, the sizable portion of individuals not routinely protecting themselves is a cause for concern.

core™ Research

Frequency of suspicious communications

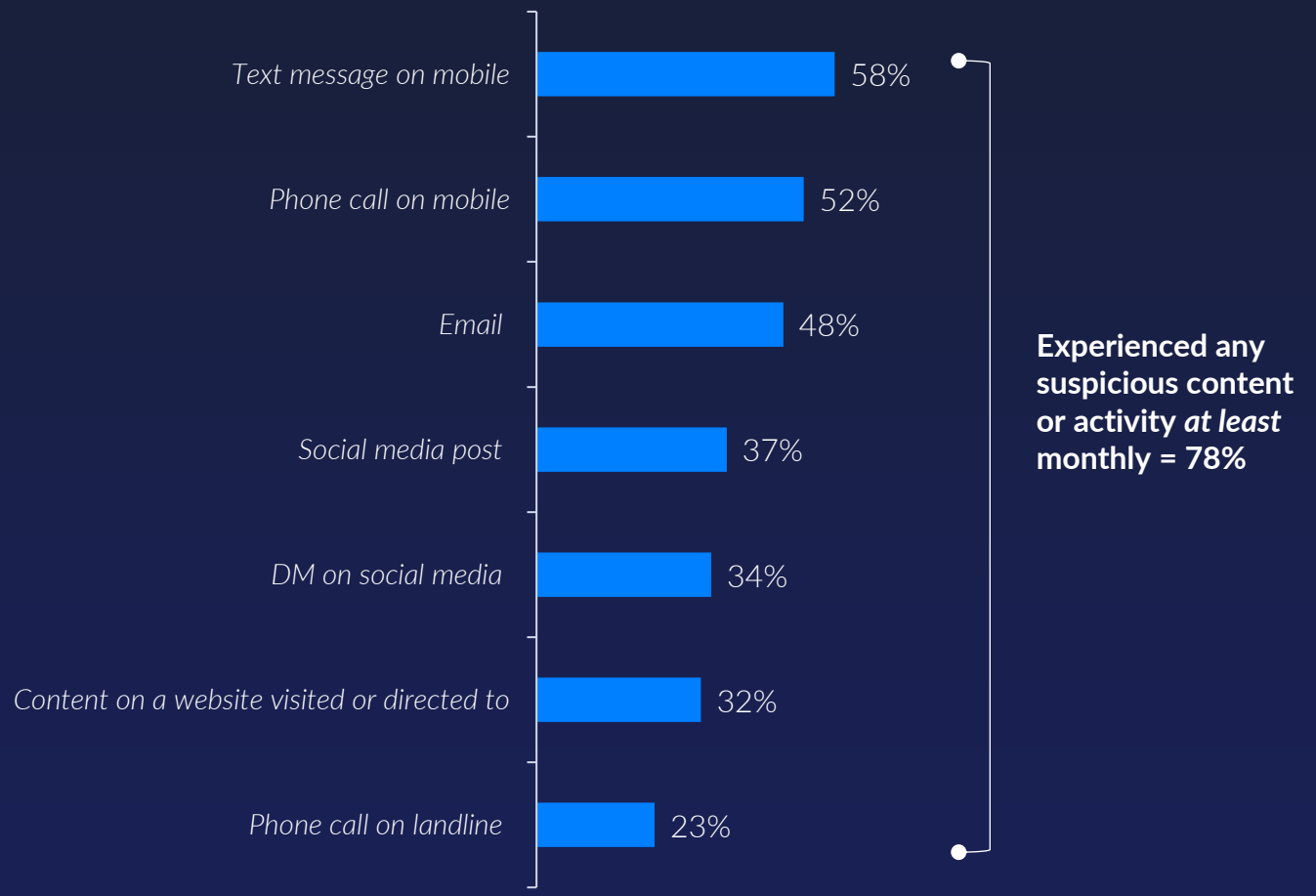
78% of adults have experience suspicious content or activity at least once a month.

core™ Research

3 in4 adults in Ireland have encountered some suspicious content or activity.

Text messages and calls on the mobile are the most prevalent channels for receiving suspicious content or activity.

Prevalence of suspicious communications at least once a month:

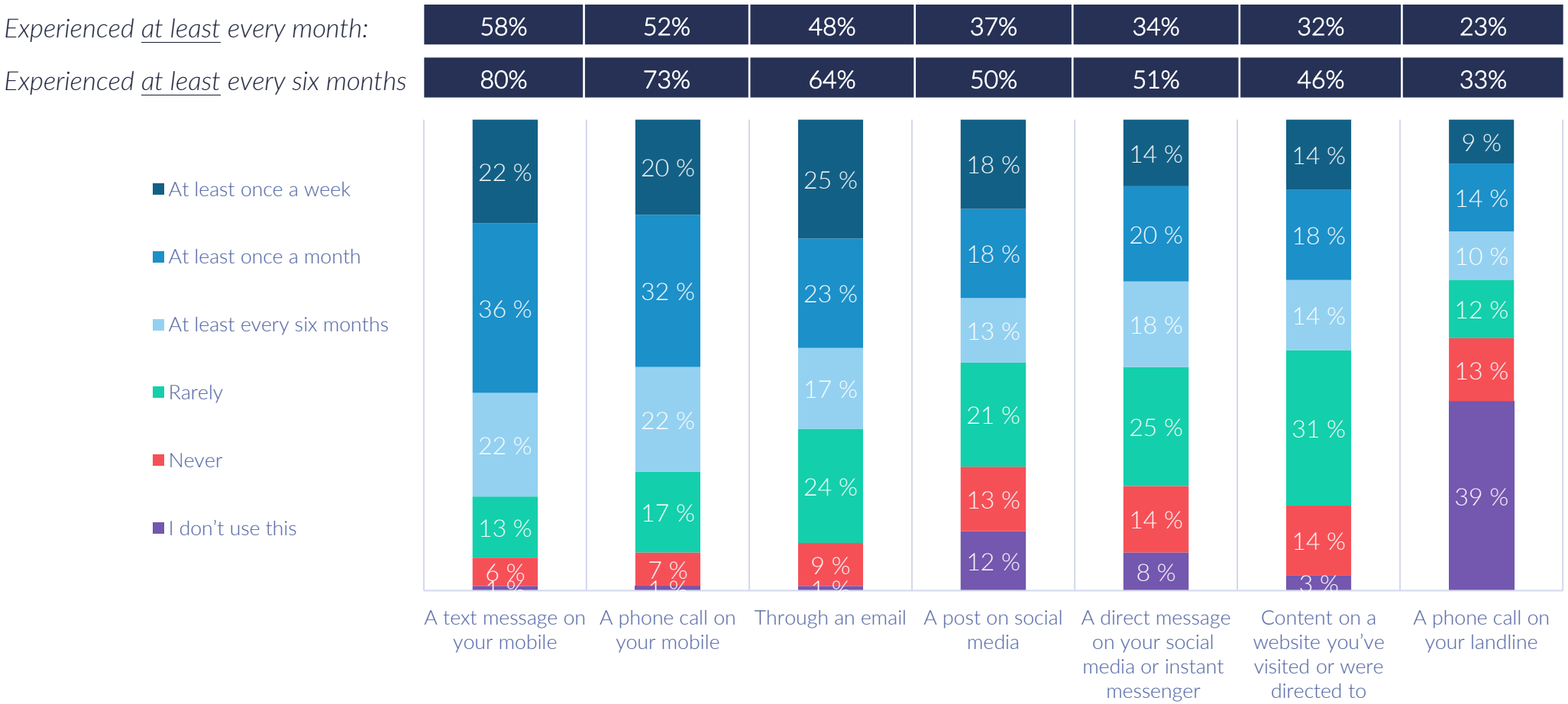


Q: How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000; Those who experienced any suspicious activity at least monthly: 782

A text message on the mobile is the most prevalent channel for receiving frequent suspicious activity, 6 in 10 say they experience this monthly.

core™ Research

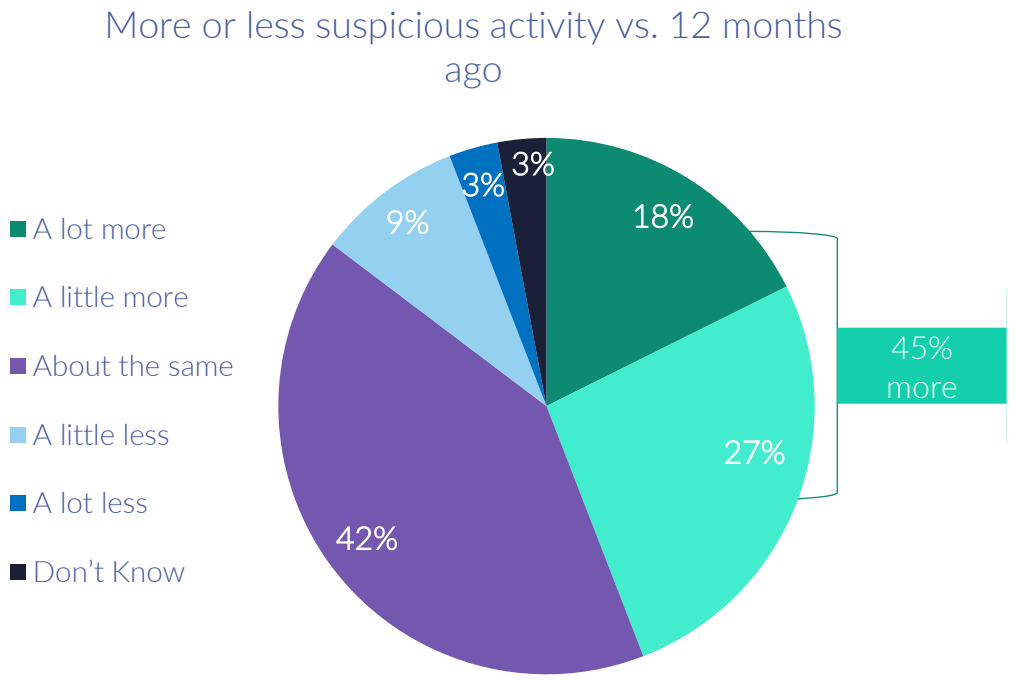
Suspicious Activity Frequency x Communication Methods



Q: How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000; Those who experienced any suspicious activity at least monthly: 782

Over two in five state they have encountered more suspicious activity compared to last year.

A further two in five say the level suspicious activity encountered is about the same.

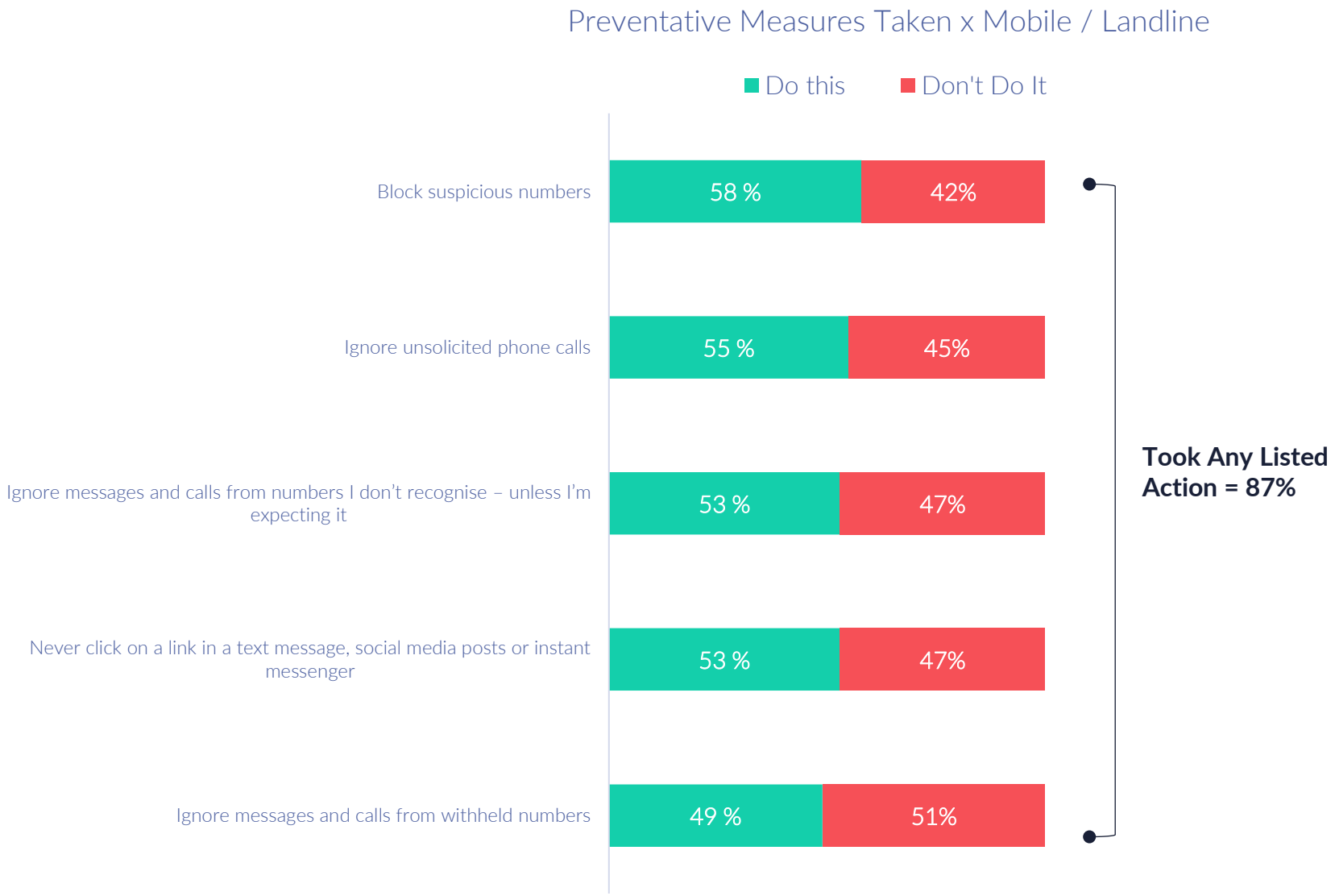


Q: Thinking back to this time last year, would you say you are encountering more, about the same or less amount of suspicious activity?
Base: 1000

Measures Taken To Protect From Scams

While 58% block suspicious numbers, 42% do not actively do this.

Around half do not ignore messages from calls and numbers they do not recognise. Over half do not ignore messages and calls from withheld numbers.

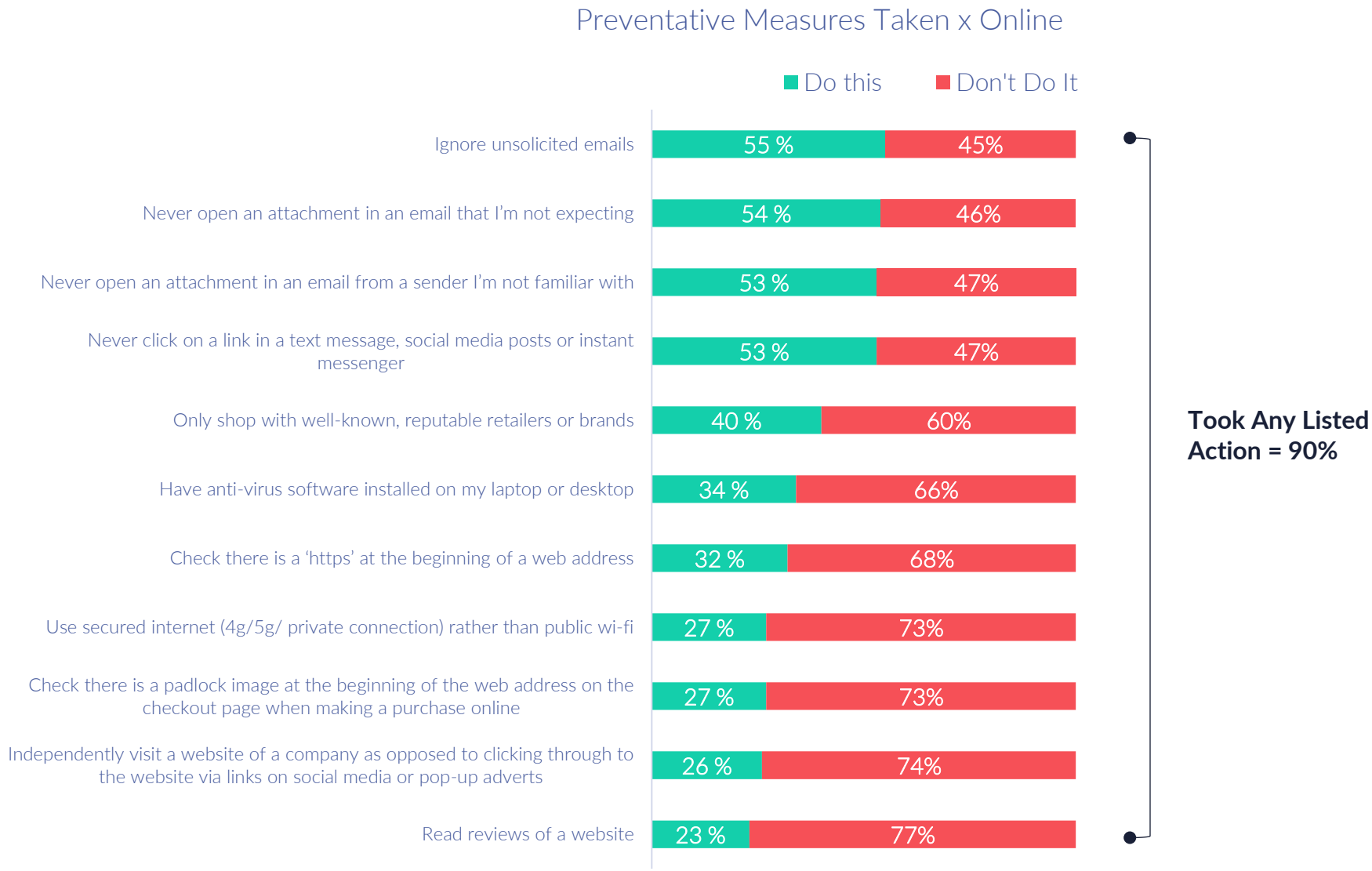


Q: What security measures do you take to protect yourself from scams?
Base: 1000

More than half ignore unsolicited emails and don't open unexpected attachments in emails, but on the flip side, just under half do not do this

round three quarters also do not:

- Read reviews of a website
- Independently visit a website rather than clicking links on social media or pop-up adverts
- Check there is a padlock image at the beginning of a web address
- Use secured internet



Q: What security measures do you take to protect yourself from scams?
Base: 1000

An Overview of the Actions and Suspicious Activity Indicators of the most common channels used by scammers.

core™ Research

	Text Message- Mobile	Phone call – Mobile	Email	DM – Social Media
PREVALENCE (AT LEAST ONCE A MONTH)	58%	**52%**	**48%**	**34%**
TOP 3 ACTIONS TAKEN (BY THOSE WHO RECEIVE AT LEAST ONCE A MONTH)	1. Ignored / deleted it (70%)	1. Blocked the number (67%)	1. Ignored / deleted it (69%)	1. Ignored / deleted it (60%)
	2. Blocked the number (59%)	2. Ignored / deleted it (58%)	2. Blocked the number (48%)	2. Blocked the number (53%)
	3. Checked company legitimacy (18%)	3. Checked company legitimacy (14%)	3. Checked company legitimacy (12%)	3. Checked company legitimacy (14%)
TOP 3 SIGNALS OF SUSPICIOUS ACTIVITY (BY THOSE WHO RECEIVE AT LEAST ONCE A MONTH)	1. Didn't recognise the number (51%)	1. Didn't recognise the number (54%)	1. Didn't recognise the sender (44%)	1. Didn't recognise the sender (39%)
	2. Not expecting a text (47%)	2. Not expecting a call (45%)	2. Poorly written content (42%)	2. Not expecting a DM (34%)
	3.Poorly written content (37%)	3. Heard/saw warnings about it (29%)	3. Not expecting an email (41%)	3.Poorly written content (34%)

Over the next few slides, we have broken out the experience and actions taken for each communication channel.

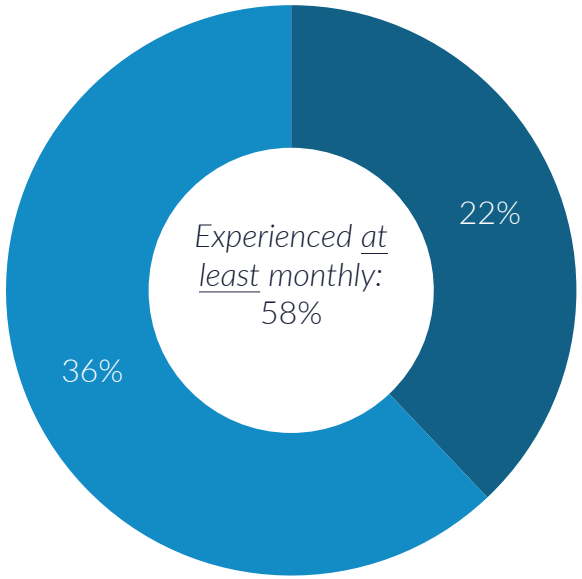
Text Message(s)

Actions Taken x Channel

Among those who have experienced suspicious activity via text message(s), over two thirds ignored or deleted the text message(s), while more than half blocked the number.

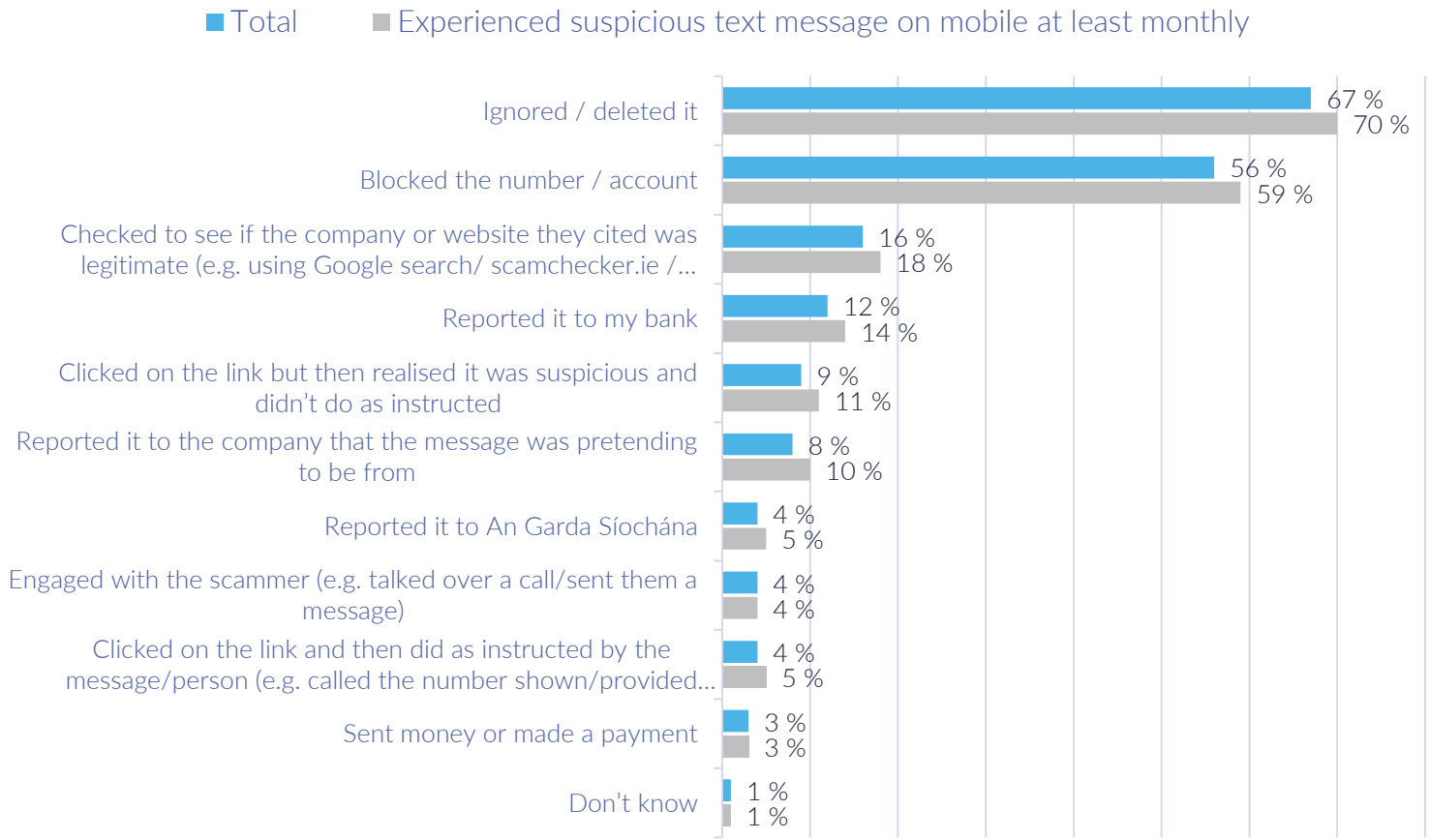
Text Message

Experienced suspicious activity via **text message on mobile** *at least* monthly



■ At least once a week ■ At least once a month

Actions Taken

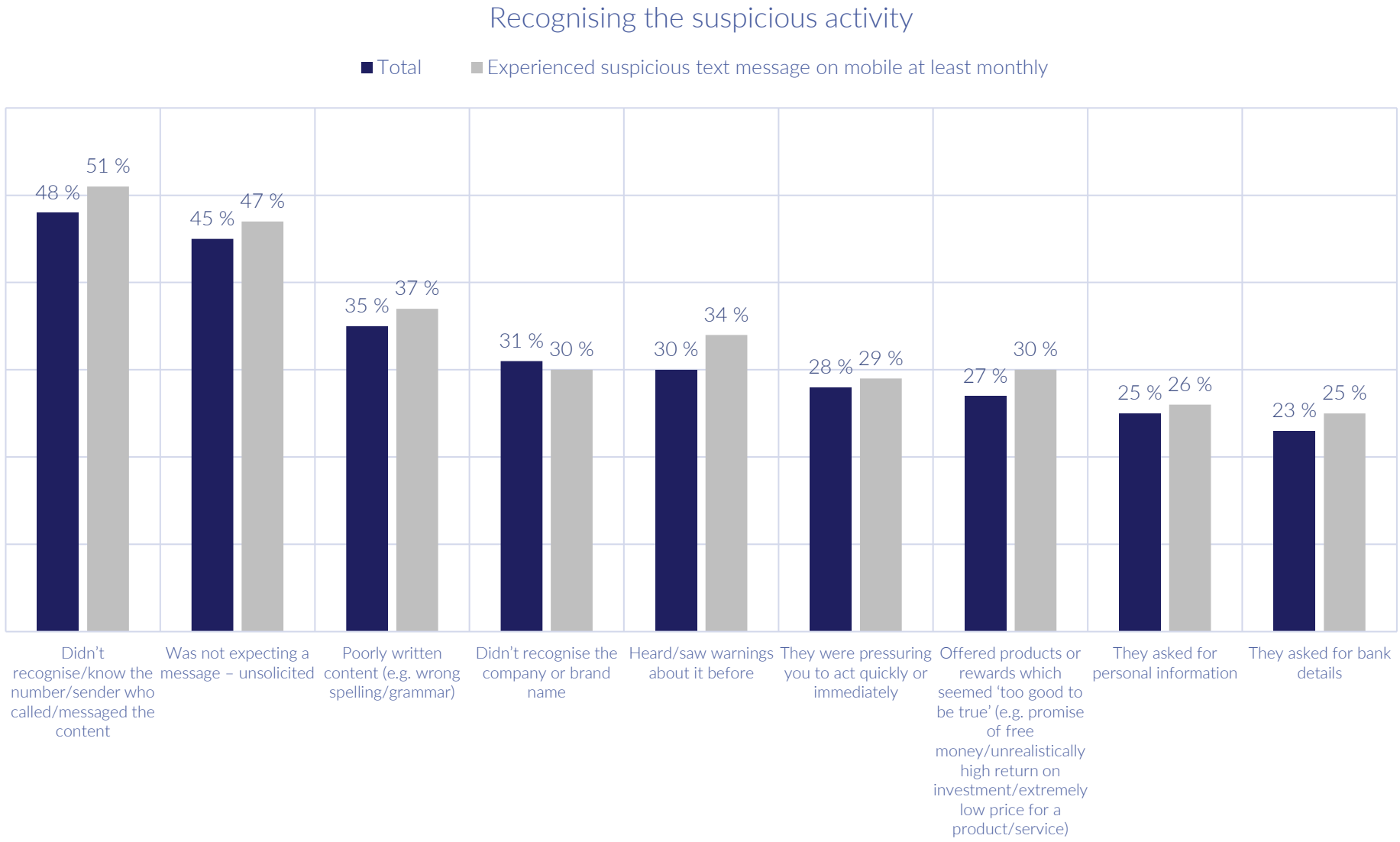


Q: How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000

Q: You mentioned that you've received suspicious content via a text message on your mobile, which if any of the following actions did you take?
Base: All those who have received a suspicious text message on mobile: 922; Those who received text message at least once a month: 580

For those who received a suspicious text message, the giveaway was not recognising the number, followed by them not expecting the message.

About half say that they recognised suspicious activity because they didn't know the sender and they were not expecting a text message.



Q: Still thinking about when you've received suspicious content via a text message on your mobile, which of the following reasons made you think it was suspicious?
Base: All those who have received a suspicious text message on mobile: 922; Those who received text message at least once a month: 580

core™ Research

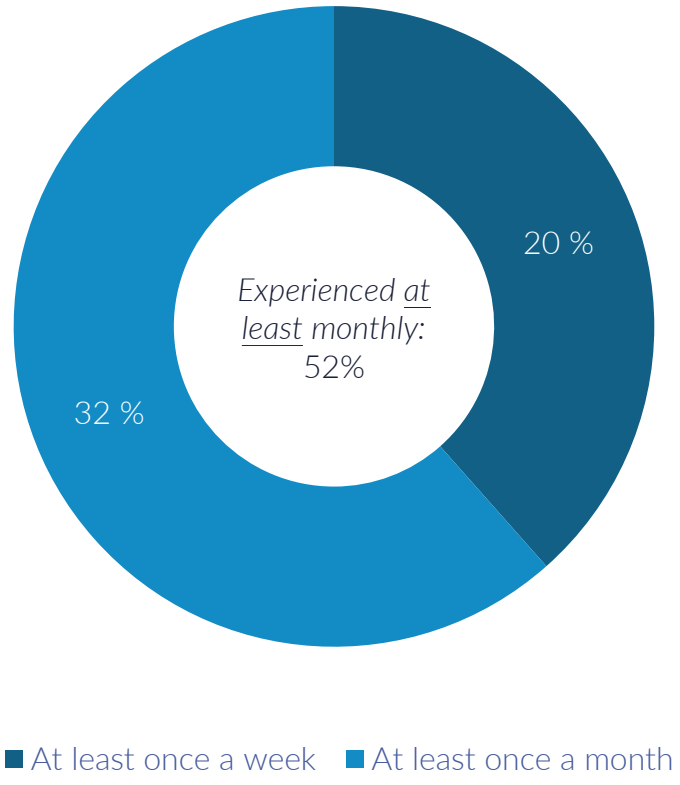
Mobile Phone Call

Actions Taken x Channel

Among those who have experienced suspicious activity via a phone call on the mobile, over six in ten blocked the number and a similar level ignored it.

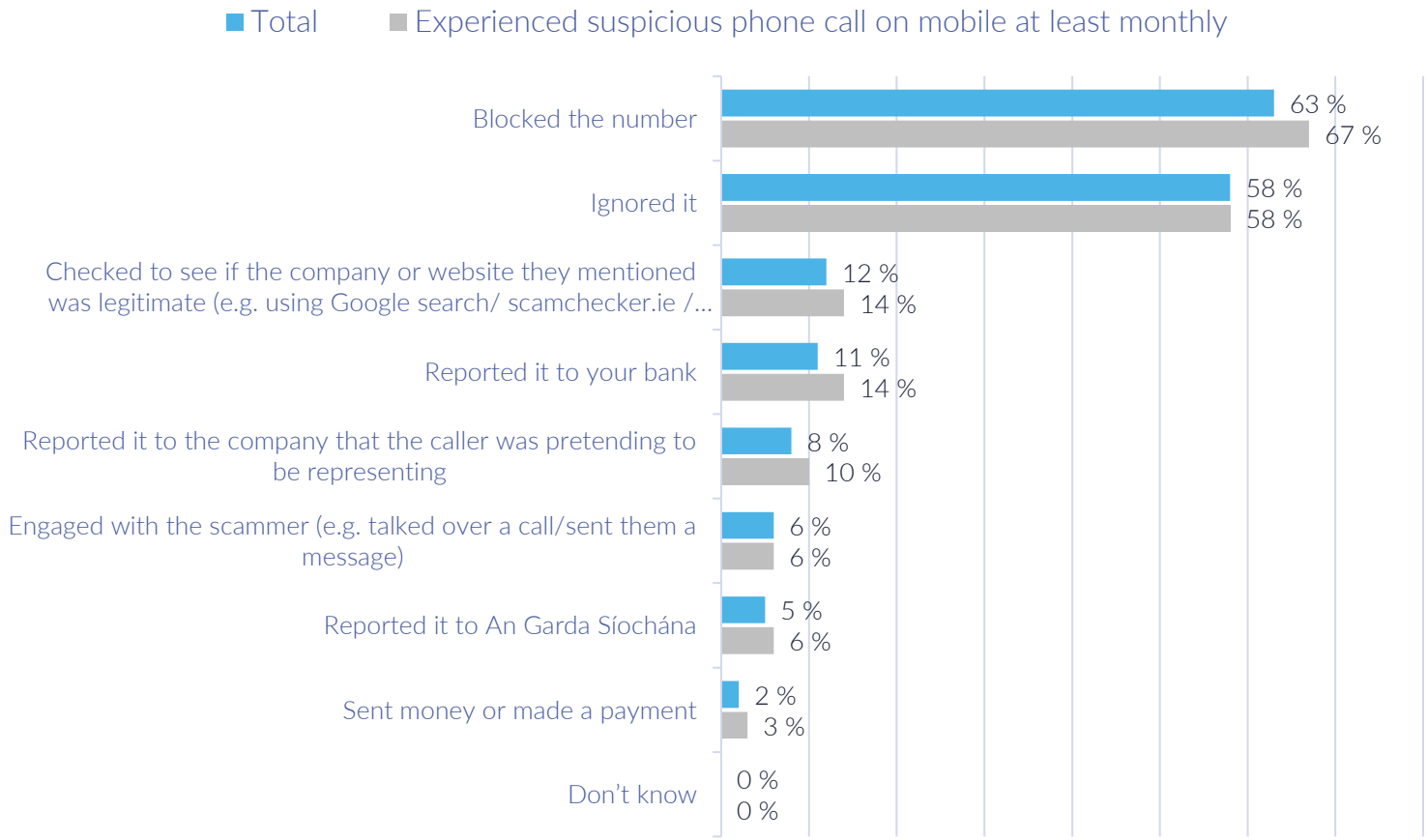
Phone Call on Mobile

Experienced suspicious activity via **phone call on mobile** *at least* monthly



How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000

Actions Taken

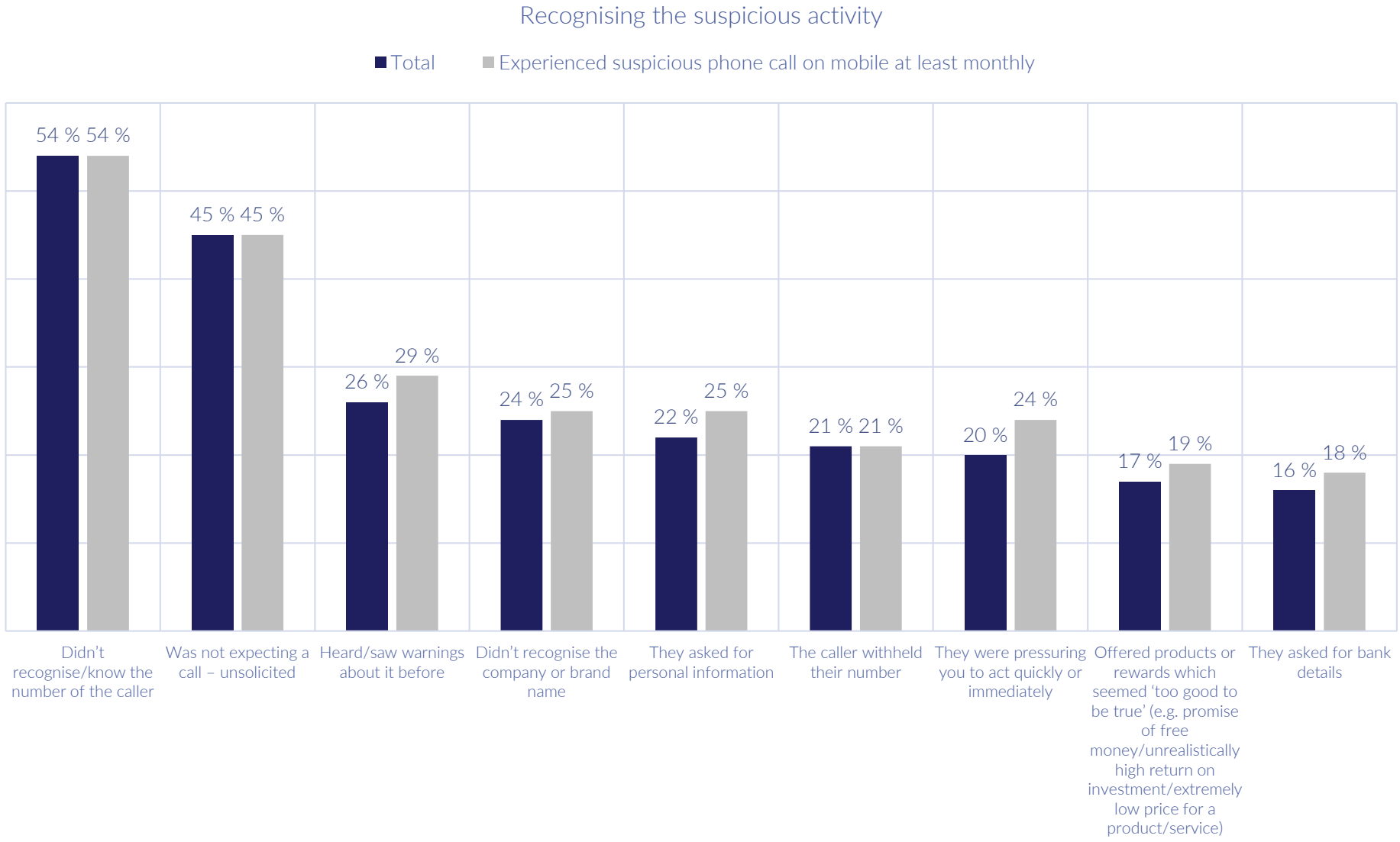


You mentioned that you've encountered suspicious activity via a phone call on your mobile, which if any of the following actions did you take?
Base: All those who have received a phone call on mobile: 907; Those who received phone call on mobile at least once a month: 518

Not recognising the phone number and not expecting the call are the most common ways to identify suspicious behaviour.

More than half say they recognise suspicious phone calls as they don't recognise the mobile number.

45% say they spotted it due them not expecting a phone call.



Still thinking about when you've received suspicious content via a text message on your mobile, which of the following reasons made you think it was suspicious? Base: 907; Those who received phone call on mobile at least once a month: 518

core™ Research

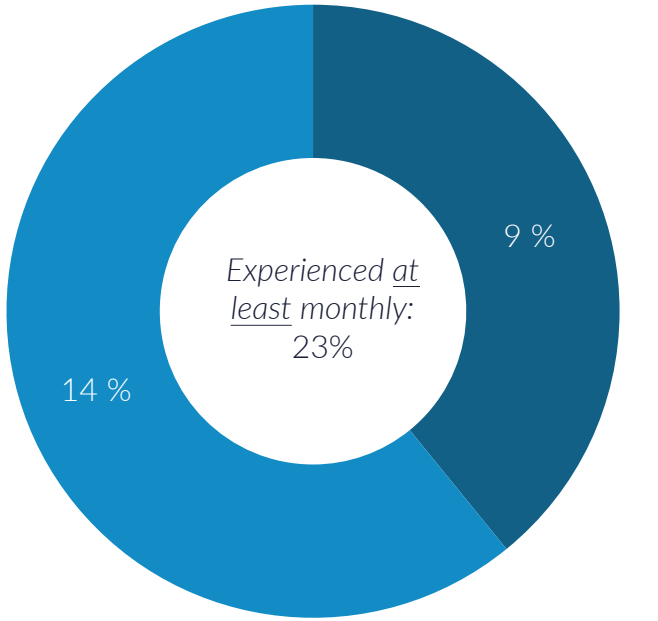
Landline Phone Call

Actions Taken x Channel

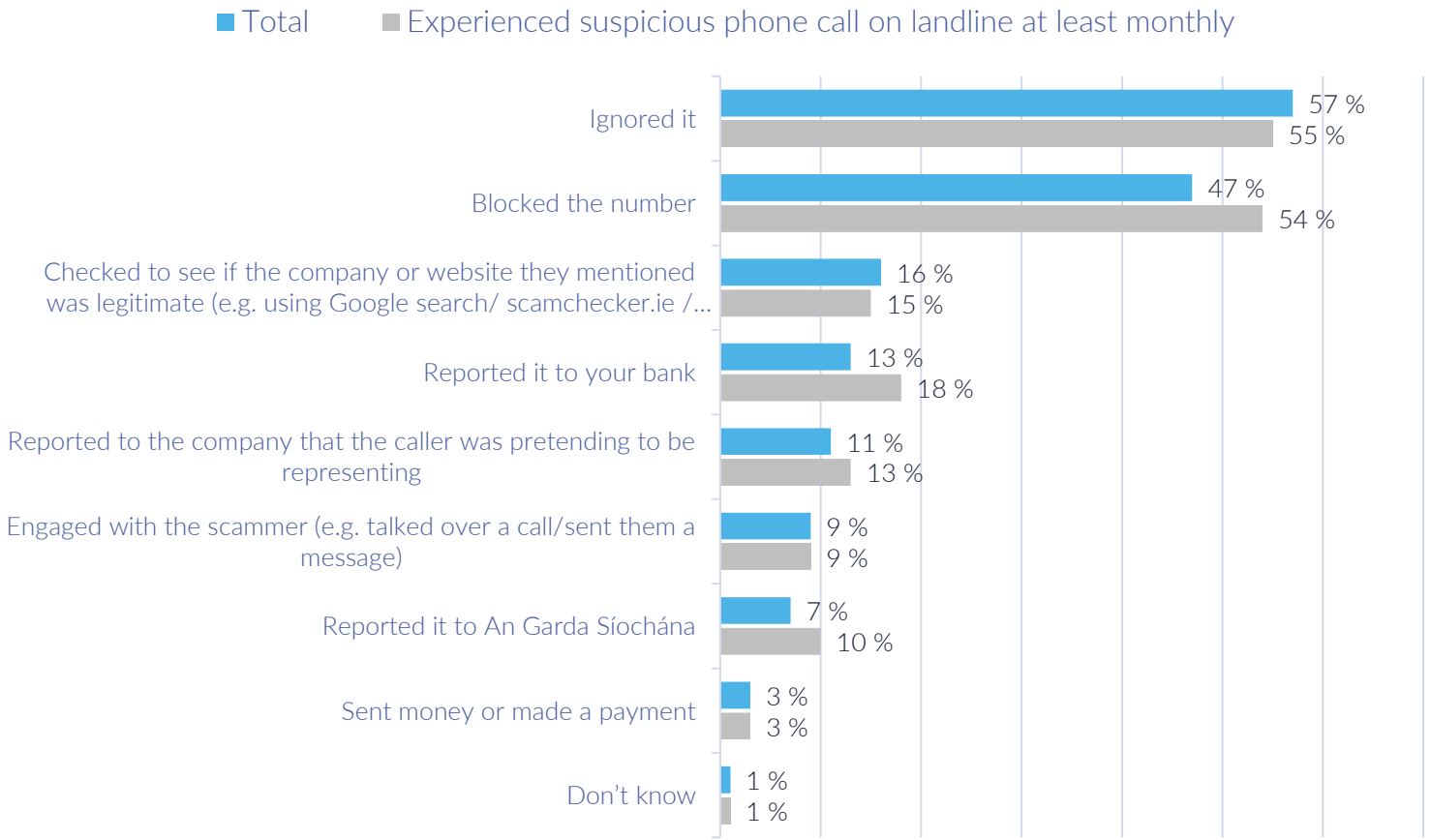
Among those who have experienced a suspicious phone call on the landline, over half ignored it and half blocked the number, a lesser extent than those who receive a suspicious mobile call. Those who receive a suspicious call *at least monthly* are more likely to block the number & report it to the bank.

Phone Call on Landline

Experienced suspicious activity via phone call on the landline *at least* monthly



Actions Taken

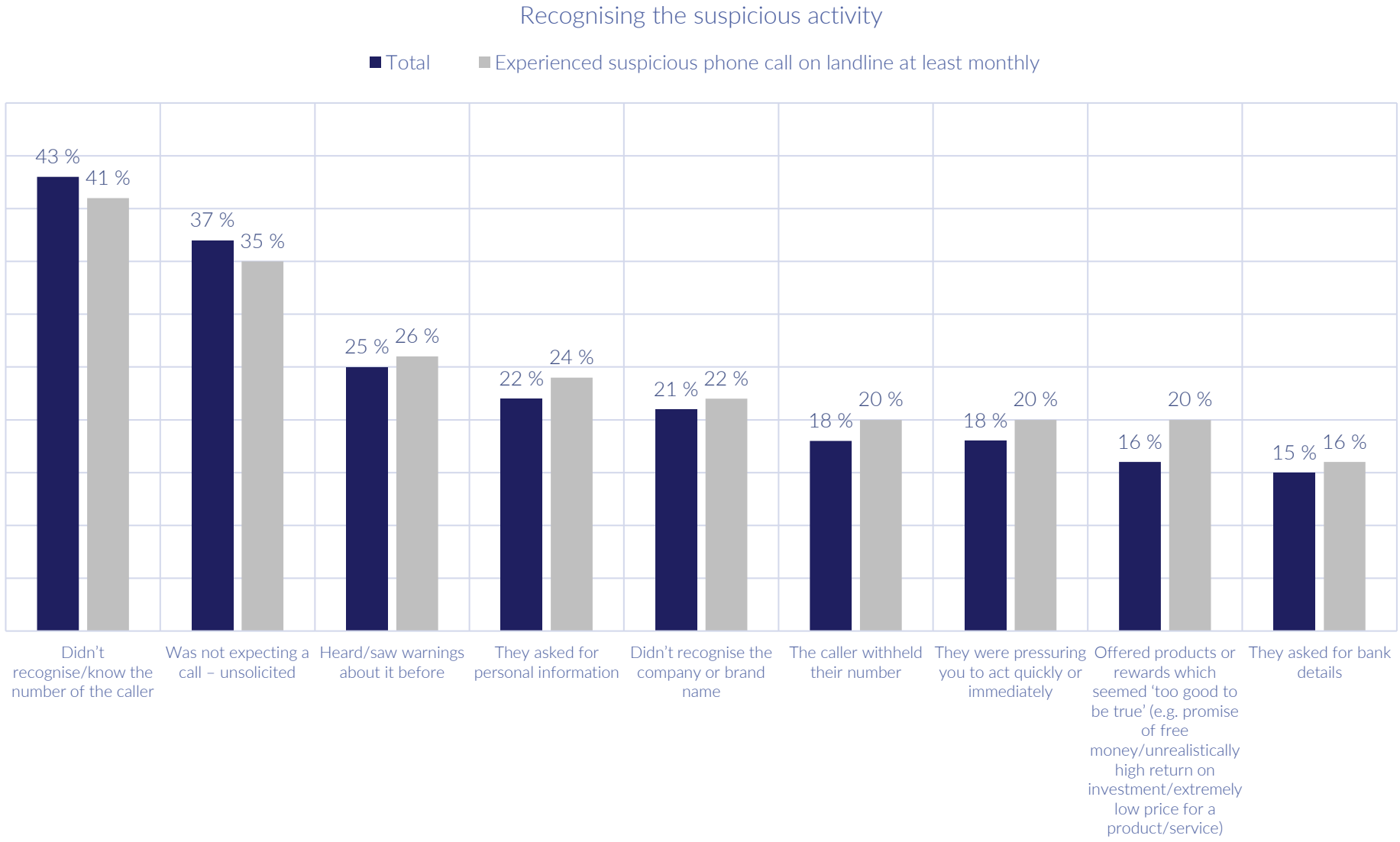


How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000

You mentioned that you've encountered suspicious activity via a phone call on your landline, which if any of the following actions did you take?
Base: All those who have received a phone call on landline: 457; All those who have received a phone call on landline: 231

To recognise the suspicious landline call, again, not knowing the number and the unsolicited call are the giveaways.

Again, this is a to lesser extent than a phone call on a mobile.



Still thinking about when you've received suspicious content via a text message on your mobile, which of the following reasons made you think it was suspicious? Base: 457; All those who have received a phone call on landline: 231

core™ Research

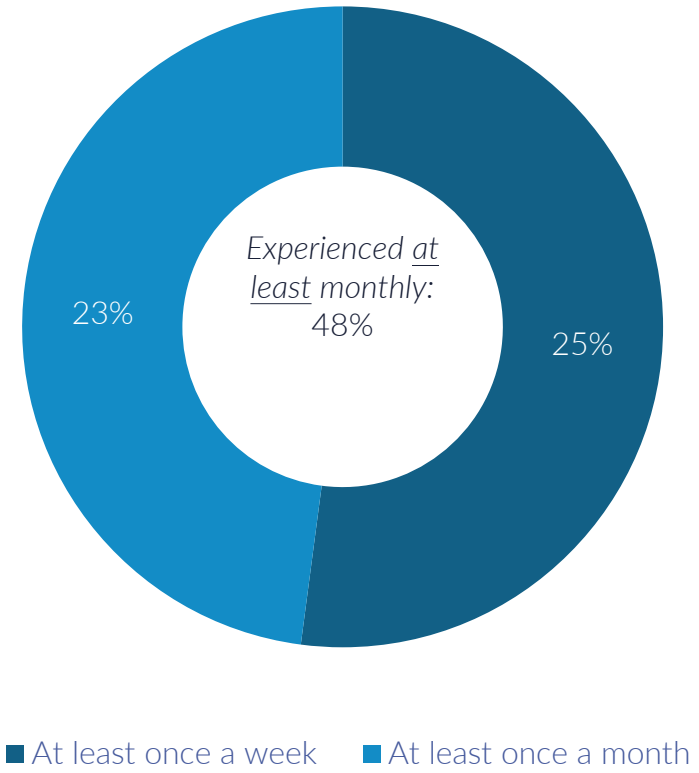
Email

Actions Taken x Channel

Among those who have experienced suspicious activity via email almost three quarters ignore or delete suspicious emails, while almost half blocked the email address.

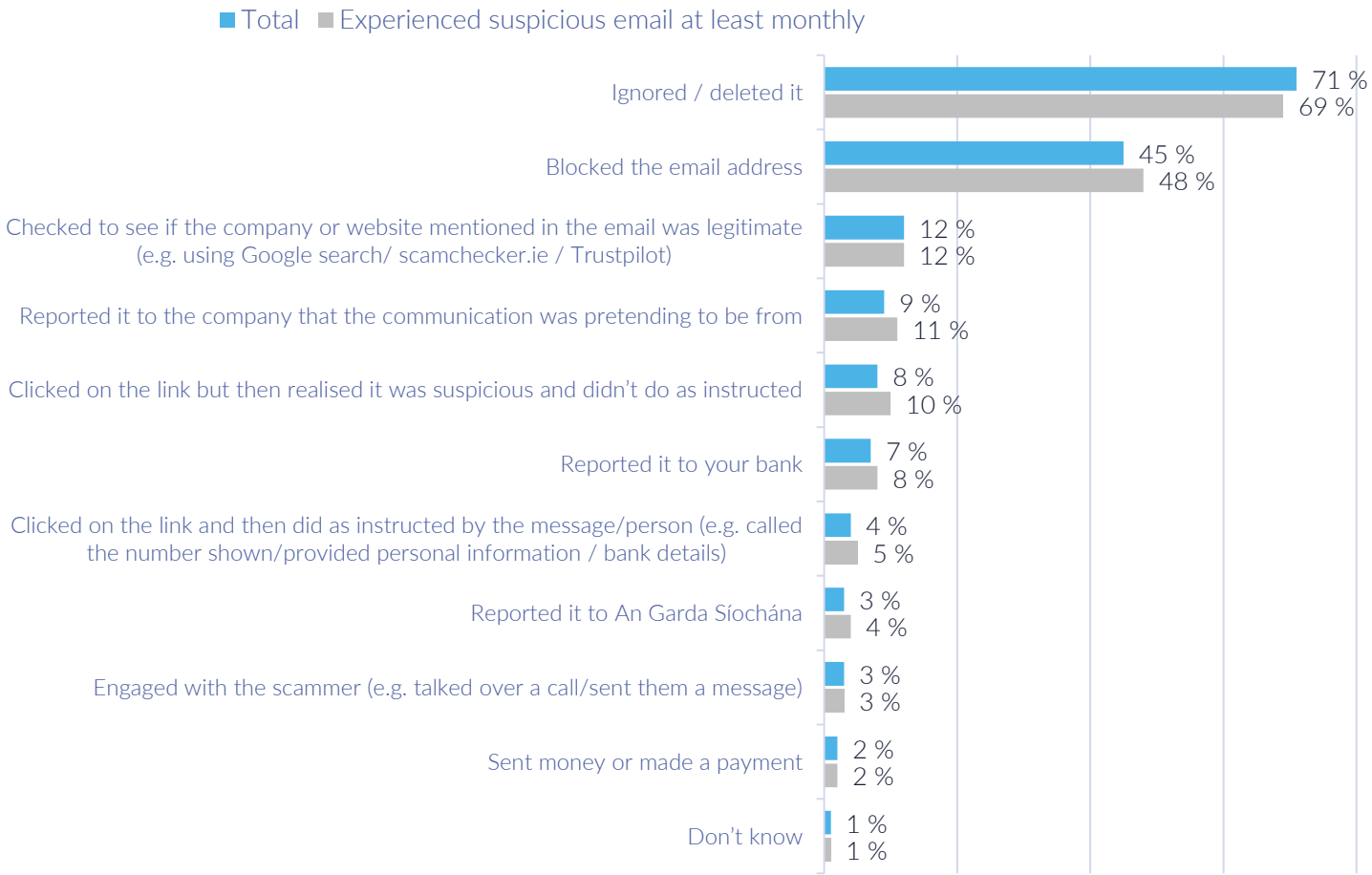
Email

Experienced suspicious activity via email *at least* monthly



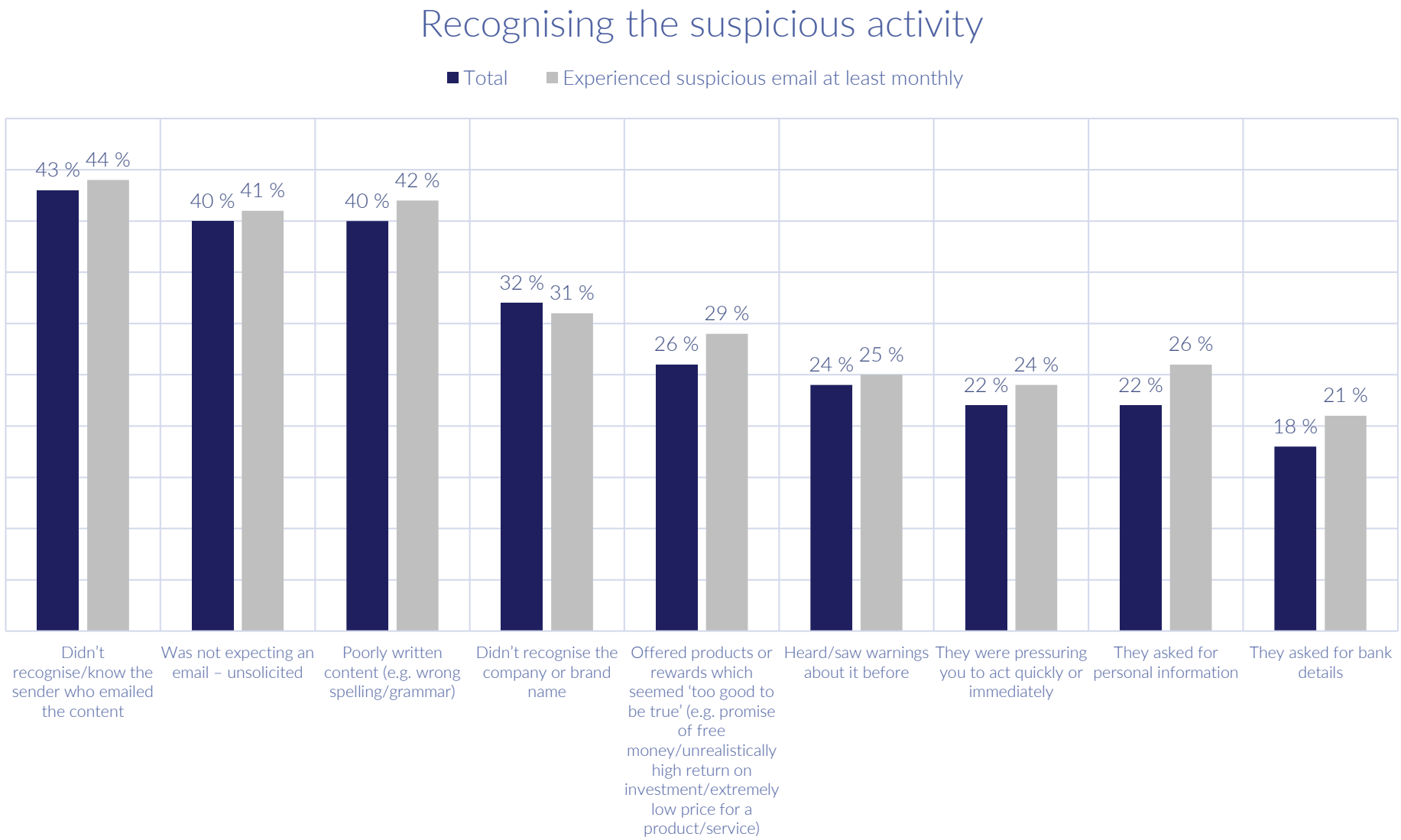
How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication?
Base: 1000

Actions Taken



You mentioned that you've received suspicious content via email, which if any of the following actions did you take?
Base: All those who have received a suspicious email: 879; All those who received an email at least once a month: 477

For those who received a suspicious email, the top three signals that it was suspicious were;
Not recognising the sender, followed by them not expecting the email or poorly written content.



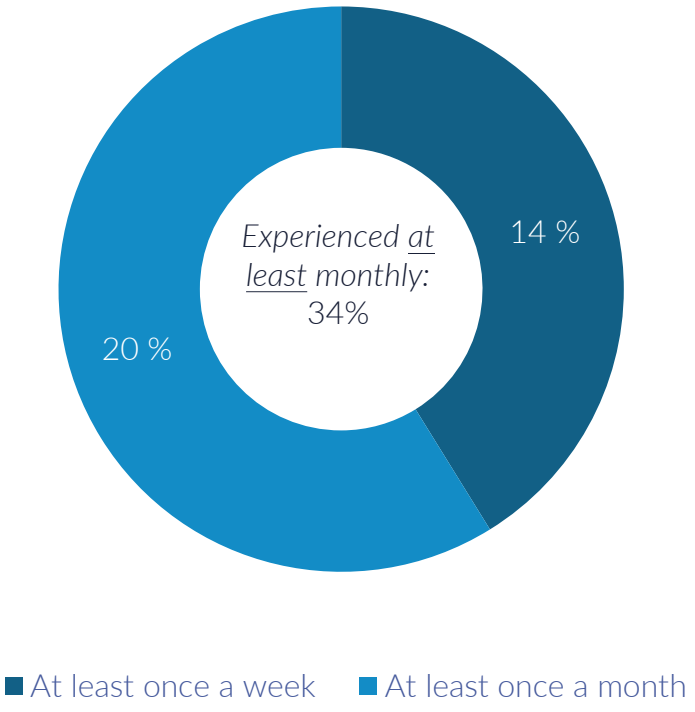
Still thinking about when you've received suspicious content via an email, which of the following reasons made you think it was suspicious?
Base: All those who have received a suspicious email: 879; All those who received an email at least once a month: 477

Direct Message
Actions Taken x Channel

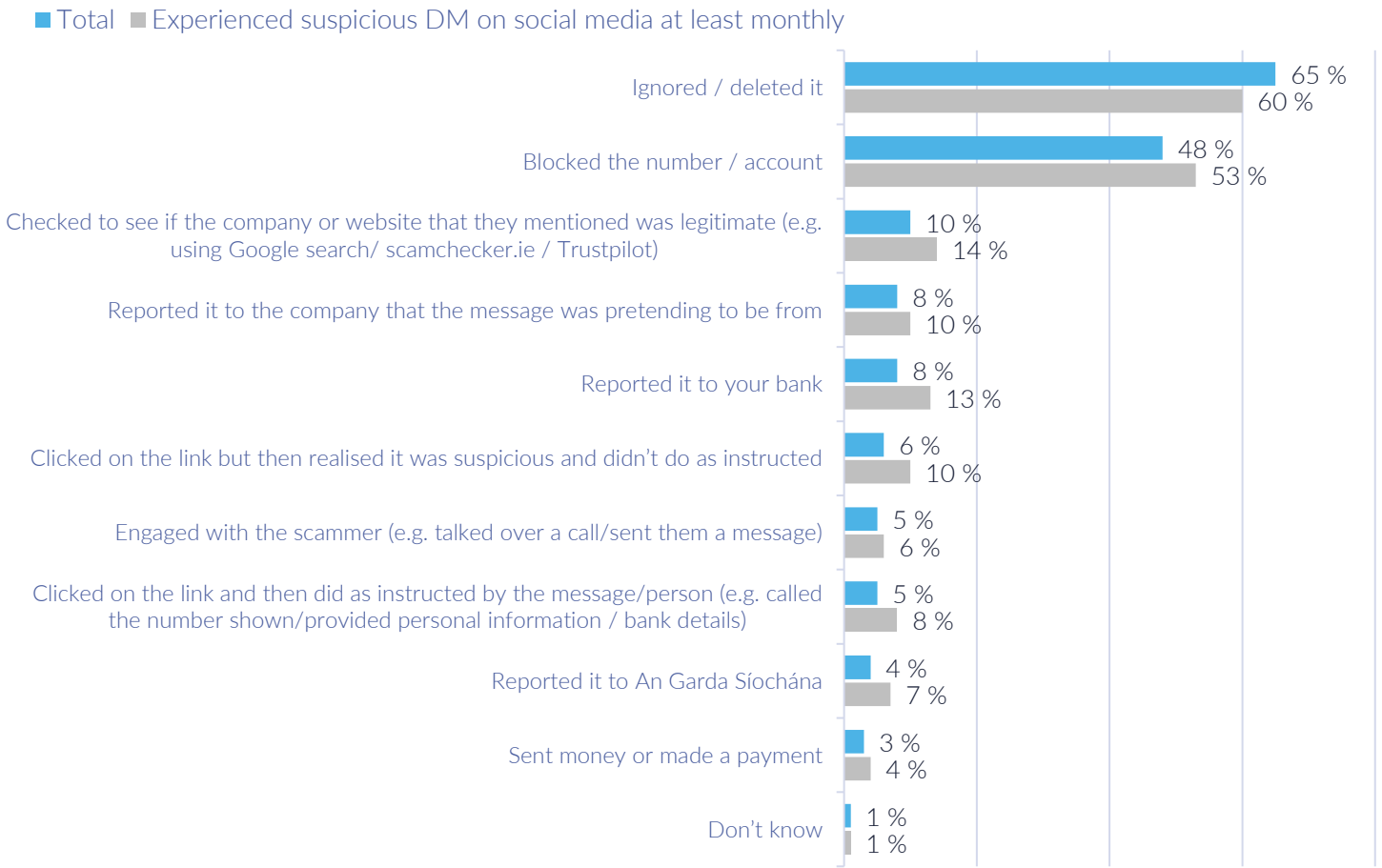
Among those who experienced suspicious activity via a direct message on social media, two thirds ignored or deleted it, while almost half blocked the account. Those who experience this *at least monthly* are less likely to ignore the message but more likely to block.

DM on social media

Experienced suspicious activity via a direct message on social media or instant messenger *at least* monthly



Actions Taken

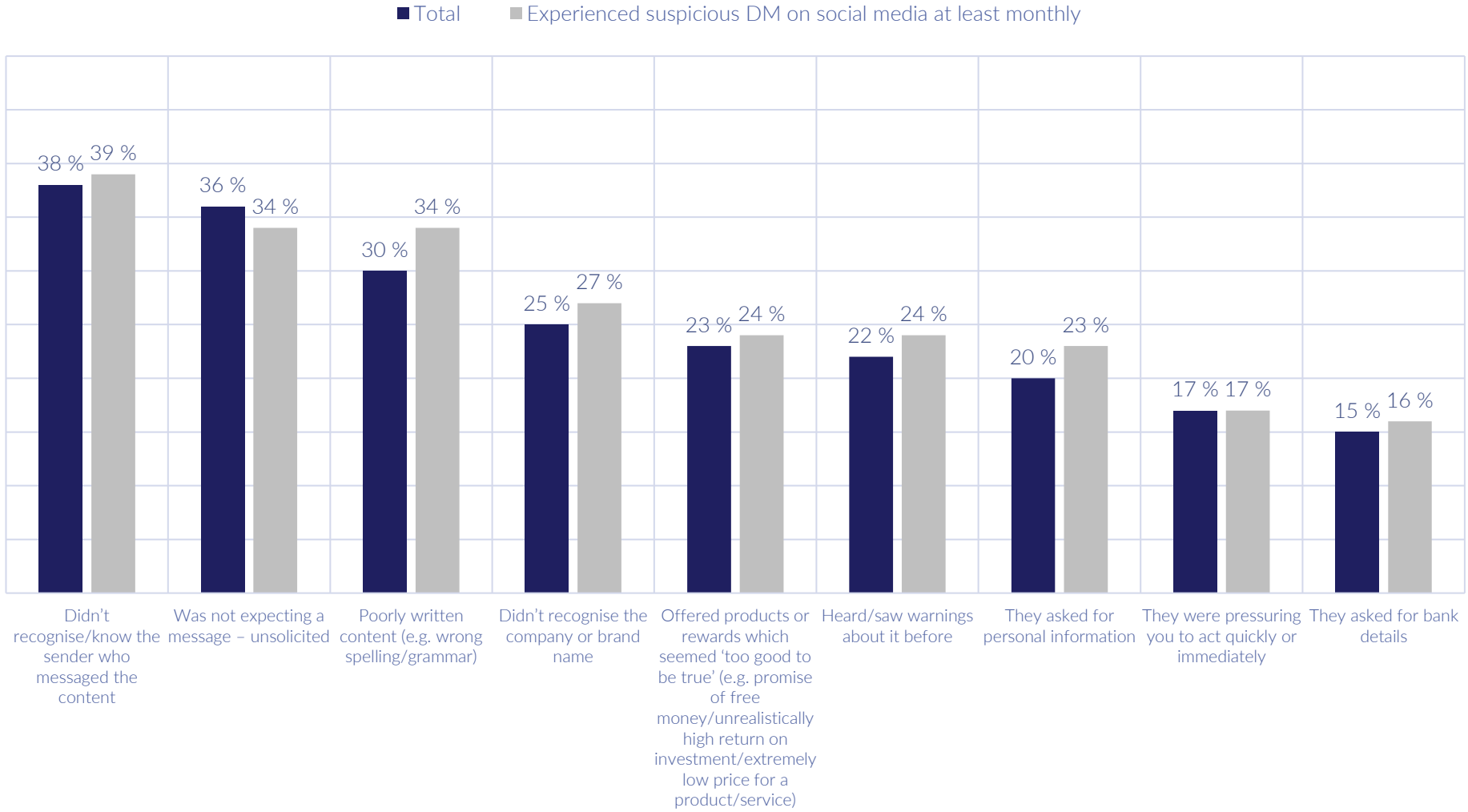


Q: How often, if ever, have you encountered suspicious content or activity via each of the following methods of communication? Base: 1000

Q: You mentioned that you've received suspicious content via a direct message on your social media or instant messenger, which if any of the following actions did you take? Base: All those who have received a suspicious direct message: 761; All those who received a DM on social media: 336

For those who received a suspicious DM, the top three signals that it was suspicious were; not recognising the sender, followed by them not expecting the message, or poorly written content.

Recognising the suspicious activity



Q: Still thinking about when you've received suspicious content via a direct message on your social media or instant messenger, which of the following reasons made you think it was suspicious? Base: All those who have received a suspicious direct message: 761; All those who received a DM on social media: 336

Banking & Payments Federation Ireland

core™ Research

The FraudSMART Social Engineering Survey

A measurement of the incidence and citizens response to scams.

t: +353 1 649 6433 1 WML, Dublin 2, D02 F206 https://onecore.ie/research/