Per•ceptive
[Research]

UNDERSTANDING CYBER SECURITY: PUBLIC PERCEPTIONS

EXECUTIVE SUMMARY

Methodology

- An online self-completion survey was sent out to the Perceptive Research Panel and completed by n=1161 people. The results were then weighted to Statistics New Zealand census gender, age and location data.

Overall Findings for the General Sample

Devices and the Internet

- Personal internet use peaks at 1-2 hours/day, but 21% are on for more than 4 hours/day.
- Almost all participants use the internet for emails, while 85% use it for social media and 82% for internet banking.
- Laptops and Smartphones are the primary devices to access the internet from.
- 58% share their devices with other people that want to access the internet. Their main concern is that a borrower might click on malicious links or access unsafe content. However, fewer than a third consider they might access social or other online membership sites.

EXECUTIVE SUMMARY

Passwords

- The vast range of sites accessed makes having a limited repertoire of passwords a necessity, and over half the sample use a relatively limited range of passwords across all their online activities.
- Propensity to change passwords is low, with two-thirds waiting to be prompted.
- Only 58% protect their own phone with locks or passwords, and 73% of those without protection on their phone also don't have tracking/blocking apps on the phone.
- Only half of those with a work smartphone have a password on it (52%), and even fewer have passwords on their work tablets (44%).

Cybersecurity

- While most people update their antivirus software and ensure they have adequate firewalls at least occasionally (82% and 68% respectively), 28% leave their devices lying around unlocked at least occasionally.
- Internet banking is considered the most secure of the online activities listed (82% rated it as secure), while nearly three quarters feel email is secure (73%).
- While two-thirds would check for a secure payment platform before making a transaction, half say they would also assess safety by the appearance of the site.

EXECUTIVE SUMMARY

Experiences of breaches

- 56% say they have received an email or request to connect from someone they don't know, while around a quarter have had someone send spam from their account or have clicked on a malicious link. Despite this, six out of ten have not changed their behaviour.
- This may be because those who have experienced a security breach in the past are less likely to feel they have control over preventing them in the future.
- Viruses and hacking resulting in changed passwords are perceived to be the most impactful security breaches. Of note is the perception that altered passwords are perceived to have a bigger effect than having passwords stolen.

Getting more information

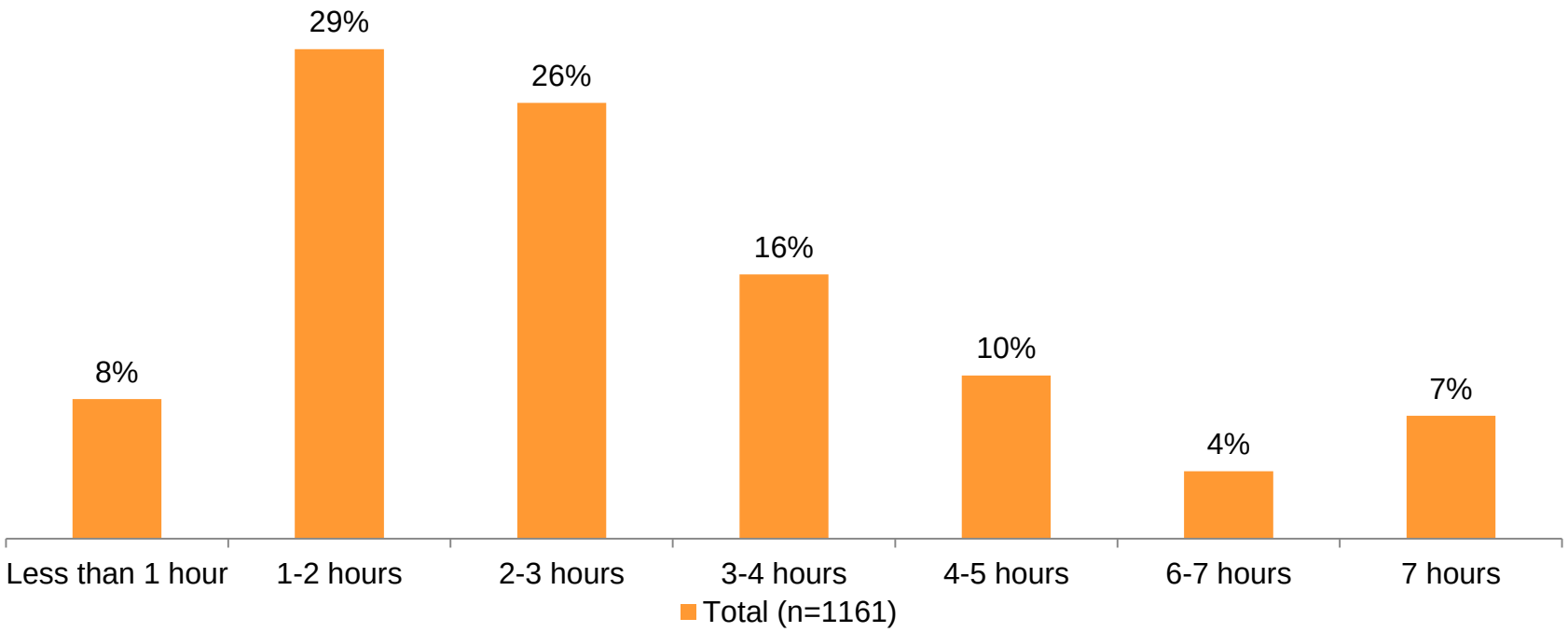
- Google is the main source of information about cyber security breaches. While 30% said they would contact a professional, a quarter said they would just fix the problem themselves. Nearly three quarters are unaware of any organisations that promote good computer hygiene.
- Nearly three quarters want proactive advice about prevention and identification of possible risk, while half also want information about who to contact if they get a virus

Per•ceptive
[Research]

DEVICES AND INTERNET

PERSONAL INTERNET USE PEAKS AT 1-2 HOURS/DAY, BUT 21% ARE ON FOR MORE THAN 4 HOURS/DAY

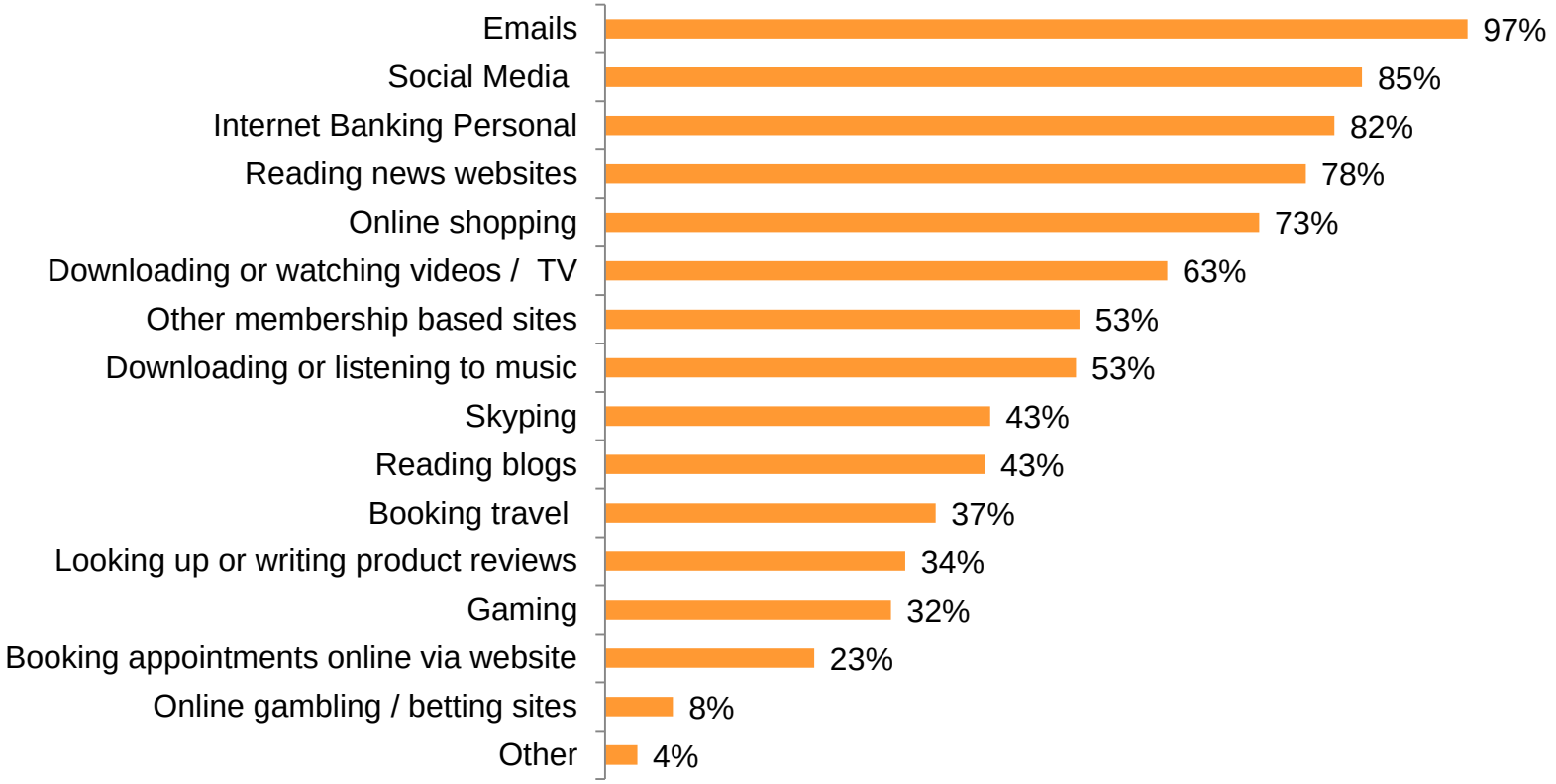
On average, how many hours a day would you spend on the internet for personal use (not including what you use for school/work)?



Base: all respondents

ALMOST ALL PARTICIPANTS USED THE INTERNET FOR EMAILS, WHILE 85% USED IT FOR SOCIAL MEDIA AND 82% FOR INTERNET BANKING.

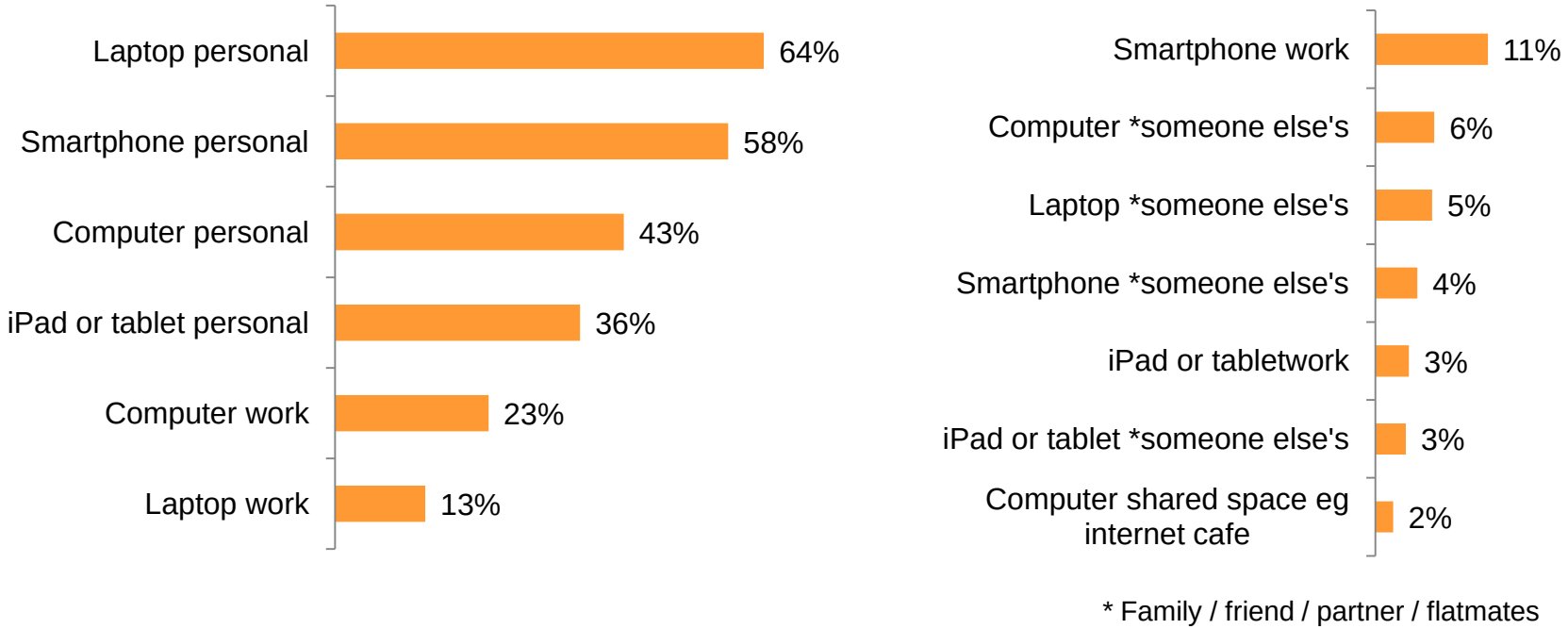
Out of the following uses, please select what you use/ or have used the internet for in the past 3 months (Select all that apply)?



Base: all respondents

LAPTOPS AND SMARTPHONES ARE THE PRIMARY DEVICES TO ACCESS THE INTERNET FROM

Which device(s) do you access the internet from for personal use (Select all that apply)?

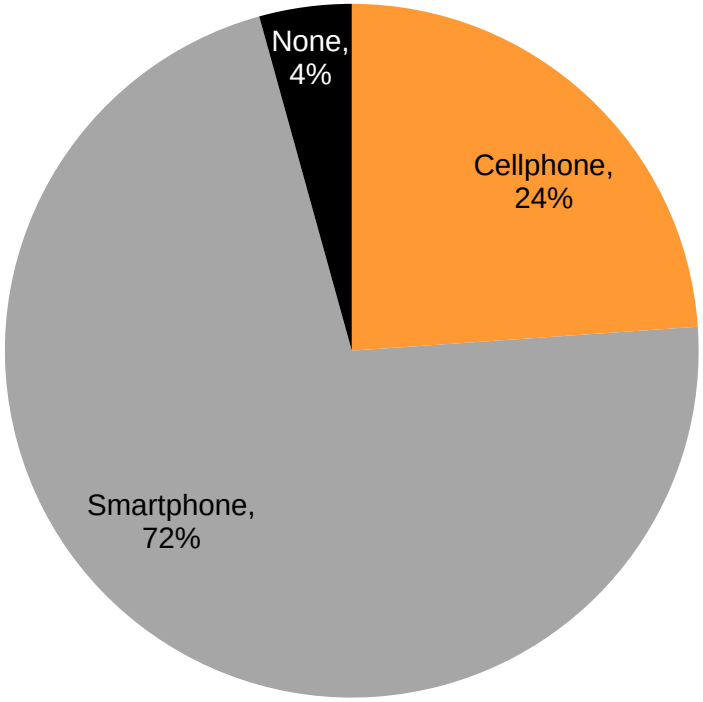


* Family / friend / partner / flatmates

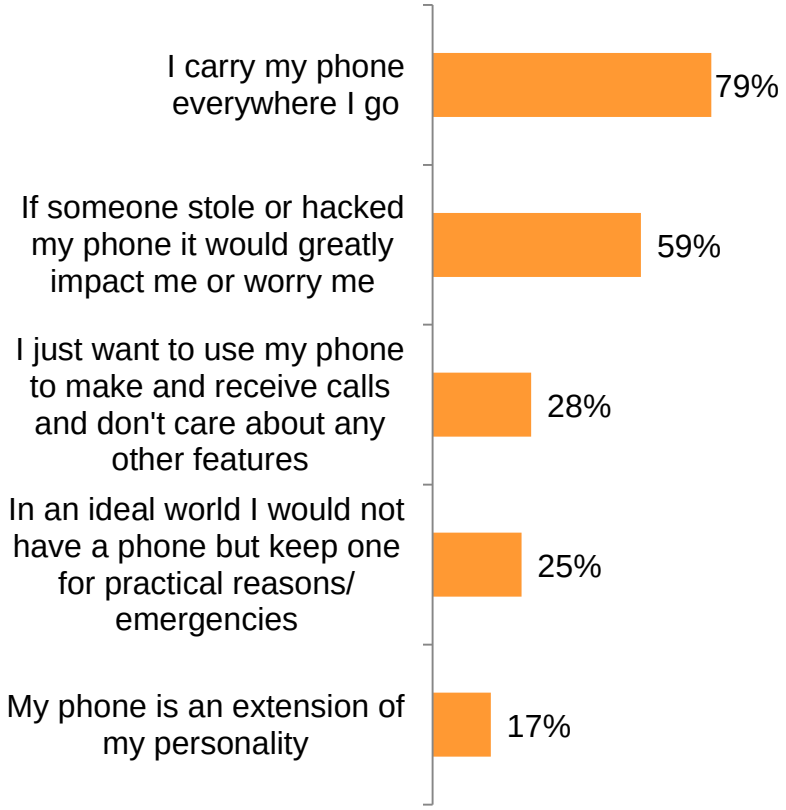
(Base: all respondents, n=1161)

ALMOST ALL HAVE SOME FORM OF CELLPHONE, AND 79% CARRY THEM WHEREVER THEY GO.
HOWEVER, AROUND A QUARTER ARE RELUCTANT USERS, ONLY USING THEM FOR THEIR BASIC FUNCTION

Do you own a cellphone or smartphone?



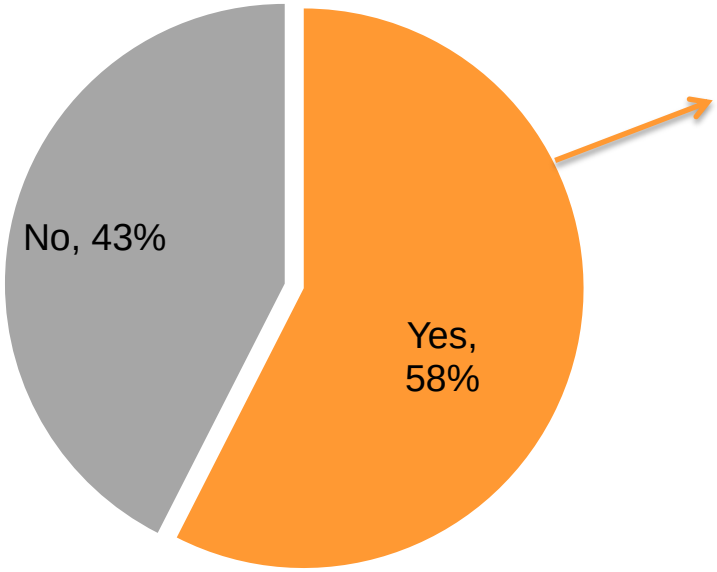
How strongly do you agree or disagree with the following statements:



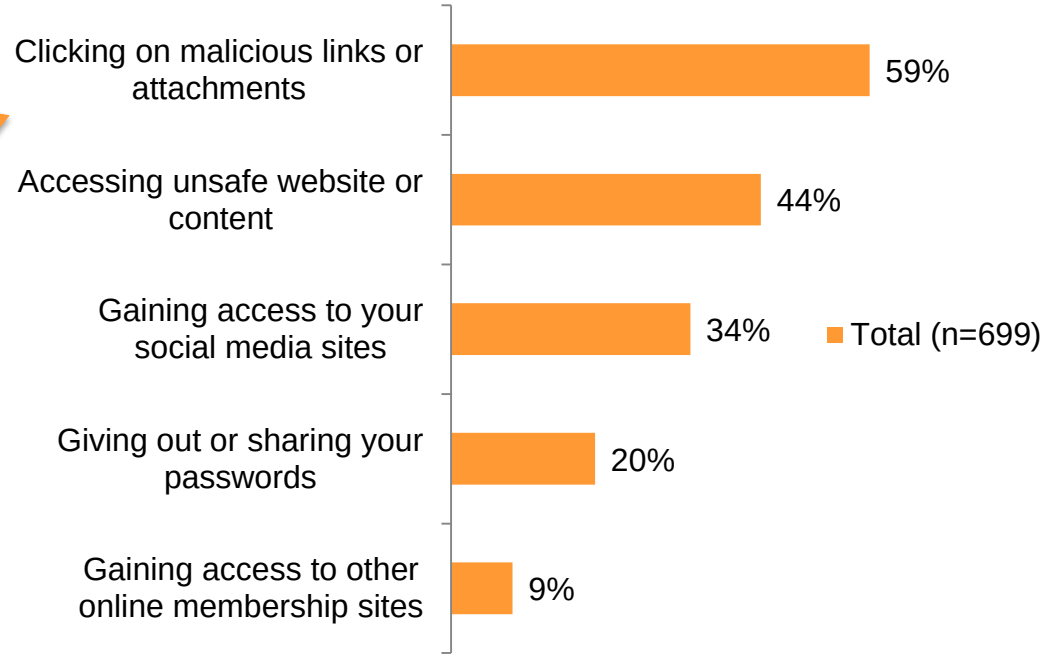
(Base: all respondents, n=1161)

58% SHARE THEIR DEVICES WITH OTHER PEOPLE THAT WANT TO ACCESS THE INTERNET. THE MAIN CONCERN IS THAT A BORROWER MIGHT CLICK ON MALICIOUS LINKS OR ACCESS UNSAFE CONTENT. HOWEVER, FEWER THAN A THIRD CONSIDER THEY MIGHT ACCESS SOCIAL OR OTHER ONLINE MEMBERSHIP SITES.

Are any of the devices you mentioned ever shared with other people that want to access the internet?



If you share or provide access to the internet from a shared device, which of the following have you seriously thought about them doing: (Select all that apply)?



Per•ceptive
[Research]

PASSWORDS

THE VAST RANGE OF SITES ACCESSED MAKES HAVING A LIMITED REPERTOIRE OF PASSWORDS A NECESSITY

- Many sites require a password, and having a different one for each platform is a cognitive nightmare
- To cope, people often simply add numbers to a base password (e.g. 01)
- Banking is one exception where people take extra care over their selection
- Qualitatively, some people don't allow a site to 'remember' their password, but for others, this is passively accepted.

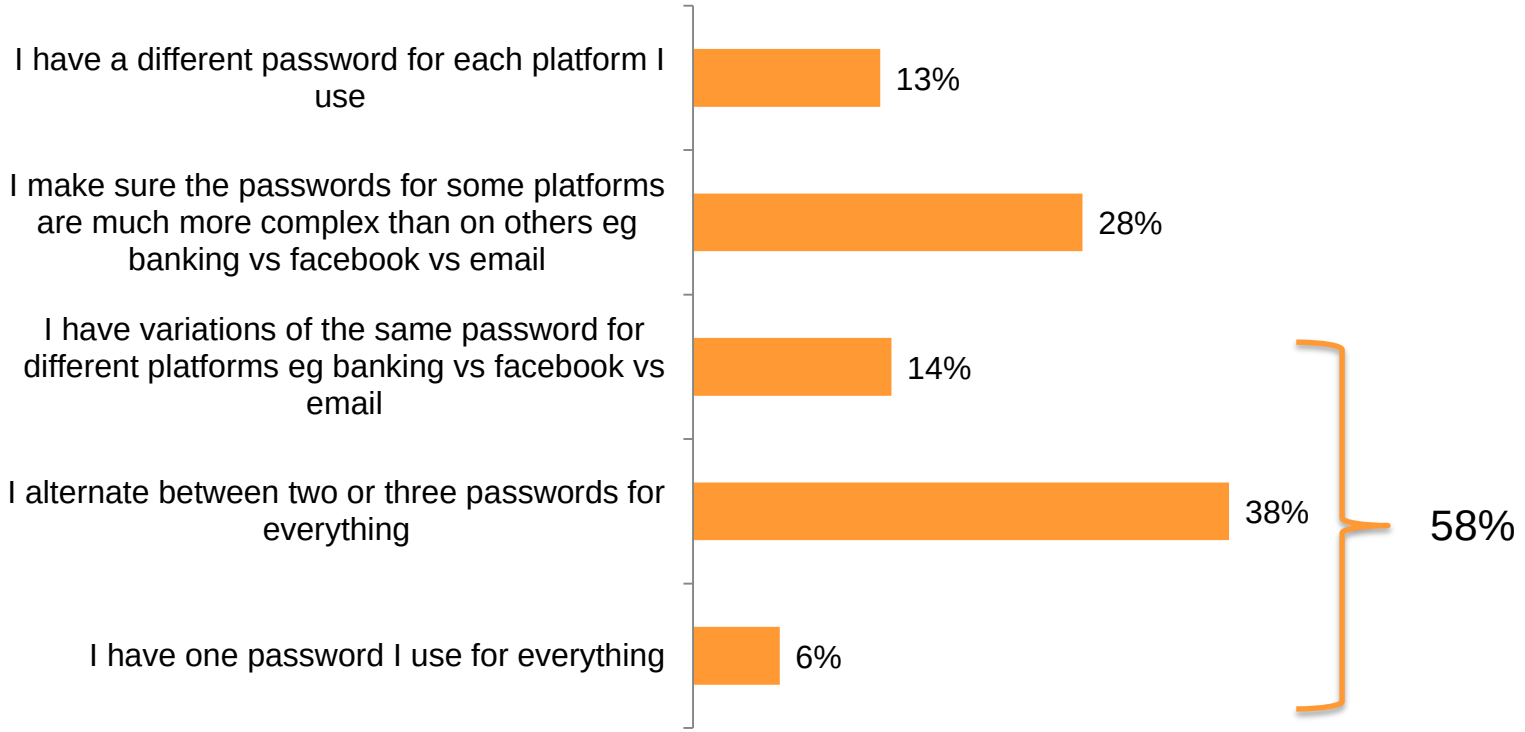
And it gets confusing and I've got about five different passwords but I can't remember which one's for what. Obviously the ones I use like internet banking, I know that one off by heart, but you know. I keep going until it lets me in. Normally in some places you have three chances and it locks you out and you've got to start all over again

I have four or five passwords I rotate between. Except internet banking, I have a different specific password just for my internet banking, because it's my money

And then they go you haven't put a new one on in 30 days, do you want to change it? And you go nah, but you know, I guess the bank's taking an active interest. Where almost every other website it's inherently saved and you don't have to remember it.

OVER HALF THE SAMPLE USE A RELATIVELY LIMITED RANGE OF PASSWORDS ACROSS ALL THEIR ONLINE ACTIVITIES.

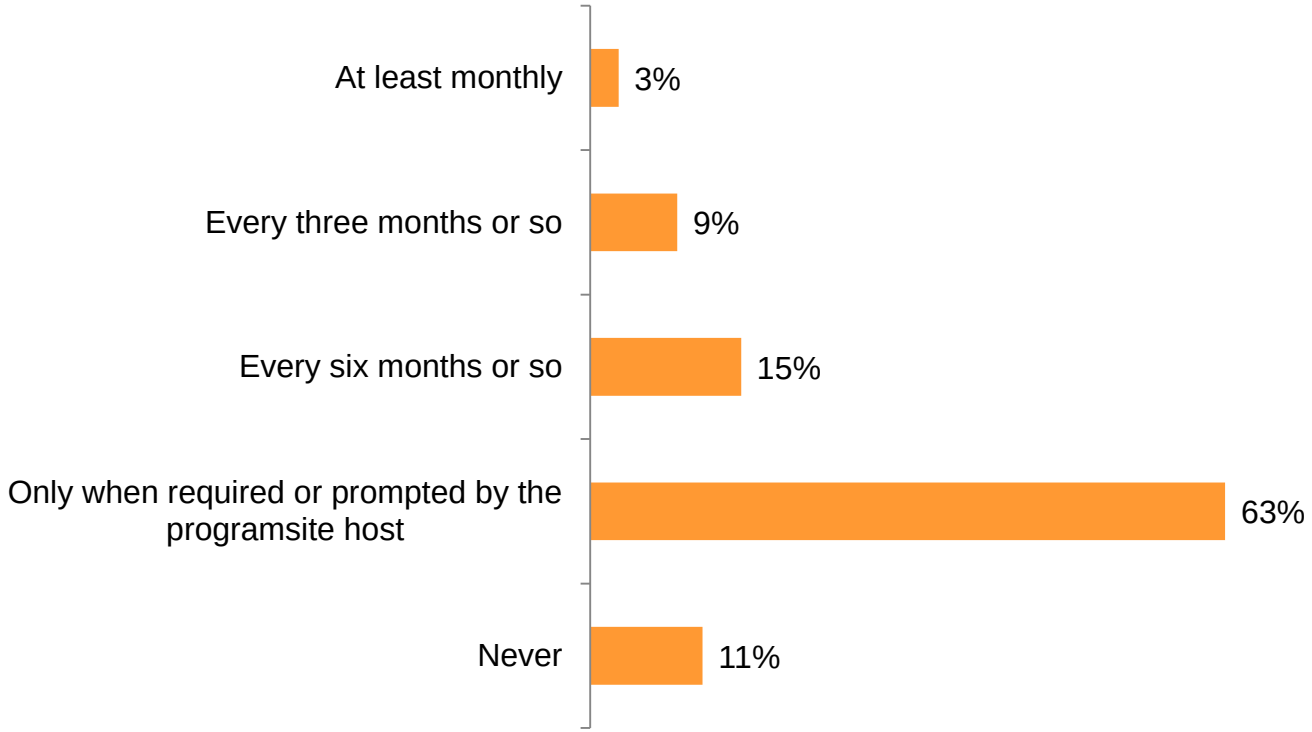
Which statement regarding your passwords applies best to you?



(Base: all respondents, n=1161)

ACROSS THE SEGMENTS, PROPENSITY TO CHANGE PASSWORDS IS LOW, WITH TWO-THIRDS WAITING TO BE PROMPTED.

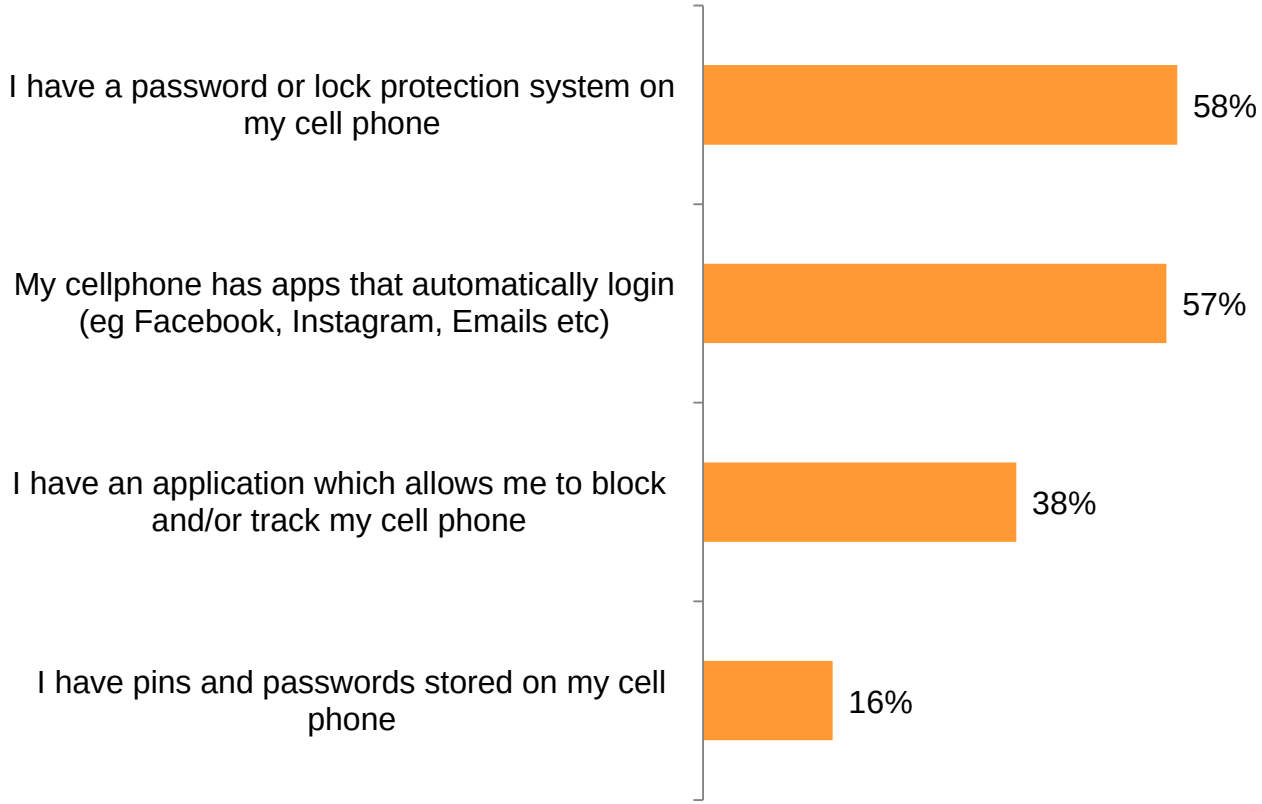
How often do you change your passwords?



(Base: all respondents, n=1161)

ONLY 58% PROTECT THEIR PHONE WITH LOCKS OR PASSWORDS.

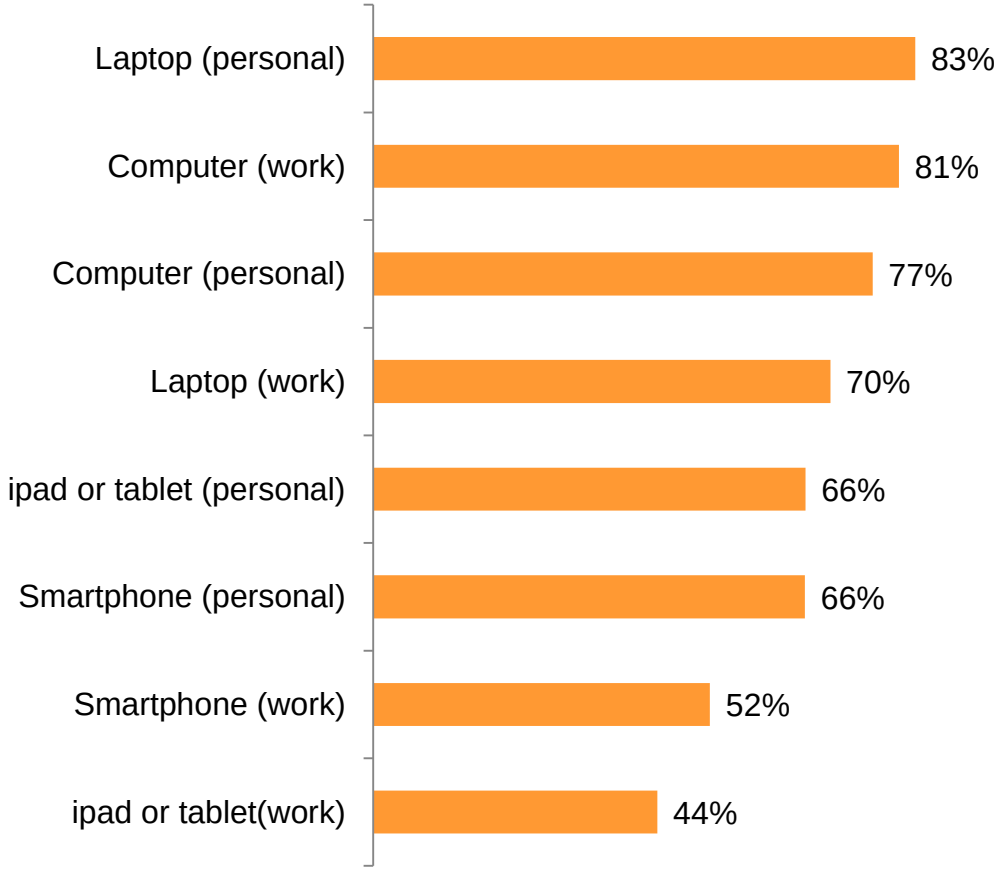
How strongly do you agree or disagree with the following statements:



(Base: all respondents, n=1161)

ONLY HALF OF THOSE WITH A WORK SMARTPHONE HAVE A PASSWORD ON IT (52%), AND EVEN FEWER HAVE PASSWORDS ON THEIR WORK TABLETS (44%)

Which of the following do you have passwords on?



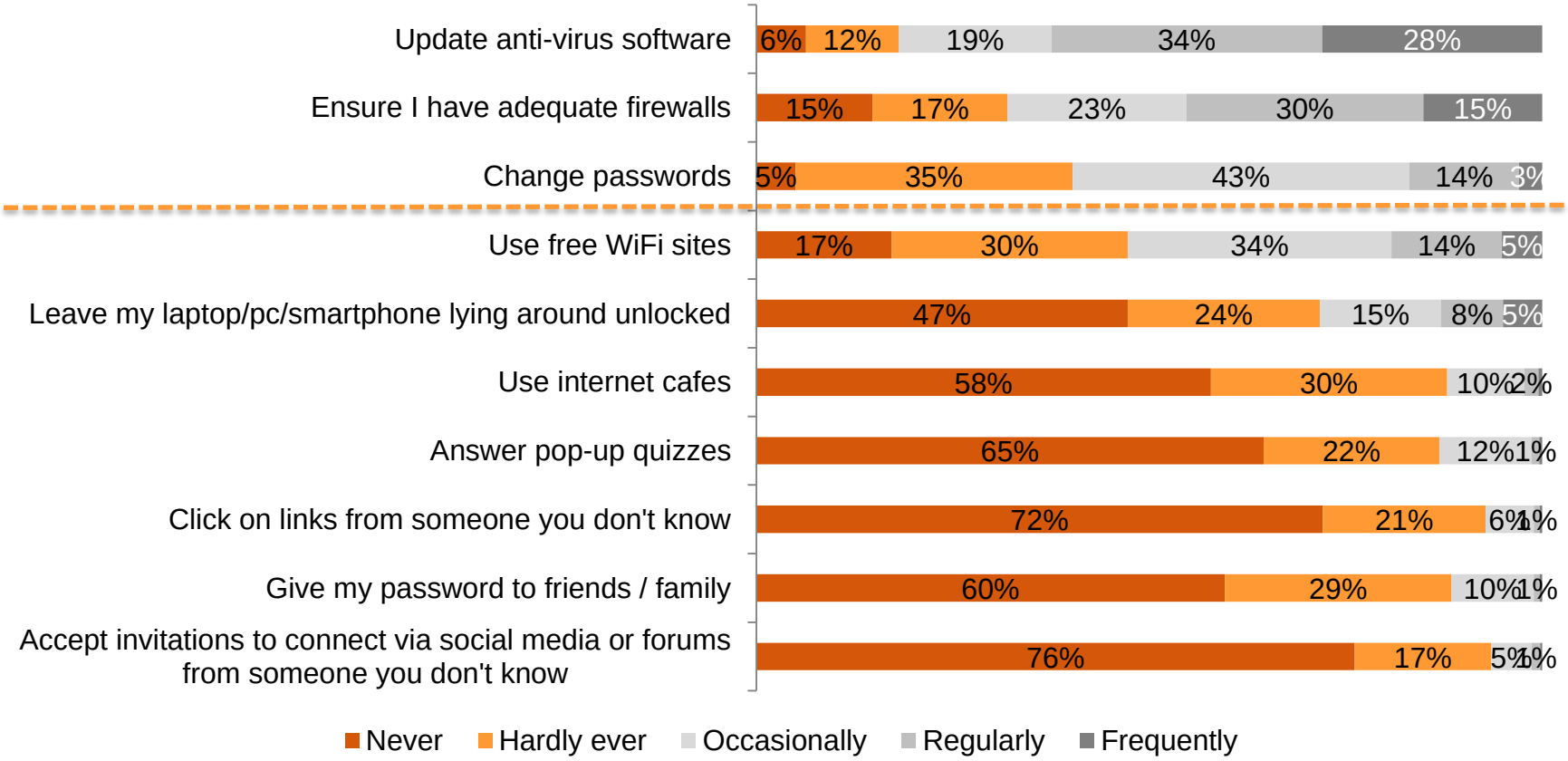
(Base: respondents that have those devices)

Per•ceptive
[Research]

CYBER SECURITY

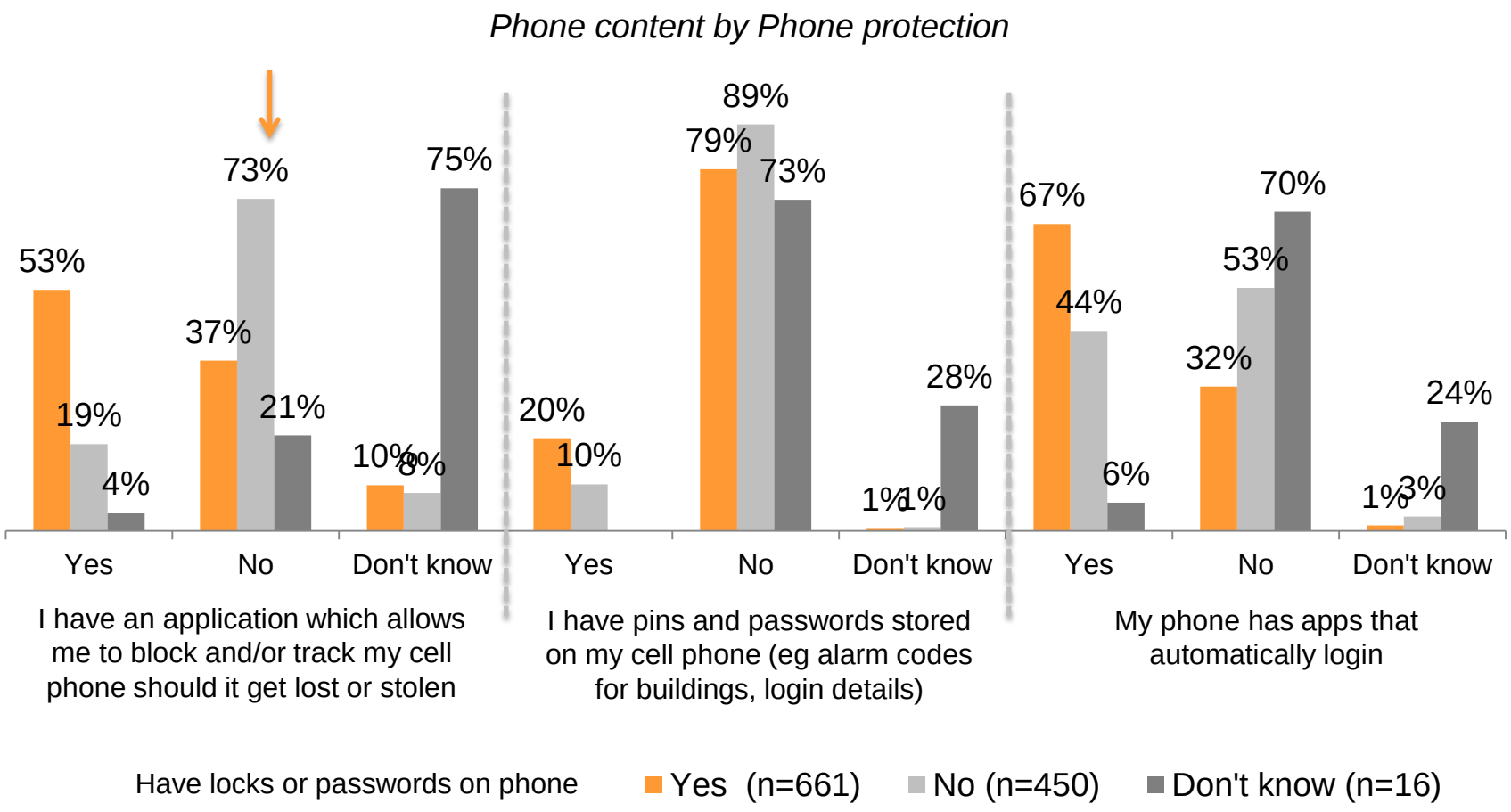
WHILE MOST PEOPLE UPDATE THEIR ANTIVIRUS SOFTWARE AND ENSURE THEY HAVE ADEQUATE FIREWALLS AT LEAST OCCASIONALLY (82% AND 68% RESPECTIVELY), 28% LEAVE THEIR DEVICES LYING AROUND UNLOCKED JUST AS OFTEN

Select how often you do the following?



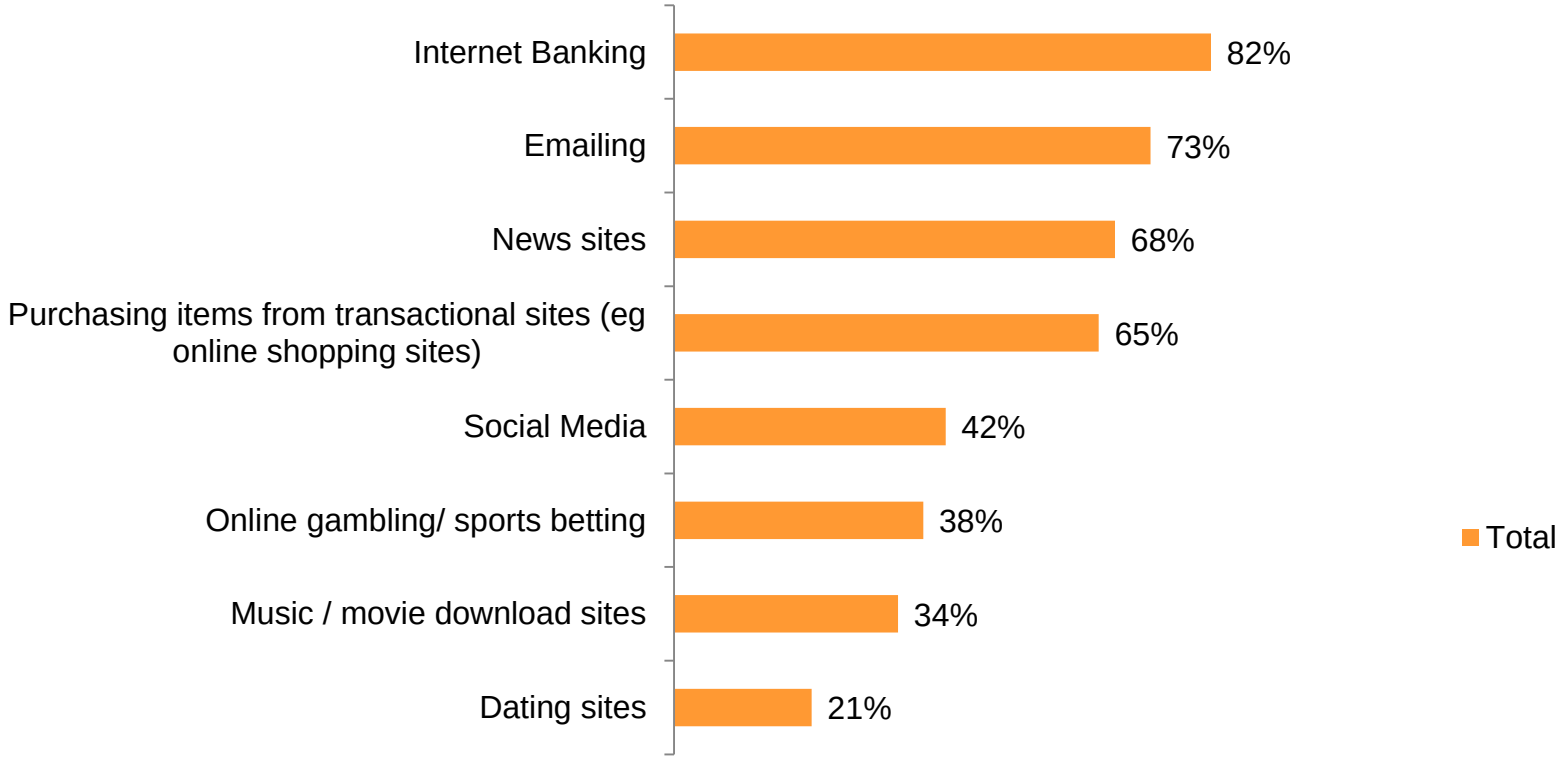
(Base: all respondents, n=1161)

73% OF THOSE WITHOUT PROTECTION ON THEIR PHONE ALSO DON'T HAVE TRACKING/BLOCKING APPS ON THE PHONE



INTERNET BANKING IS CONSIDERED THE MOST SECURE OF THE ONLINE ACTIVITIES LISTED (82% RATED IT AS SECURE), WHILE NEARLY THREE QUARTERS FEEL EMAIL IS SECURE (73%)

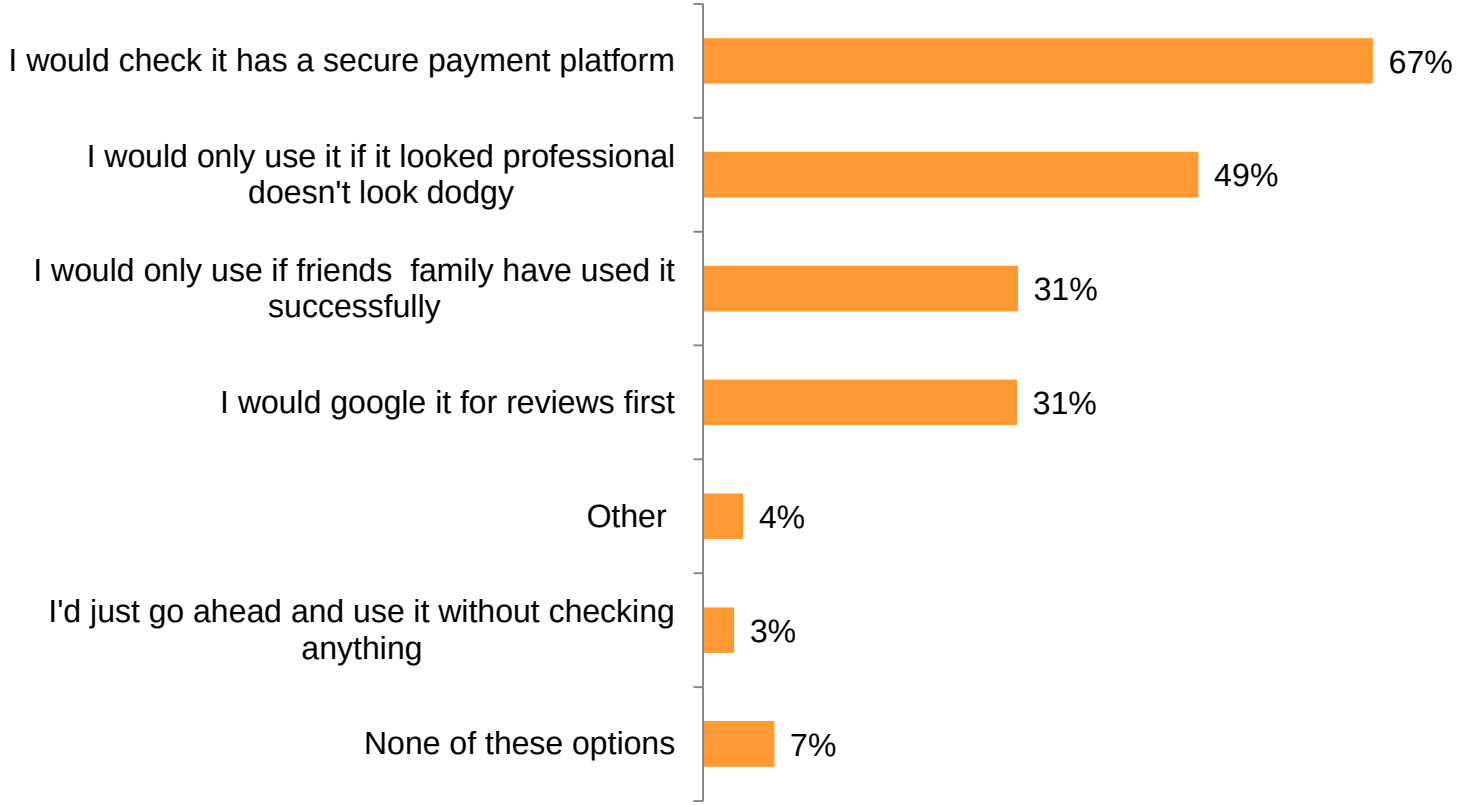
How safe and protected do you feel undertaking the following activities online (4+5, where '5' is Extremely secure):



(Base: undertake the activity)

WHILE TWO-THIRDS WOULD CHECK FOR A SECURE PAYMENT PLATFORM BEFORE MAKING A TRANSACTION, HALF SAY THEY WOULD ALSO ASSESS SAFETY BY THE APPEARANCE OF THE SITE.

Before you use a transactional website (i.e. a website you purchase things through) what do you do to check that it is trustworthy (Select all that apply)?



(Base: all respondents, n=1161)

FOR A NUMBER OF PEOPLE, THE FIRST INDICATION OF WHETHER A SITE IS SAFE IS THAT IT DOESN'T LOOK 'DODGY'

- However, when queried as to what makes a site look safe, most people were unable to define this.

Well you tend to stick with the big boys, the guys like Microsoft or whatever who have put a lot into their brand and they're invested in their brand. So anything that's coming from them should be pretty good. (25-45 year group)

I would make the assumption, I would pass the onus onto the bank, basically make the assumption that if they are offering this on their site and offering me to use it and something goes wrong then essentially they'll have to cover it. So I just trust that their systems are robust enough. (55+ group)

Normally dodgy sites will have flashing stuff and say really cheesy things. You look at it and it's like no, you can't believe that, it's too good to be true, things like that. (13-15 year group)

Yeah, it'd be like you've just won a free MacBook for being the ten thousandth visitor. (13-15 year group)

Per•ceptive
[Research]

EXPERIENCES OF BREACHES

IMPACT OF CYBER SECURITY BREACHES (QUALITATIVE)

Scamming	• Most people find scamming ‘laughable’, a minor annoyance • A familiar issue, many have had a silly email • Generally easily ignored
Hacking	• The most concerning event, but likelihood and implications not top of mind • A sense of invasion • Serious implications if it involves work emails (unprofessional, commercial sensitivity) • Potential for social humiliation (e.g. if a Facebook account) • Potential for private information to be used for many nefarious purposes (bank details, passwords etc)
Viruses	• Happens to ‘other people’ • Everyone has stories of a disastrous event that has ruined a computer or deleted important files • Perception that anti-virus programmes keep them safe • Less of an issue for those with Macs

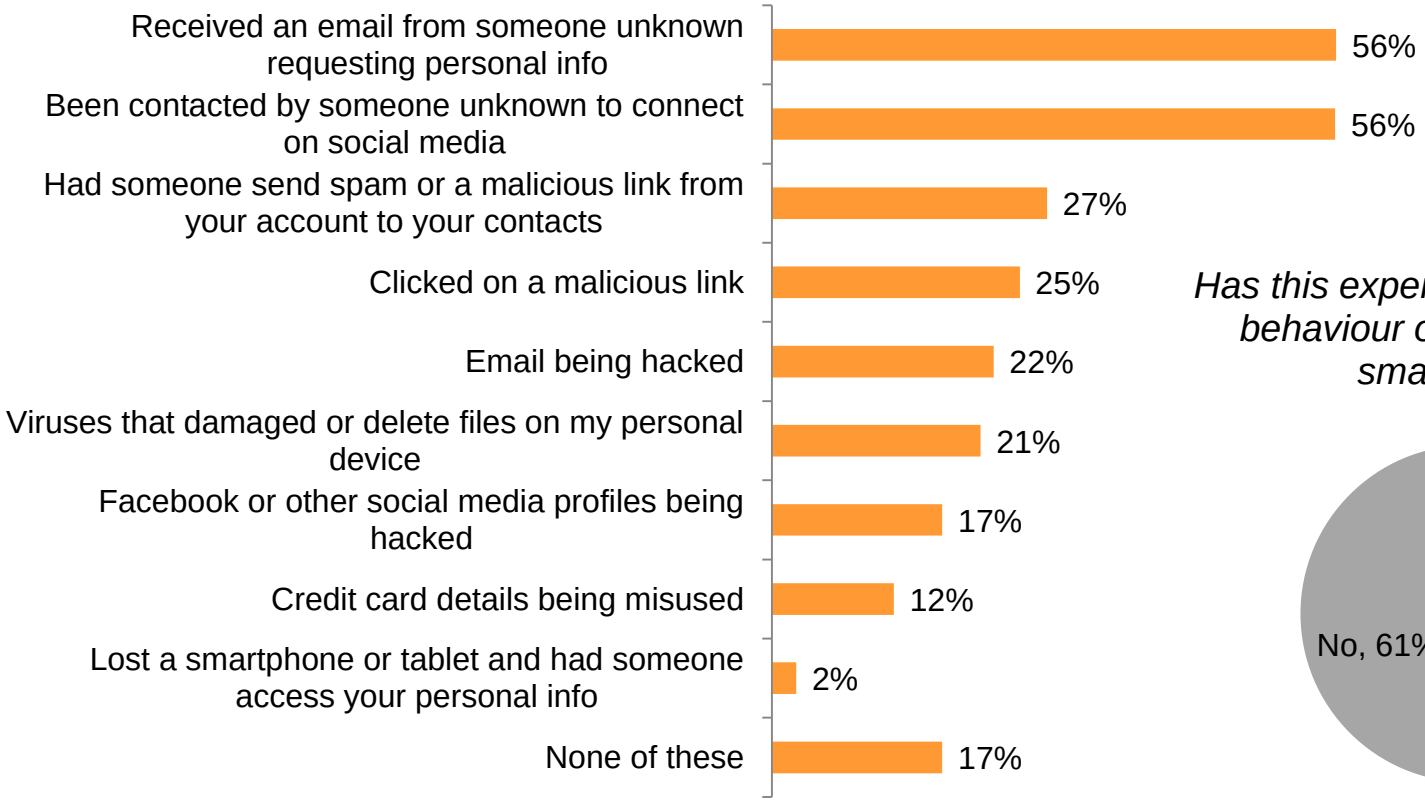
A STEREOTYPICAL CYBER 'VICTIM' CHANGES DEPENDING ON THE BREACH

Scamming		Older women • Naïve, want to help • Haven't been exposed to the issue previously • Less understanding of how they work
Hacking		Everyone with an email, but seldom thought about
Viruses		Older or younger generations • Young - On the internet more often, clicking on more sites • Especially young are even more vulnerable, more likely to fall for dodgy sites • Older – naïve, may fall for lures to click on malicious links

16-45 years less likely to think they are at risk of any cyber security breaches

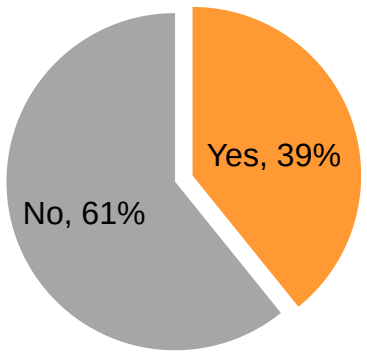
56% SAY THEY HAVE RECEIVED AN EMAIL OR REQUEST TO CONNECT FROM SOMEONE THEY DON'T KNOW, WHILE AROUND A QUARTER HAVE HAD SOMEONE SEND SPAM FROM THEIR ACCOUNT OR HAVE CLICKED ON A MALICIOUS LINK. DESPITE THIS, 6 OUT OF 10 HAVE NOT CHANGED THEIR BEHAVIOUR.

Have you ever experienced any of the following (Select all that apply)?



(Base: all respondents, n=1161)

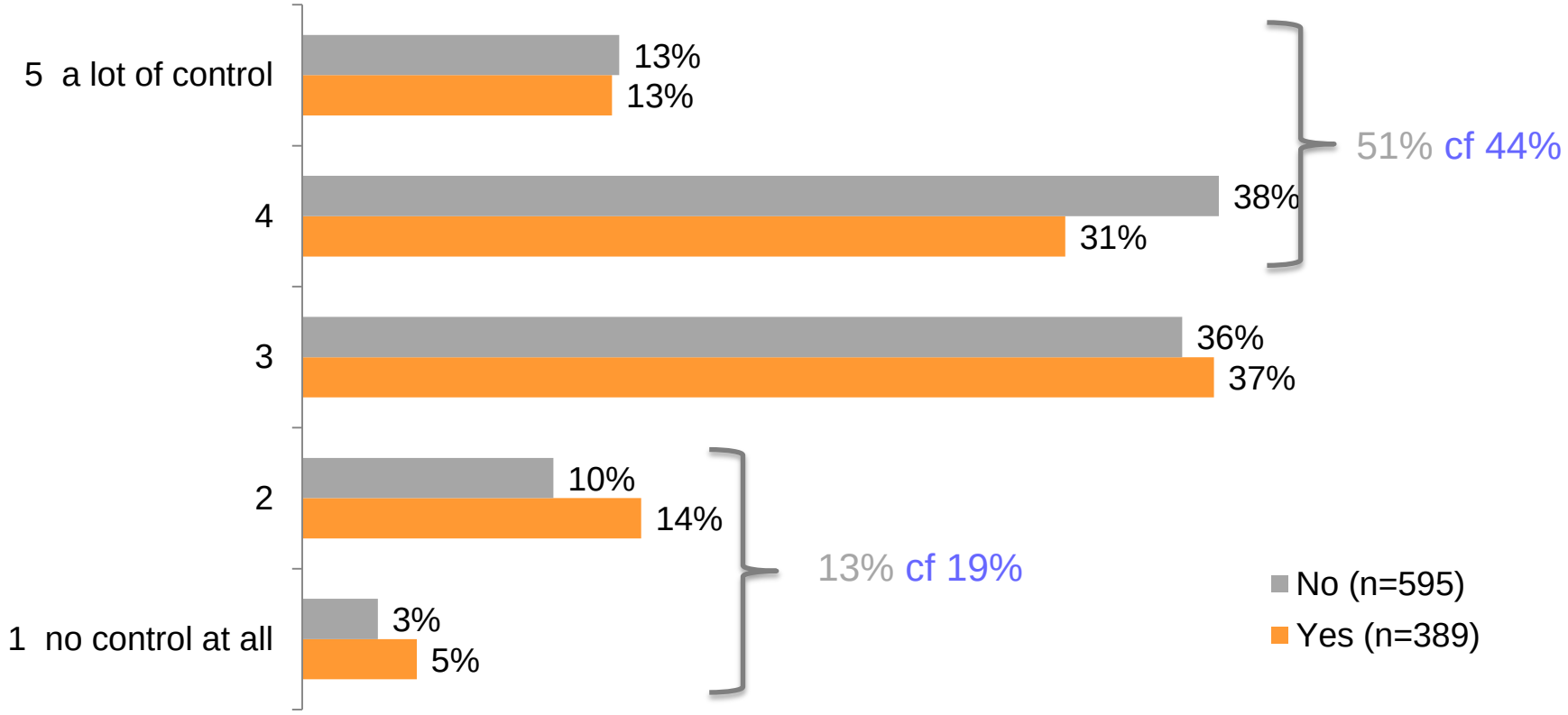
Has this experience changed your behaviour on computers and smartphones?



(Base: those who experienced a breach)

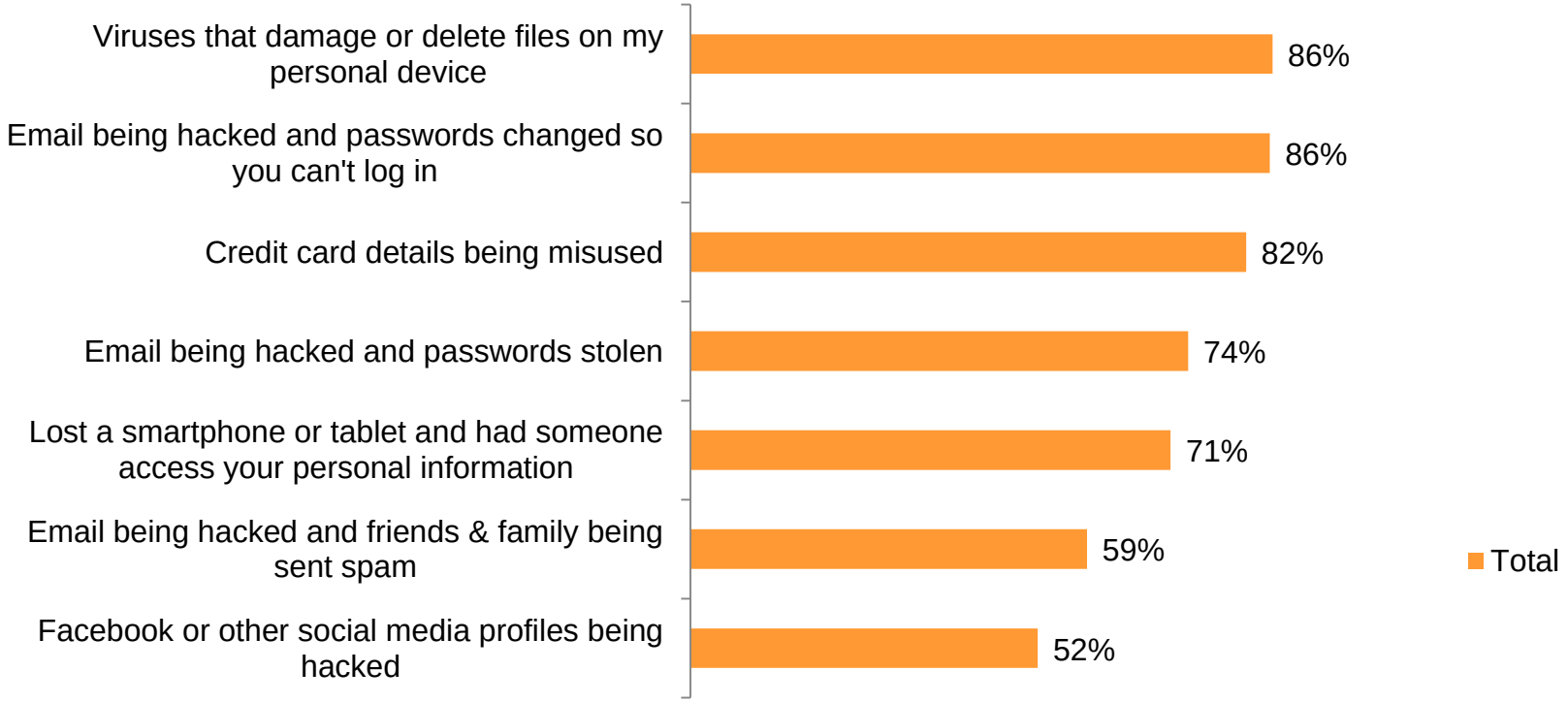
THOSE WHO HAVE EXPERIENCED A SECURITY BREACH IN THE PAST ARE LESS LIKELY TO FEEL THEY HAVE CONTROL OVER PREVENTING THEM

Level of control experienced by those who have experienced a security breach or not



VIRUSES AND HACKING RESULTING IN CHANGED PASSWORDS ARE PERCEIVED TO BE THE MOST IMPACTFUL SECURITY BREACHES.
OF NOTE IS THE PERCEPTION THAT ALTERED PASSWORDS WOULD HAVE A BIGGER EFFECT THAN HAVING PASSWORDS STOLEN.

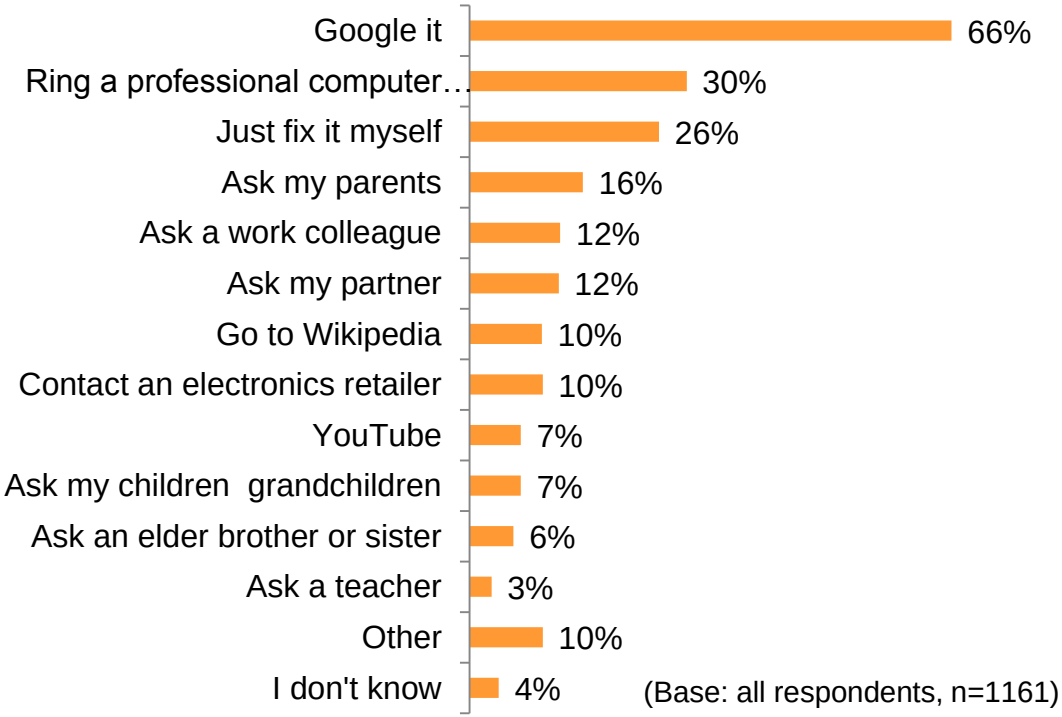
Please indicate how much impact the following security breaches would have if you personally experienced them (4+5 where '5' is Very large impact)



(Base: all respondents, n=1161)

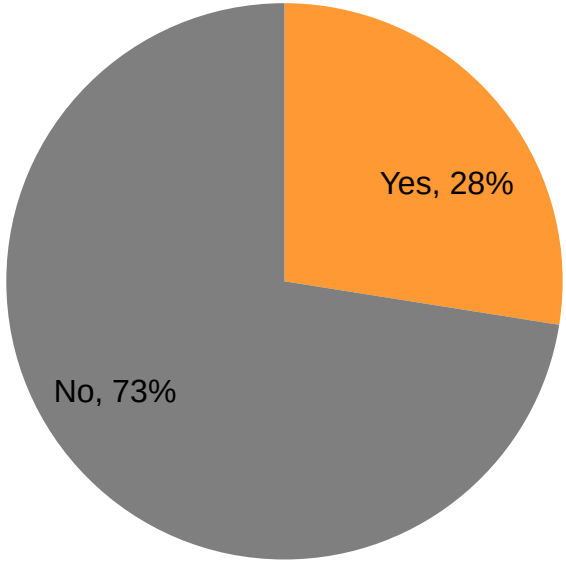
GOOGLE IS THE MAIN SOURCE OF INFORMATION ABOUT CYBER SECURITY BREACHES. WHILE 30% SAID THEY WOULD CONTACT A PROFESSIONAL, A QUARTER SAID THEY WOULD JUST FIX THE PROBLEM THEMSELVES.
NEARLY THREE QUARTERS ARE UNAWARE OF ANY ORGANISATIONS THAT PROMOTE GOOD COMPUTER HYGIENE

If you wanted to find out about a potential cyber security breach (e.g. malicious link, worrying email etc), who / what would you go to get more information (Select all that apply)?



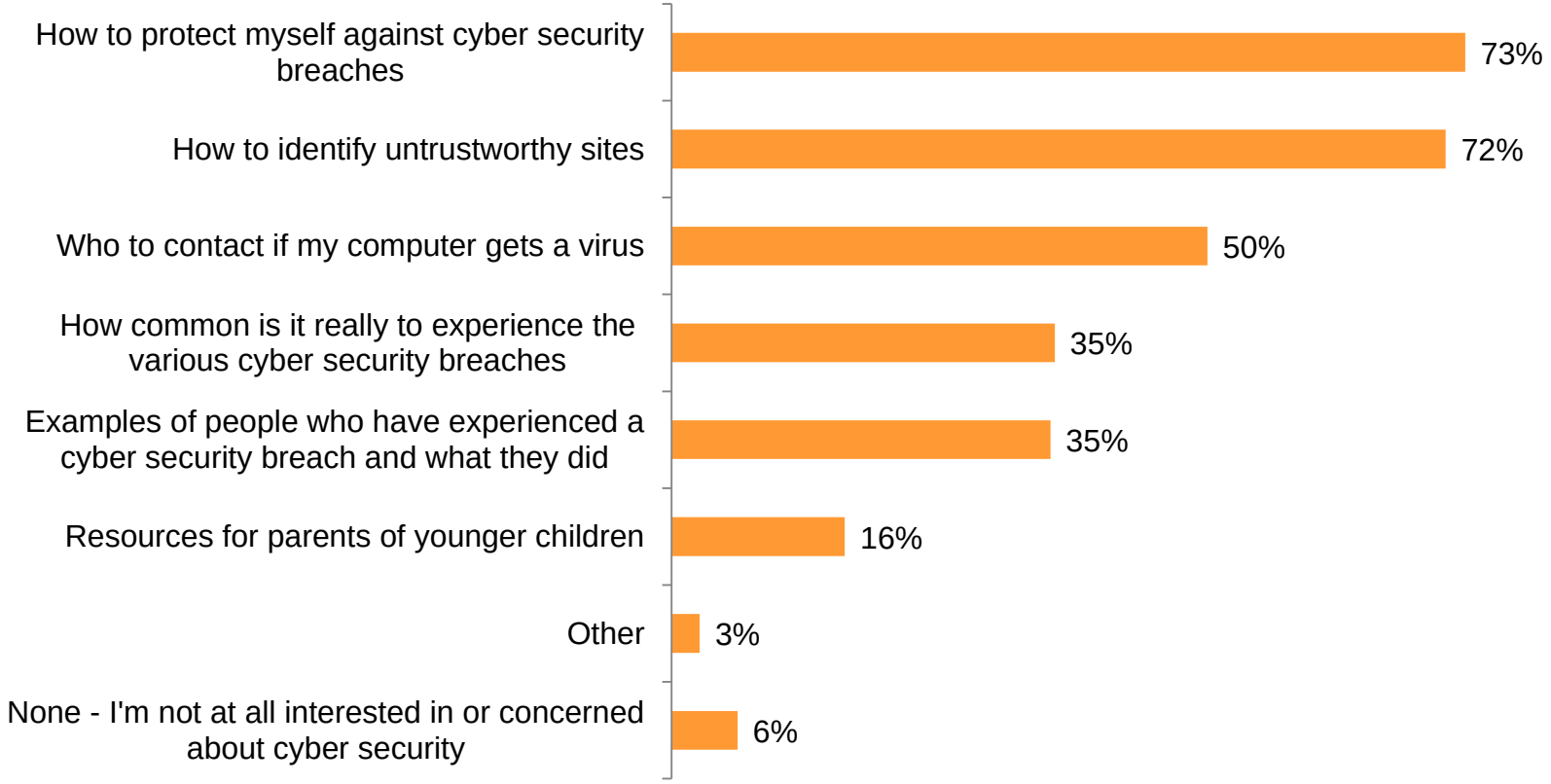
(Base: all respondents, n=1161)

Are you aware of any organisations that promote good computer hygiene and provide information on how to protect your cyber security?



NEARLY THREE QUARTERS WANT PROACTIVE ADVICE ABOUT PREVENTION AND IDENTIFICATION OF POSSIBLE RISK, WHILE HALF ALSO WANT INFORMATION ABOUT WHO TO CONTACT IF THEY GET A VIRUS.

When it comes to cyber security, which information would be most interesting to you (Select all that apply)?



(Base: all respondents, n=1161)