ESET Survey Report USA // January 2019

ESET CYBERSECURITY BAROMETER

USA 2018

“Sadly, 87 percent of Americans surveyed believe that the risk of becoming a victim of cybercrime is increasing.”

“Nine out of ten Americans now see cybercrime as a challenge to the country’s security, bigger than drug trafficking, money laundering, and several other major crimes.”

ENJOY SAFER TECHNOLOGY™

PREFACE

The *ESET Cybersecurity Barometer USA* is a survey of public opinion about cybersecurity, cybercrime, and related privacy concerns in America. The survey was conducted because there is a lack of publicly-funded research quantifying American public attitudes towards, and experience of, these critically important issues. This is problematic because public support is vital to the success of cybersecurity efforts, including cybercrime deterrence and data privacy protection. Those efforts are in turn the key to maximizing the benefits of a wide range of digital technologies upon which the US is heavily reliant.

As a security software company with three decades of experience fighting criminal abuse of digital technology, ESET understands that people are one of the three key factors involved in defeating cybercrime, the other two being process and technology. Furthermore, people are victimized by cybercrime, people elect the politicians who determine cybercrime policy, and people foot much of the tax bill for law enforcement efforts to reduce cybercrime.

Therefore, knowing what the public thinks about cybercrime and cybersecurity is essential to successful cybercrime policy development and to success in society's cybersecurity efforts. (For more on this, see the article "Why ask the public about cybercrime and cybersecurity?" on WeLiveSecurity, the ESET research website.)

In 2018, the ESET Cybersecurity Barometer was fielded to a survey sample of 3,500 people (2,500 in the US and 1,000 in Canada). The 2018 Canadian report was published here. A report focusing on inter-country comparisons – encompassing North America and the 28 nations of the EU – will also be published. We hope to repeat these surveys in 2019 to enable longitudinal studies that encompass both continents.

The ESET Cybersecurity Barometer is modelled on prior studies conducted by the European Union (EU), published as the "Special Eurobarometer: Cyber Security." The EU has conducted four of these studies, the most recent of which was published in 2017. They provide longitudinal research across 28 countries based on a 1,000 person sample from each country. Such research has the potential to help a wide range of cybersecurity stakeholders, including policymakers, consumers, companies, and government agencies. The ESET Cybersecurity Barometer seeks to extend the potential benefits of this type of research to North America.

METHODOLOGY

The survey reported here polled 2,500 US adults using standard CAWI methodology with random sampling based on age, gender, and place of residence. It was conducted for ESET in September of 2018 by MNFORCE using the Research Now SSI panel.

CONTENTS

1. EXECUTIVE SUMMARY

2. CYBERCRIME AS A THREAT TO SECURITY AND PRIVACY

3. CYBERSECURITY AND PRIVACY CONCERNS

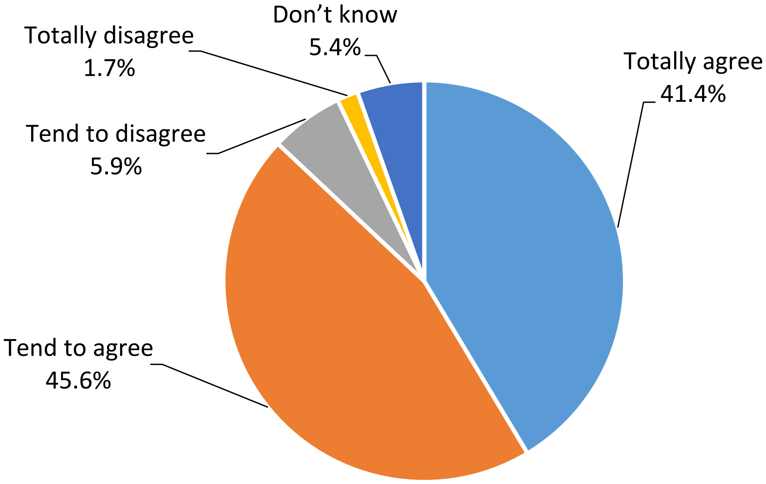
4. CYBERSECURITY AND PRIVACY RESPONSES

5. DISCUSSION

1. EXECUTIVE SUMMARY

The survey findings indicate that Americans are very concerned about cybersecurity, with 87% of respondents agreeing that the risk of becoming a victim of cybercrime is increasing. One third are concerned that their personal information is not kept secure by websites.

These findings should be worrying news for companies whose business models rely on public trust in the internet. It should also concern politicians and the government, including law enforcement agencies. The survey findings strongly suggest that US efforts at cybercrime deterrence have not given the American public much cause for hope.



Do you agree with this statement: I believe the risk of becoming a victim of cybercrime is increasing?

To put the public's level of concern about cybercrime in perspective: it is now seen by many as a serious threat to America. A shocking nine out of 10 survey respondents said cybercrime was an important challenge to the internal security of the country. Clearly, this finding has significant implications for public policy: Americans see cybercrime as more of a challenge to internal security than drug trafficking and money laundering, putting it up there with terrorism and corruption.

Cybercrime is not some vague, theoretical threat for Americans: close to 60% of respondents had found malicious code on one or more of their devices and 30% had experienced identity theft. Seven out of 10 said that they had data privacy concerns like misuse of their personal data when they went online to bank or shop. All of which suggests that a serious realignment of crime-fighting resources is needed, as well as improvements in privacy protection. Indeed, less than half of the US adults surveyed thought the authorities were doing enough to fight cybercrime (respondents gave government and law enforcement higher scores for their efforts against terrorism and drug trafficking).

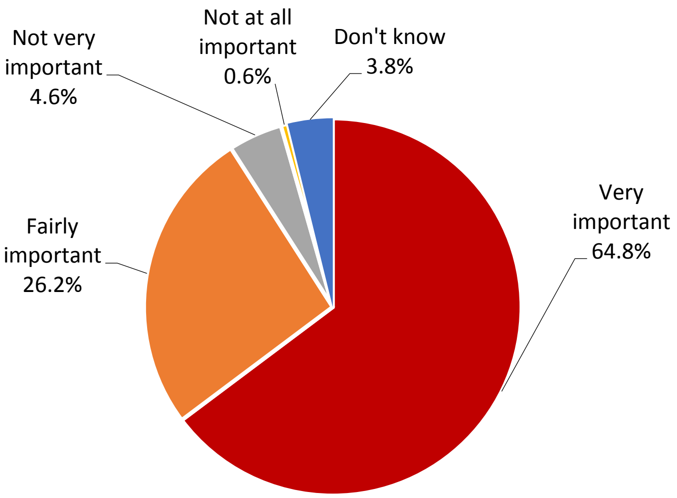
These ESET Cybersecurity Barometer finings clearly imply that many Americans think there is too much cybercrime and not enough cybersecurity; as a result, some Americans are reducing their use of online technology. Fears of identity theft and misgivings about data privacy loom large. To the extent that this situation impedes progress and threatens the promised benefits of the next wave of digital transformation, concerted action by government agencies and corporate entities to improve this situation would seem to be seriously overdue.

2. CYBERCRIME AS A THREAT TO SECURITY AND PRIVACY

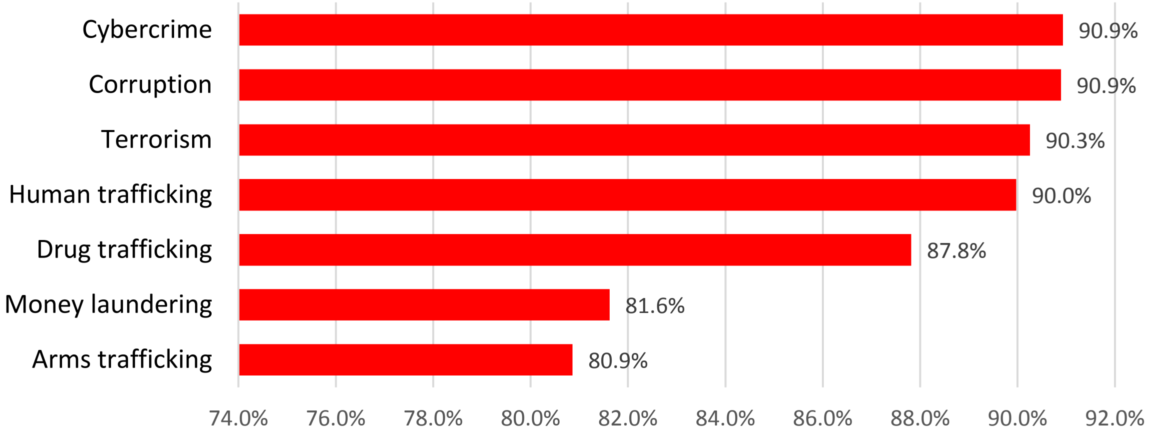
The ESET Cybersecurity Barometer reveals that most Americans now consider cybercrime to be an important challenge to the internal security of the USA, with nine out of 10 saying it is either very important (65&) or fairly important (26%).

This perception of cybercrime appears to be widely shared across America, with the Midwest region expressing slightly more concern than the national average. In the Northeast not one respondent was prepared to say that cybercrime was not important.

To place this in perspective, it would appear that Americans consider cybercrime to pose more of a challenge to their country's internal security than a number of other serious criminal activities such as money laundering or trafficking in drugs or weapons.

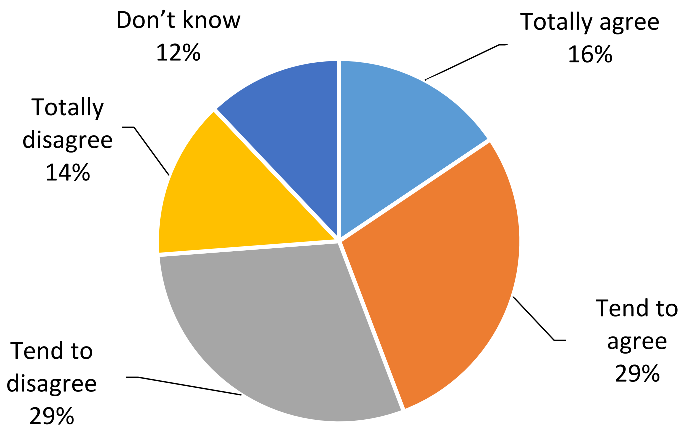


How important is cybercrime as a challenge to the internal security of the USA?



Importance of criminal activity as a challenge to the internal security of the USA (percentage of respondents who chose Fairly important or Very important)

There are probably multiple factors contributing to this high level of concern about cybercrime. The survey data speaks to two of them: personal experiences with cybercrime, and the perception that people have of the government's response to the problem, or lack thereof.



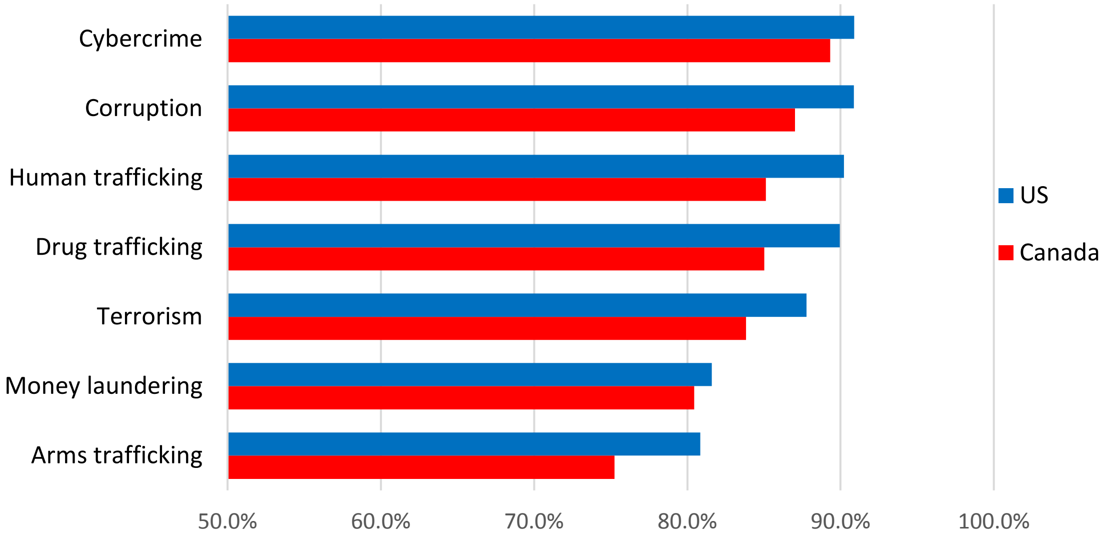
Are the police and other law enforcement authorities in America doing enough to fight cybercrime?

When it comes to the government’s response to cybercrime, fewer than half of US adults surveyed (45%) thought that the police and other law enforcement authorities were doing enough to fight cybercrime.

While it is not uncommon for criminologists to find that public perceptions about crime are out of sync with the number of crimes experienced, these responses about the adequacy of law enforcement’s response to cybercrime may explain why most Americans think cybercrime will increase in the future. After all, only 14% of respondents “totally agree” that the authorities are doing enough to fight cybercrime. (On the bright side, the survey found that Americans think the government is doing a better job against terrorism and arms trafficking.)

To put these responses in context, it should be noted that fighting cybercrime is not easy - most cybersecurity professionals concur that fighting crime in cyberspace is quite different from tackling crime in physical space, and considerably harder. The police and other law enforcement authorities cannot be expected to gain ground against criminals in cyberspace without serious investment in skills and resources. Hopefully, the high levels of concern registered by this survey will be seen as a clear signal that such investment should be a higher priority in public policy than it has been so far.

Americans are not alone in putting cybercrime at the top of the crime list. When Canadians were asked the same questions, cybercrime emerged as the most important challenge in Canada as well. (Canadian respondents did express a slightly lower level of concern than their southern neighbors for each of these criminal activities, but the concern gap around cybercrime was relatively small.)

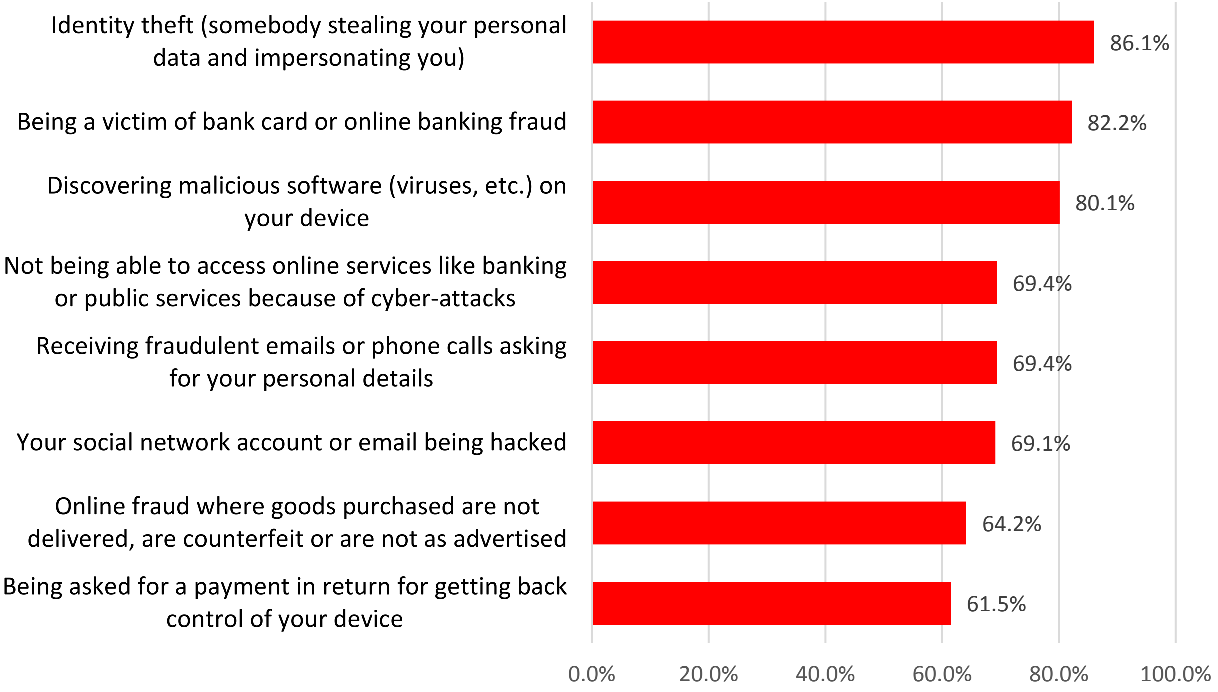


Importance of criminal activity as a challenge to the internal security of your country (percentage of respondents who chose Fairly important or Very important)

3. CYBERSECURITY AND PRIVACY CONCERNS

The ESET Cybersecurity Barometer asked US adults how concerned they were about experiencing or being a victim of various forms of cybercriminal activity such as the hacking of their email or social network account, discovering malware on their computer, or being asked for a payment in return for getting back control of a device (ransomware).

The next two charts explore the responses, which indicate that the biggest concern of all is also the most privacy invasive: identity theft, or ID theft, defined in the survey as *somebody stealing your personal data and impersonating you*. This is closely followed by concern about becoming a victim of bank card or online banking fraud. Malware infection rounds out the top three worries.



Percentage of respondents registering concern about experiencing cybercriminal activity
(Fairly concerned plus Very concerned)

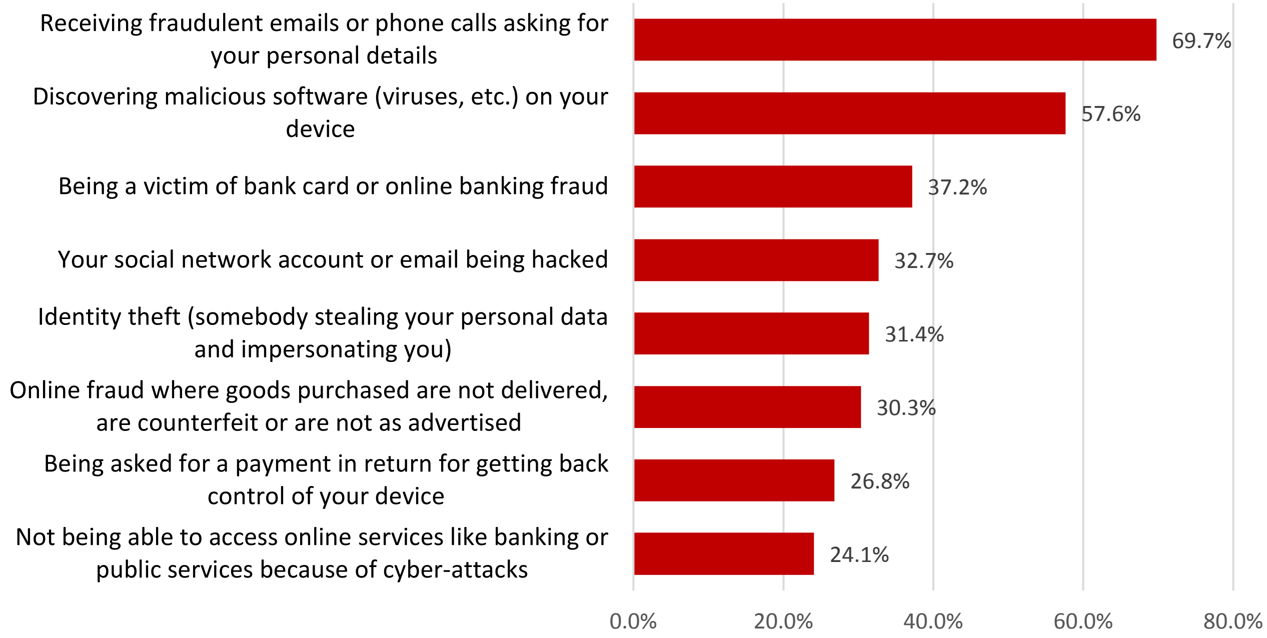
(Note that asking for a payment *in return for getting back control of your device* is one way to describe ransomware, but the survey question was developed – and tracked in the EU – before the term ransomware was widely used. It is possible that more people would have expressed concern if the survey had employed the term ransomware.)

Taken as a whole, these responses to questions about specific threats to cybersecurity and privacy may help to explain why Americans think cybercrime is such a big problem: all eight issues are concerning to more than 60% of respondents, and the top three issues concern more than four out of five. That suggests a deep level of concern relative to the ever-increasing volume of personal information being collected over the internet and the high level of trust people are expected to place in this technology.

The level of concern about cybercrime showed little variation between regions. Concern was lowest in the West and highest in the South. The Northeast was almost identical to the national average while the

Midwest was slightly below. Survey respondents in the US expressed more concern about each of these risks than those in Canada (you can access the Canadian report here).

The level of concern that a population has about becoming a victim of a particular crime may not always be a direct reflection of how much of that crime the population has experienced, so the survey also includes this question: *How often have you experienced or been a victim of the following situations?* The survey tracks the same categories as in the questions about levels of concern. The results show that two categories of criminal activity had been experienced by more than half of all US respondents: fraudulent requests for personal information and malware.



Respondents who had experienced cybercriminal activity (often or occasionally)

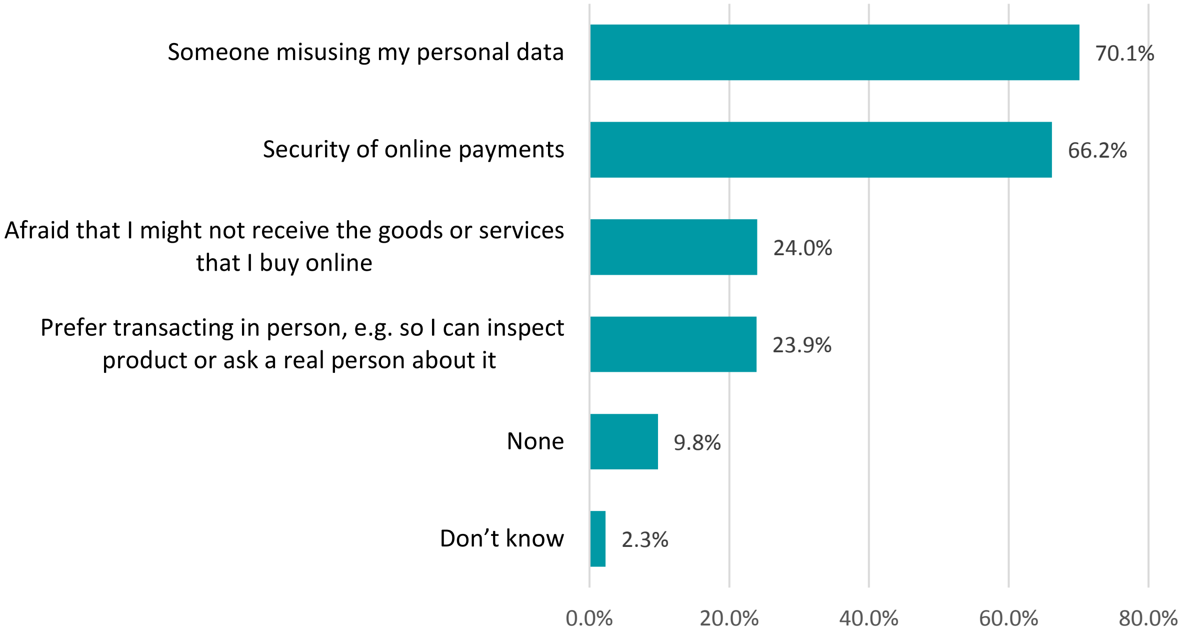
Perhaps the most striking finding here is that over 30% of the adult Americans that we surveyed had experienced ID theft. To put this in perspective, it indicates that the level of ID theft in the US is 45% higher than in Canada. Could this result be an anomaly? Possibly, but it should be noted that at least one other contemporaneous study has indicated that the identity theft rate in the US above 30%.

At 27%, the rate at which respondents experienced ransomware – a demand for payment in return for getting back control of a device – is also worrying. However, the survey did not capture how many people actually paid such demands – a shortcoming that will be corrected in future editions.

Sadly, respondents in America experienced all of the issues at higher rates than the people we surveyed in Canadian, with the exception of malware. It appears that malicious code is experienced by almost three out of five Canadians, the same as for Americans.

As might be expected, the survey found that concerns about crime are more widespread than the experience of crime. Criminologists often find that this is the case, and fear of specific crimes can be amplified by heavy media coverage and well-intentioned victim advocacy. This can also have positive effects, like attracting resources to address the problem and encouraging crime-reducing behavior among potential victims. Of course, some crimes are worse than others in terms of their impact on people's lives. For example, anecdotal evidence suggests that identity theft can be very unsettling to people, a violation of personal privacy that may cause a greater psychological impact than some other forms of digital crime.

The survey results suggest that concerns about cybercrime add to worries about data privacy. When asked about a variety of concerns related to online banking and shopping, 70% of Americans surveyed indicated that they are worried about the misuse of personal data supplied online. This suggests that the companies with whom Americans do business online need to do more to convince customers that their data privacy is taken seriously. (Reducing the number of data breaches would also help.)



What concerns do you have, if any, about using the internet for things like online banking or buying things online?

As you can see, two thirds of respondents (66%) in America expressed concern about the security of online payments. Again, this could be interpreted as a call to online merchants to step up their security efforts and demonstrate that they take the security of online transactions seriously.

Interestingly, concern about misuse of personal data involved in online transactions did not vary much across America, but there were regional variations around other concerns, like the non-delivery of goods and services bought online. On this issue there was much more concern in the South but somewhat less in the Northeast.

Somewhat surprisingly, Americans as a whole were less concerned about non-delivery of online purchases than Canadians (24% in the US compared to 32% in Canada). The preference for performing transactions in person as a response to online security concerns was a lot higher in the Northeast of the US (28%) than across the rest of the country (24%).

When responses about online activities were tabulated, several regional variations of note were apparent. It seems that the uptake of online banking in the Midwest is below the national average, even though respondents in the region use email more than anyone else. Apparently the South does more social networking and TV watching over the internet than other regions.

Which of the following activities do you do online?	REGION				
	South	West	Midwest	Northeast	US Overall
Online banking	78.0%	77.5%	74.4%	77.0%	76.9%
Buying goods or services (holidays, books, music, etc.)	75.7%	78.0%	77.2%	75.2%	76.5%
Selling goods or services	28.6%	26.3%	28.7%	29.1%	28.2%
Using online social networks	78.2%	68.5%	70.6%	71.3%	73.0%
Sending or receiving email	85.8%	85.1%	86.0%	81.8%	84.9%
Reading news	67.4%	70.0%	71.7%	68.0%	69.0%
Playing games	51.2%	45.2%	48.6%	52.7%	49.5%
Watching TV	50.8%	44.4%	39.3%	48.8%	46.5%

To help assess privacy concerns related to use of the internet the survey asks respondents if they agree or disagree with this statement: *I am concerned that my online personal information is not kept secure by websites*. Sadly, one third of US respondents said that they totally agreed, compared to one in four Canadians.

Given the extent to which companies and government agencies have come to rely on the internet as a tool for communication and interaction with the public, these numbers should be worrying. If the public doubts the ability of organizations to protect personal data from exposure, those organizations may find it much harder than expected to realize net gains from further digital transformation, such as big data, location data, machine learning, and the Internet of Things.

The survey also asked people if they agreed with this statement: *I am concerned that my online personal information* is not kept secure by public authorities. Unfortunately, more than three quarters of US respondents (76%) either tended to agree or totally agreed, versus two thirds in Canada. Somewhat surprisingly, concern was lowest in the West (72%) while all three of the other regions reported slightly higher concern than the national average.

When it comes to improving cybersecurity and addressing the risks of cybercrime, it is helpful to know the degree of confidence that people have in their ability to understand the problem. The ESET Cybersecurity Barometer found that two thirds of the North Americans surveyed considered themselves to be well informed about the risks of cybercrime (either 'Fairly well' or 'Very well informed'). However, confidence was considerably higher in the US (70%) than in Canada (62%).

In comparison, when this same question was asked of the residents of all 28 EU countries in 2017, the average "well-informed" percentage was only 46% for the region as a whole; however, there was considerable variation between countries (ranging from 27% in Bulgaria to 76% in Denmark).

As the following table shows, there were some regional variations within the US. Folks in the Midwest considered themselves less well informed, while people in the Northeast appeared to be most confident.

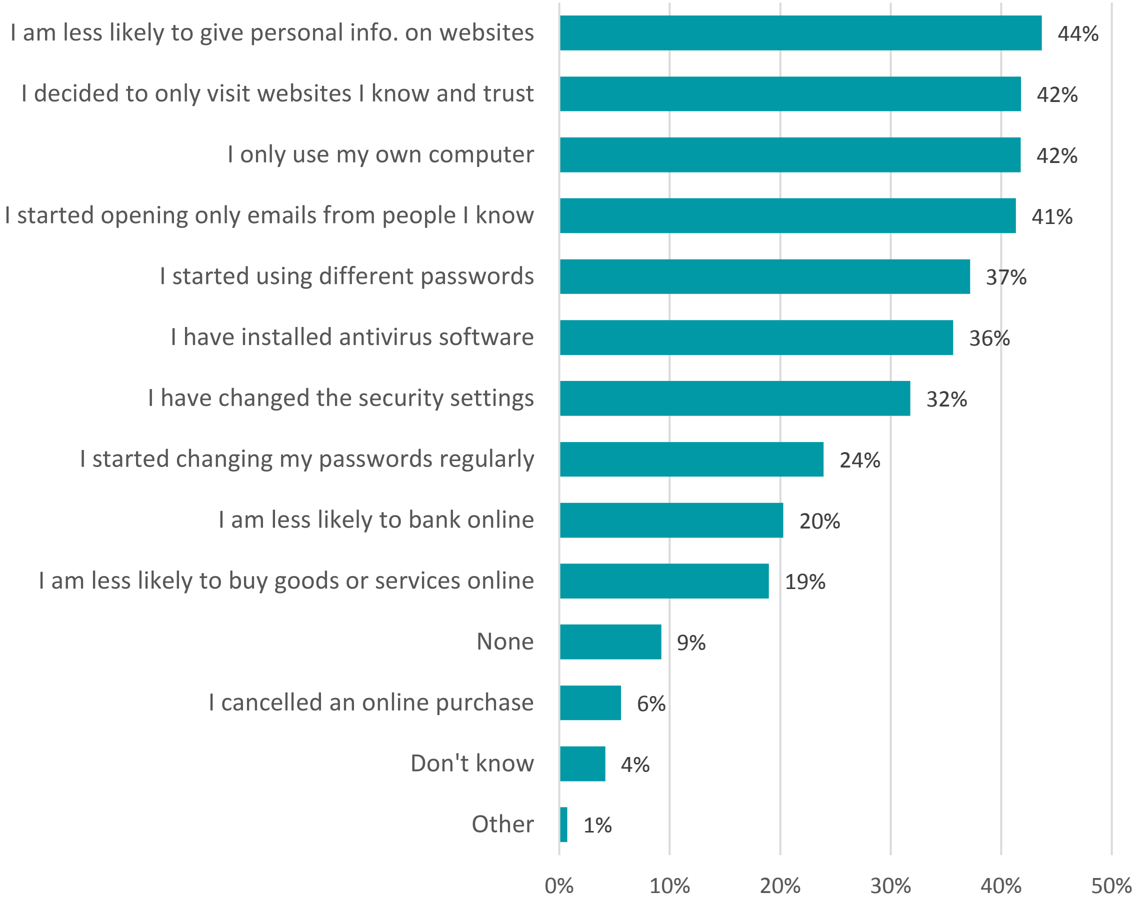
How well informed do you feel about the risks of cybercrime?		REGION				
		South	West	Midwest	Northeast	US Overall
	Very well informed	21.1%	19.6%	16.5%	20.5%	19.7%
	Fairly well informed	49.6%	50.1%	52.4%	52.3%	50.8%
	Not very well informed	22.9%	25.0%	26.2%	21.7%	23.9%
	Not at all informed	3.0%	2.6%	2.5%	2.3%	2.6%
	Don’t know	3.4%	2.8%	2.5%	3.3%	3.0%

Being well-informed about cybercrime is one thing, believing that you are able to protect yourself against cybercrime is another. The survey found that just over two thirds of Americans surveyed appear confident in this regard, totally agreeing or tending to agree with the following assertion: I am able to protect myself sufficiently against cybercrime, for example. by using antivirus software. Conversely, the other third may represent market growth potential for security vendors.

I am able to protect myself sufficiently against cybercrime, e.g. by using antivirus software		REGION				
		South	West	Midwest	Northeast	US
	Totally agree	23.3%	22.9%	19.0%	21.9%	22.0%
	Tend to agree	46.9%	44.0%	46.3%	42.0%	45.1%
	Tend to disagree	17.3%	19.2%	19.9%	20.5%	18.9%
	Totally disagree	3.6%	3.8%	4.6%	4.5%	4.0%
	Don’t Know	8.9%	10.1%	10.2%	11.1%	9.9%

4. CYBERSECURITY AND PRIVACY RESPONSES

Americans have taken a variety of actions in the last three years because of security and privacy issues when using the internet. These range from only using their own computers (42%) to changing passwords (37%). More than a third of those surveyed have installed antivirus software. Slightly less than a third have adjusted their security settings.



Actions taken in last three years because of security and privacy issues when using the internet

Companies that rely heavily on internet transactions should note that a significant percentage of people said that they are less likely to shop or bank online due to security and privacy concerns (19% and 20% respectively). These percentages surely represent lost opportunities for retailers and financial firms. Marketing to this demographic with messaging that emphasizes how seriously your organization takes privacy and security might be productive.

Marketers should also note that 44% of Americans surveyed said that they chose to give out less personal information on websites in response to security and privacy concerns. This suggests that marketing strategies based on data aggregation may be facing more headwind if cybersecurity does not improve. Conversely, these statistics might prove useful to Chief Information Security Officers (CISOs) and Chief Privacy Officers (CPOs) as they argue the case for greater emphasis on cybersecurity within their organizations.

As means of assessing respondents' security priorities, the ESET Cybersecurity Barometer asked: Have you changed your password to access your account(s) for any of the following online services during the last 12 months? Seven categories of accounts were presented and as you can see in the table below, email accounts were the primary concern (this assumes that a password change reflects security concern or prioritization). Note that the South reported the highest password change rates for the top three categories: email, social networks, and shopping websites.

	South	West	Midwest	Northeast	US Overall
E-mail	65.1%	61.0%	63.2%	60.9%	62.9%
Online social networks	48.8%	40.7%	42.7%	42.8%	44.5%
Shopping websites	45.6%	44.9%	40.0%	39.5%	43.1%
Online banking	50.1%	53.4%	50.5%	49.4%	50.8%
Online games	16.0%	13.3%	16.3%	15.8%	15.4%
Public services websites	13.6%	14.6%	12.0%	13.9%	13.5%
Other	0.8%	1.6%	1.7%	1.4%	1.3%
None	14.7%	14.9%	15.6%	15.6%	15.1%

One closely-related question was not asked in this survey: on which of your accounts are you using two-factor authentication, sometimes referred to as 2FA? The market penetration of this technology would be interesting to see; for example, are people resisting 2FA because they find it too cumbersome, or are they embracing it because of security and privacy concerns fueled by the relentless rise of cybercrime?

The lack of a 2FA question comes from the history of the original Barometer question set which was developed before 2FA was widely deployed for online activity. This highlights a dilemma for digital security researchers – how to create consistent longitudinal studies of a topic that is always evolving, sometimes very quickly?

The next EU Barometer on Cybersecurity may answer that question, and the next ESET Barometer for the US will definitely explore some additional topics, such as the use of 2FA.

5. DISCUSSION

Cybersecurity is concerned with the protection of digital technologies – technologies upon which we are now heavily dependent – against criminals and other entities who seek to abuse those technologies for their own selfish ends. Public support for efforts to reduce cybercrime is critical to society's efforts to preserve the benefits of digital technologies. That is why it is so important to know what the public thinks about cybercrime and cybersecurity, the safety of online activities, and the privacy of personal data shared with companies or government agencies.

In the EU, the value of knowing what the public thinks about challenges to prosperity and security led to an ongoing series of surveys conducted to gauge public sentiment and better understand the wants and needs of EU citizens. Known as the Barometer series, this included the EU Barometer for Cybersecurity. The data from that project has not only helped to inform policy decisions about cybersecurity and data privacy in EU countries, it also provided valuable input for commercial marketing projects. In addition, academic researchers have used the data to analyze the relationship between cybercrime experience and online technology adoption.

Unfortunately, the US and Canadian governments apparently do not feel that it is their responsibility to undertake similar surveys of their citizens. Indeed, multiple administrations in both the US and Canada seem content to let companies be the default source of data about the cybercrime problem, but there are several problems with that approach.

Anyone in government who is faced with requests for additional resources to fight cybercrime may reasonably ask: what is the size of the problem you are trying to solve? If your answer is based on the results of a survey that was carried out by a company that sells security-related products and services, your argument is open to accusations of bias – "they just want to increase their sales" – as well as criticisms of the survey's methodology if it is not up to par.

The same weakness can affect the private sector as well. Any CEO who does not want to believe that the public perceives cybercrime to be a serious threat may choose to discount commercially-sponsored research. One motive for wanting to ignore growing evidence of a looming cybercrime crisis might be reluctance to increase the cost of a hardware or software product to make it more secure.

Despite almost universal endorsement, the concepts of security by design and privacy by design have not yet been fully embraced. We still see numerous companies failing to adequately test products in pre-production, or simply decide to accept cyber-risks rather than spend the money to reduce them. Sadly, too many hardware and software products are still shipping with hard-to-patch vulnerabilities that can be exploited by bad actors and thus contribute to cybercrime.

Being able to answer accusations of bias is why the ESET Cybersecurity Barometer was fielded with the same set of questions as the EU research. Furthermore, the survey was conducted by a reputable survey firm using accepted methodology. ESET believes the results are solid and suitable to be used by policy makers working on the cybercrime problem without fear of challenge.

With that in mind, it is possible for ESET to state with confidence that in 2018, a significant majority of Americans thought the following when it comes to cybercrime and cybersecurity:

- Cybercrime is an important challenge to their country's security, more so than drug trafficking, money laundering, and other serious crimes
- The risk of becoming a victim of cybercrime is increasing
- The privacy of personal information supplied online is at risk

Those data points help make the case that urgent action to reduce cybercrime is in the interests of the government and the private sector, as do the following:

- Three quarters of Americans are concerned that their online personal information is not kept secure by public authorities
- Security and privacy concerns have made one in five Americans less likely to bank online or buy goods or services online

It is reasonable to conclude that the findings of the ESET Cybersecurity Barometer strongly suggest that – unless cybersecurity initiatives and cybercrime deterrence are made a top priority of government agencies and corporations – the rate at which systems and data are abused will continue to rise, further undermining the public's trust in technology, trust that is vital to America's economic wellbeing, now and in the future.

Author: Stephen Cobb, CISSP
Senior Security Researcher

ABOUT ESET

For 30 years, ESET® has been developing industry-leading security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving digital security company. Backed by R&D centers worldwide, ESET was the first digital security company to earn 100 Virus Bulletin VB100 awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on LinkedIn, Facebook and Twitter. For more ESET research, security advice, and expert opinion, visit WeLiveSecurity.