



POLLING MEMO: NATIONAL SURVEY ON CYBERSECURITY, TRUST, AND TECH POLICY.

SURVEY SHOWS AMERICANS TRUST U.S. COMPANIES MOST — AND DEVICE MANUFACTURERS IN PARTICULAR — TO CLOSE THE TECHNOLOGY TRUST GAP AND WANT GOVERNMENT TO SUPPORT TECH INNOVATION AND GLOBAL COMPETITIVENESS WITHOUT ADDITIONAL MANDATES AND REGULATION.

→ Trusted Future and the National Security Institute surveyed nearly 3,200 respondents, assessing technology usage habits, views on cybersecurity and privacy, and priorities for tech policy, investment, and regulation.

KEY FINDINGS OF THE SURVEY INCLUDE:

- 1** There is a significant technology trust gap among Americans, with most believing that we ought to have a higher level of security for online data than we have today.
 - Consumers trust U.S. companies—and U.S. device manufacturers the most—to protect their data and to help close the technology trust gap.
- 2** The vast majority of respondents own smartphones and use them as their primary access point to the Internet.
 - Consistent with the use of smartphones as the primary access point to the Internet, new cyber attack vectors specifically targeting these devices are emerging, as two-thirds of respondents reported receiving an attempted cyber intrusion via text message.
- 3** A majority of respondents favor U.S. government support and investment in American technology leadership, and want Congress to avoid mandates or aggressive regulation of tech companies that would harm our global competitiveness.

BY A LARGE MARGIN, AMERICANS BELIEVE THERE IS A TECHNOLOGY TRUST GAP, WITH 63% OF RESPONDENTS INDICATING THAT WE OUGHT TO HAVE MORE SECURITY FOR ONLINE DATA THAN WE DO TODAY.

Nearly two-thirds of Americans believe there is a gap between the level of confidence we should have in the security of our personal data online compared to the level we actually have, with just 15% disagreeing. Large majorities of Americans are concerned about various types of security threats to their personal data, with nearly 7 in 10 Americans indicating concern about malware, trojans, phishing or smishing attacks, spyware, viruses, or third-party data breaches. And nearly half of respondents indicated that they were more concerned about protecting their sensitive personal data on a smartphone over a laptop or desktop computer.

Do you believe America faces a technology trust gap — a gap between the level of confidence we should have in the protection of our personal data online versus the level we actually have?

YES	NO	DON'T KNOW
63%	15%	22%

For each of the following cybersecurity threats, could you indicate your level of concern:



Nearly 7 in 10 Americans registered concern about multiple groups of cyber threats.

	TOTAL CONCERNED	TOTAL NOT CONCERNED	DON'T KNOW
Data Breaches	79%	18%	3%
Malware	75%	20%	5%
Spyware	75%	21%	4%
Trojans	73%	23%	4%
Computer Viruses	73%	23%	4%
Other	70%	24%	6%
Ransomware	66%	29%	5%
Phishing/Smishing	65%	32%	3%

Given the types of sensitive information you use with your devices, are you more concerned with protecting personal data on a smartphone than on a laptop or desktop computer?

YES	NO	DON'T KNOW
47%	38%	15%

CONSUMERS TRUST AMERICAN COMPANIES SIGNIFICANTLY MORE THAN FOREIGN COMPANIES ACROSS THE BOARD—AND TRUST U.S. DEVICE MANUFACTURERS THE MOST—TO SECURE THEIR PERSONAL DATA.

Respondents registered a strong preference for American technology companies over their foreign counterparts and foreign governments on whom to trust to protect their personal data. American device manufacturers were the most trusted entity, with 48.7% of respondents indicating they either completely or mostly trusted them with 17.5% saying they completely or mostly did not trust them, for a net trust rating of +31%. Foreign governments rated the lowest of any option, with a -47% rating. While the public distrusted all foreign entities across the board, foreign device manufacturers had a -33% net trust rating.

To what extent do you currently trust each of the following organizations to protect your personal data?

	NET TRUST RATING	TOTAL TRUST	TOTAL DISTRUST	NEITHER
U.S. Device Makers	31%	49%	18%	33%
U.S. App/Software Devs	12%	34%	21%	45%
U.S. Government	5%	35%	30%	35%
U.S. Social Media Cos.	-22%	23%	45%	32%
Foreign Device Makers	-33%	14%	47%	39%
Foreign App/Software Devs	-41%	13%	53%	34%
Foreign Social Media Cos.	-44%	13%	57%	30%
Foreign Governments	-47%	11%	58%	31%

Which one of the following would you trust most to increase the protection of your personal data?










1% Foreign digital device makers	1% Foreign governments	1% Foreign app and software developers	2% Foreign social media companies	5% American social media companies	8% American app and software developers	17% The U.S. government	31% American digital device makers
--------------------------------------------	----------------------------------	--------------------------------------------------	---------------------------------------------	----------------------------------------------	---------------------------------------------------	-----------------------------------	----------------------------------------------



CONSUMERS OFTEN TAKE ADVANTAGE OF BUILT-IN SECURITY FEATURES TO HELP THEM PROTECT THEIR PERSONAL DATA.

Respondents indicated that they keep their data safe in a range of ways. Large numbers of respondents indicated that they regularly avoided certain risky activities on their own, such as avoiding suspicious links in emails or texts (77%) and using sensitive apps on public Wi-Fi (61%). Many of the affirmative actions to protect personal data that scored highly among respondents are often built into or prompted on devices or operating systems, such as downloading apps from trusted sources (official app stores 61%; well-known companies 58%), updating the operating system (59%), using strong or complex passwords (58%), and updating software and apps (56%). Actions that relied mostly on the users themselves were not regularly used by the majority of respondents, such as checking device settings for security and privacy (40%) or checking app settings for security and privacy (38%).

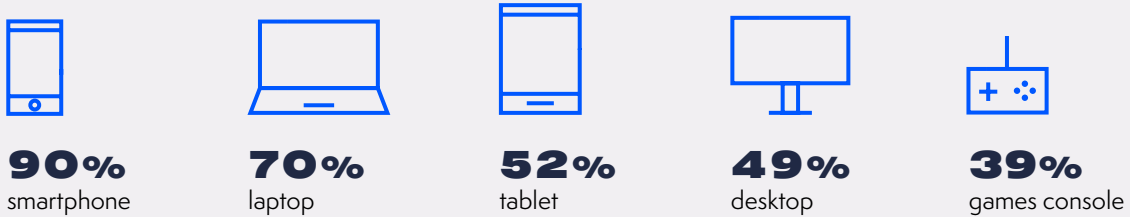
■ When online, how often do you do the following things to keep your data safe?

	REGULARLY	OCCASIONALLY	FOR SPECIFIC PURPOSES ONLY	RARELY/ NEVER	DON'T KNOW/ NOT SURE
 Avoid suspicious links sent via email or text	77%	12%	5%	3%	3%
 Avoid using sensitive apps (banking, etc.) when on public WiFi	61%	17%	9%	8%	5%
 Only download apps from official app stores	61%	17%	11%	6%	5%
 Update the operating system or device software (e.g., iOS/Android/MacOS/Windows)	59%	21%	8%	7%	5%
 Use strong or complex passwords	58%	24%	10%	4%	4%
 Only download apps from well-known software or device companies	58%	19%	12%	6%	5%
 Update your software or apps	56%	26%	9%	5%	4%
 Check device settings for security and privacy	40%	33%	13%	10%	4%
 Check app settings for security and privacy	38%	31%	14%	12%	5%

SMARTPHONES ARE BECOMING INCREASINGLY ESSENTIAL TO ALMOST EVERYTHING WE DO.

Considerably more respondents indicated that they owned a smartphone (90%), than any other device option, with laptop the next highest at 70%. Smartphones are increasingly the gateway to the Internet, with nearly twice as many using smartphones as their primary online access point (45%), then the next closest choice (laptops at 25%). And people are using them a lot, with nearly 75% of respondents using their smartphones for more than three hours a day. Smartphones are so essential to some that 21% said that they would prefer to have a root canal rather give up their smartphone for a week.

Which of the following online devices do you currently own or have regular access to?



Of the devices you own, which one do you tend to use most often to go online?



Across all devices, how much time do you estimate that you tend to spend using your digital devices on an average day?



■ Which would you rather do, go to the dentist for a root canal or give up your smartphone for a week?

Smartphones have become so essential that 21% of respondents said they would rather get a root canal than give up their smartphones for just a week.



ROOT CANAL

VS



1 WEEK

■ Thinking back over the COVID-19 pandemic, which of the following statements best describe the amount of time you tend to spend using your mobile devices now, compared with before the pandemic?



Cybercriminals go where the users are, and with increasing smartphone usage, new forms of attacks are on the rise: two-thirds of respondents report receiving illegitimate texts in the last year that were likely intended to trick them into giving up private information or installing malware. This form of cyber attack vector, called smishing (the SMS/text version of phishing) is growing in significance along with the ubiquity of smartphones and the sensitive information that they contain.

■ Within the last year, have you personally gotten a text message from either an unknown sender or an illegitimate one claiming to be legitimate and asking you to click on a link?



A smishing attack is the SMS/text version of a phishing email attack.

STRONG MAJORITIES FAVOR U.S. GOVERNMENT POLICY THAT SUPPORTS AMERICAN LEADERSHIP ON TECHNOLOGY WITH BIPARTISAN INVESTMENT IN INNOVATION, WHILE ONLY AROUND A THIRD WANT NEW REGULATIONS OR GOVERNMENT MANDATES ON TECHNOLOGY COMPANIES.

The priorities of the American people were clear: they value American technological leadership, with nearly 7 in 10 Americans (68%) viewing U.S. technological leadership as necessary to make the United States a home for the good paying jobs and industries of the future, and with 6 in 10 concerned that China may dislodge American technological leadership and the pathway to those jobs.

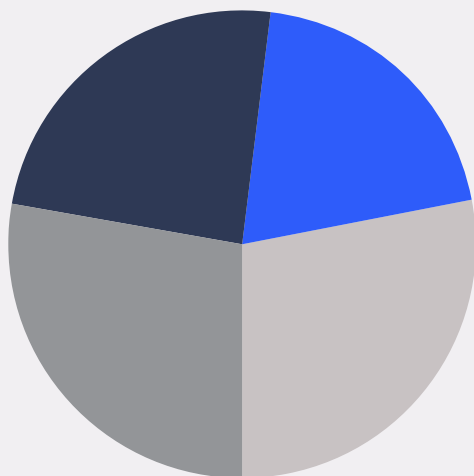
Nearly the same 6 in 10 urge the United States to lead an Atlantic alliance with our European partners for a strong and united tech policy to counter China (59%), want Congress to promote U.S. technology leadership with bipartisan investment in research and innovation to stay on the cutting edge and to better compete with China (59%), and expect the U.S. government to fight for a level playing field, including global standards that apply equally to American companies and our foreign competitors, like Chinese companies (60%).

And nearly two-thirds (64%) believe that Congress has a key role in promoting U.S. technology leadership to ensure we maintain our lead as home to the world's most innovative companies.

Equally clear is what the American people do not want: more than half of Americans want Congress to avoid degrading U.S. technology leadership or hamstringing our ability to build cutting edge technologies (55%), while only around a third of respondents want government security mandates (28%) or aggressive regulation of technology companies (37%).

And nearly half of Americans (44%) want the government to avoid managing the security practices of private sector companies when it comes to protecting individual privacy and security and instead focus on security incentives or permitting private sector companies to set their own security practices.

In order to better to protect individual privacy and security, do you think it is more effective to:



24%

Have the government incentivize the security practices of private sector companies.

20%

Allow private sector companies to set their own security practices with no government involvement.

28%

Have the government mandate the security practices of private sector companies by law or regulation.

28%

Don't know/not sure.

Thinking about the global competitiveness of the United States, to what extent do you agree or disagree with each of the following statements when it comes to technology?

	AGREE	DISAGREE	Neither Agree nor Disagree
We need US technology leadership so that America maintains its current position as a global leader and so that America becomes home to the good paying jobs and industries of the future.	68%	5%	27%
Congress should promote US technology leadership, ensure we maintain our lead as home to the worlds' most innovative companies, and help advance American technology leadership.	64%	5%	31%
China is seeking to dislodge American technology leadership, and wants to become the world's leading innovator, so that Chinese companies control the jobs and industries of the future.	60%	8%	32%
Bipartisan investment in emerging technologies, research, and innovation can help us stay on the cutting edge in order to better compete with China.	60%	5%	35%
For US companies to compete on a level playing field around the globe, they need the US government to fight for global standards that apply equally to American companies and our foreign competitors, like China and its companies.	60%	7%	33%
It is critical that America lead and alliance with European partners to ensure we have a more uniform approach to technology policy and protect innovation in order to effectively counter China.	59%	5%	36%
Congress should avoid degrading US technology leadership, or hamstringing our ability to build cutting edge technologies, because that could allow Chinese companies to gain global pre-eminence.	56%	8%	36%
US technology companies have become too successful and powerful and, as a result, Congress needs to aggressively regulate these companies even if that means making America less competitive with China globally.	37%	23%	40%



trustedfuture.org



nationalsecurity.gmu.edu