National Privacy Test Report

National Privacy Test
Powered by NordVPN

Results of the National Privacy Test Wrapped Up

National Privacy Test (NPT) is a digital security campaign that promotes cyber security and privacy among Internet users around the world. We seek to educate general public about cyber threats and the importance of data and information security in the digital age. The objective of this research is to determine the global level of awareness about online security and privacy as well as to provide practical advice.

The NPT research started on March 23, 2017, via an online survey of adult Facebook users, mainly targeting English-speaking population from the United States, the United Kingdom, Canada and Australia. At the end of the first stage, 4,636 respondents have completed the survey, with an average score of 48%. More detailed results and preliminary insights are provided on this report page.

Knowledge Questions Overview

In this section, questions were designed to test the level of knowledge Internet users possess about online privacy and security. The questions cover various topics, such as metadata collection, both public and home Wi-Fi security, and privacy threats caused by information sharing on social networks. Also, respondents were asked if they are able to recognize secure and unsecure websites based on URLs given. Answers to these knowledge questions allow drawing insights about how well Internet users are informed on security and privacy topics and whether the awareness differs among countries.

Internet Protocol Security

URL with both 'https' and 'www' is considered secure by twice as many users as one without 'www'.

NPT Score 35%

Security on Public Hotspots

Checking a bank account on public Wi-Fi seen as risky but shopping online assumed to be safer.

NPT Score 68%

Password Strength

The vast majority of respondents in all countries are aware of what makes a strong password.

NPT Score 92%

Wi-Fi Security

Almost 2/3 knew that a Wi-Fi password should be strong but were unsure about more advanced options.

NPT Score 24%

Social Network Oversharing

Social media users know the basic threats of oversharing but struggle with the less obvious ones.

NPT Score 66%

Data Collected by Web Browsers

Users know the basic data that browsers collect but not the full scope of collection.

NPT Score 51%

ISP Metadata Collection

Australians know most about ISP metadata collection, likely because of their data retention law.

NPT Score 38%

Internet of Things (IoT) Privacy Issues

Most users know that IoT lacks encryption, but 23% are not familiar with IoT privacy threats.

NPT Score 40%

Behavior Questions Overview

The aim of the behavioral questions section is to check how Internet users react to common situations happening online, as well as how they manage their personal accounts and devices in terms of security. For example, with more and more services implementing 2-factor authentication as a security measure to prevent user accounts from being hijacked, we want to know how people are adopting this feature in practice. The questions in this section also cover antivirus usage, the way Internet users handle scam emails or if there are any signs of being overly paranoid about privacy.

Phishing scams

Almost all users would ignore an email request from their bank to provide personal information.

NPT Score 93%

Browser autofill forms

Most users across all countries would not allow their browsers to save sensitive information.

NPT Score 93%

Confirmation emails

Only about 50% of users realized that an order confirmation email does not pose a threat.

NPT Score 52%

Antivirus usage

Most users allow their antivirus software to update automatically, which is good for security.

NPT Score 81%

2-Factor Authentication

Mixed results: more than 50% use 2FA but over one third don't know what it means.

NPT Score 43%

Product Questions Overview

The section of product questions is focused on several categories of digital products – messaging apps, cloud storage and email providers. The questions in this short section are aimed to help to find out whether Internet users know which service providers are recommended by various security experts as the most privacy-focused. The questions were designed to feature both the most popular brands and those less mainstream but highly oriented to personal data security and privacy.

Email providers

Gmail, which scans messages for ad targeting, considered the most privacy-focused provider by 37%.

NPT Score 7%

Secure messaging

Over one third were not sure which messaging app was considered the most secure and private.

NPT Score 11%

Cloud storage

Most users trust big brand names, while more privacy-focused services are less known.

NPT Score 5%

Key Takeaways

One of the main goals of this project was to find out the extent of general awareness about online privacy and security. We had a hypothesis that an average Internet user is somewhat familiar with the major threats that are featured in media frequently, but may struggle with specific actions and tools required to avoid them. The test results have largely confirmed this theory but also provided more specific insights into user assumptions and behavior.

Users are aware of basic security issues

The vast majority of those who took the test (92%) can identify a truly strong password and 95% can spot a suspicious email posing as a request from their bank.

Only main types of collected private data are well known

Most of the respondents were able to correctly identify at least the main types of private data collected by Internet service providers and web browsers. As expected, users know that their browsing habits, locations and IP addresses are tracked. However, less than 25% knew that browser tracking goes as far as collecting data about font preferences and screen resolutions.

Users hold contradictory beliefs about actions on public Wi-Fi

While checking a bank account on a public hotspot is assumed to be very risky (less than 2% agree that is safe), entering banking credentials to make a purchase online is seen as a lesser risk (23% think it is safe). This points to a lack of understanding of just how vulnerable users can be on public networks, where the level of security is unknown and anyone with basic hacking skills can access sensitive data of everyone connected.

Unexpectedly, Gmail is perceived as privacy-focused

Although most of the respondents struggled to decide which email providers are privacy-focused, 37% chose Gmail––likely because of its brand strength and overwhelming popularity. What makes this result rather unexpected is the fact that private Gmail messages are scanned by Google and then used to improve custom ad targeting.

Information overload is confusing to Internet users

Only slightly over 50% of the respondents realized that an email confirming a genuine online purchase does not pose a security threat. The outcome shows that the topics of online privacy and security can be very confusing for an average Internet user. If they are surrounded with information on various threats for long enough, every little thing starts looking like another phishing attempt.

Demographic Overview

Who answered our questions?

NPT distributed a self-selected online survey on Facebook, mainly targeting English-speaking users from the United States, the United Kingdom, Canada and Australia. At the end of the first stage, 4,636 respondents have completed the survey, with an average score of 48%.

Main Countries

32%	23%	23%	22%
United States	United Kingdom	Canada	Australia

The survey was taken by similar numbers of respondents from the main four countries.

Respondents' Gender

43%	26%	29%	2%
Male	Female	Other / I'd rather not tell	Unknown

Almost half of the survey takers were male, while around a quarter chose to not disclose their gender.

Respondents' Age

17%	8%	4%	3%	7%
13-17	18-25	26-35	36-45	46-55
14%	21%	24%	2%	
56-65	66+	Other / I'd rather not tell	Unknown	

Around a quarter of respondents preferred to keep their age unknown.

Score by country

The test was targeted mainly to English-speaking Internet users from Australia, Canada, the United Kingdom and the United States. If comparing the results among countries, Australia takes the lead with the overall score of 52%. It is a slightly higher result than the average of the whole sample (48%). Australians demonstrating better knowledge regarding online security and privacy might be related to the country's recent controversial metadata retention law, which requires telecommunications companies to collect and store customers data for at least two years.

Nevertheless, there is no significant difference between the scores of these four countries. As the average results only reach around 50%, it is clear that increasing awareness of online security and privacy is relevant to Internet users, irrespective of the country they come from.

Average score

Average score	Country
50%	United States 1502 respondents
49%	United Kingdom 1074 respondents
47%	Canada 1074 respondents
52%	Australia 1063 respondents