



PUBLIC POLL FINDINGS AND METHODOLOGY

Nearly 1 in 3 Americans report being a victim of online financial fraud or cybercrime

New Ipsos poll, on behalf of Wells Fargo, finds about half guess they could be a victim of online fraud in the future, yet most feel confident about the steps they're taking to avoid that

Topline Findings

Washington, D.C., December 1, 2023 – A new Ipsos poll, conducted on behalf of Wells Fargo, finds that while many Americans are confident that they have taken enough steps to prevent being the victim of financial cybercrime in the future, nearly one in three say they have already personally been the victim of online financial fraud or cybercrime. Americans who report being victims of online financial fraud or cybercrime are most likely to say they were a victim of credit card fraud. Among all Americans, nearly half say it is at least somewhat likely they could be a victim of online financial fraud in the future. At the same time, about three in four say they store personal account information with at least one online retailer.

Detailed Findings

1. Nearly 1 in 3 Americans (31%) report being a victim of online financial fraud or cybercrime.
 - Americans ages 35-54 (36%) and 55+ (34%) are more likely to report that they have been a victim of financial cybercrime compared to those ages 18-34 (22%).
2. Among online financial cybercrime or fraud victims, about two-thirds (64%) report they were a victim of credit card fraud.
 - Credit card fraud is the most common type of online financial fraud, distantly followed by data breach (32%), account hacking (31%), online banking fraud or scam (23%), and phishing (14%).
3. Victims of cyberfraud are most likely to react by changing their passwords (93%) or contacting their financial provider (85%).
 - However, fewer victims took the additional actions of placing a fraud alert on their credit report (61%), contacting the credit bureaus (44%), reporting fraud to law enforcement (34%), or scanning their information on the dark web (26%).
4. While most are confident in the steps they have taken to prevent cyberfraud, almost half of American adults (48%) continue to feel it is likely they will become a victim of financial cybercrime in the future.
 - Overall, 73% are confident that they have taken enough steps to prevent them from being the victim of financial cybercrime or online financial fraud.
 - Still, nearly half of Americans (48%) say it is at least somewhat likely they could become a victim of financial cybercrime or online banking fraud in the future.





PUBLIC POLL FINDINGS AND METHODOLOGY

- Women are more likely than men to say they are likely become a victim of financial cybercrime or online banking fraud in the future (53% vs. 45%, respectively). Americans ages 55+ are also more likely than those ages 18-34 to say they are likely to become a victim of financial cybercrime or online banking fraud in the future (54% vs. 40%, respectively).
 - At the same time, about three in ten (28%) acknowledge that they don't have strong enough passwords on their online financial accounts.
5. Many are engaging in a potentially risky behavior with online retailers: storing personal account information. A bare majority (51%) agree that the convenience of saving their account information with an online retailer during checkout outweighs the risk of exposing their information to a data breach.
- A significant majority (76%) say they have their account information saved with retailers. Half say 5 or fewer retailers know their account information, 12% say their information is on hand for 6-10 retailers, and 14% say either more than 10 or they have lost count. Just 24% say they have not stored any account information with a retailer.
6. One in four Americans (25%) only review their financial statements for suspicious activity every few months, or a few times a year.

These are the findings of an Ipsos poll conducted between September 15-18, 2023, on behalf of Wells Fargo. For this survey, a sample of 1,005 adults age 18+ from the continental U.S., Alaska, and Hawaii was interviewed online in English. This sample includes 319 individuals who say they have experienced financial cybercrime or online financial fraud, and it includes 686 individuals who say they have not experienced financial cybercrime or online financial fraud.

The poll has a credibility interval of plus or minus 3.8 percentage points for all respondents. The poll has a credibility interval of plus or minus 6.7 percentage points for individuals who report having experienced financial cybercrime or online financial fraud. The poll has a credibility interval of plus or minus 4.6 percentage points for individuals who report not having experienced financial cybercrime or financial fraud.

For full results, please refer to the following annotated questionnaire:

NOTE: All results show percentages among all respondents, unless otherwise labeled. Reduced bases are unweighted values.

*NOTE: * = less than 0.5%, - = no respondents, NA = not applicable*





PUBLIC POLL FINDINGS AND METHODOLOGY

Full Annotated Questionnaire

Q1. Have you ever been a victim of financial cybercrime or online financial fraud? Examples of financial cybercrime include online banking fraud, credit card fraud, account hacking, data breach, and phishing.

	Total
Base: All Respondents	1005
Yes	31%
No	69%

Q2. **[ASK IF Q1=YES]** Which type of online financial cybercrime or fraud were you a victim of? Select all that apply.

	Total
Base: All Answering	319
Credit card fraud	64%
Data breach	32%
Account hacking	31%
Online banking fraud or scam	23%
Phishing	14%
Other	2%

Q3. **[ASK IF Q1=YES]** As a victim of financial cybercrime or fraud, which, if any, of the following actions did you take to limit additional exposure to fraud?

	Changed my passwords	Contacted my bank/financial provider.	Placed a fraud alert on your credit report	Contacted the credit bureaus	Reported fraud to law enforcement	Scanned my information on the dark web
Base	319	319	319	319	319	319
Yes	93%	86%	61%	44%	34%	26%
No	7%	14%	39%	56%	66%	74%

Q4. **[ASK IF Q1=NO]** Do you personally know somebody who has been a victim of financial cybercrime or online financial fraud?

	Total
Base: All Respondents	686
Yes	29%
No	71%





PUBLIC POLL FINDINGS AND METHODOLOGY

Q5. [ASK IF Q1=NO] If you were to become a victim of financial fraud, how likely would you be to take the following actions?

	Contact my bank/financial provider	Change my passwords	Place a fraud alert on your credit report	Report fraud to law enforcement	Contact the credit bureaus	Scan my information on the dark web
Base	686	686	686	686	686	686
Very likely	83%	83%	69%	62%	59%	23%
Somewhat likely	11%	12%	24%	25%	26%	19%
Not so likely	4%	4%	6%	11%	12%	32%
Not at all likely	2%	1%	2%	3%	3%	27%

Q6. If you had to guess, what is the likelihood that you will become a victim of financial cybercrime or online banking fraud in the future?

	Total
Base: All Respondents	1005
Very likely	8%
Somewhat likely	40%
Not so likely	44%
Not at all likely	8%

Q7. How confident are you that the steps you have taken are enough to prevent you from being the victim of financial cybercrime or online financial fraud in the future?

	Total
Base: All Respondents	1005
Very confident	12%
Somewhat confident	61%
Not so confident	24%
Not at all confident	4%



PUBLIC POLL FINDINGS AND METHODOLOGY

Q8. How much do you agree or disagree with each of the following statements?

	Base	Agree strongly	Agree somewhat	Disagree somewhat	Disagree strongly
I avoid clicking on links or downloading attachments from unknown senders.	1005	72%	20%	6%	2%
Keeping my financial information secure is a priority for me.	1005	64%	32%	3%	1%
I avoid entering sensitive information on public Wi-Fi networks.	1005	57%	32%	10%	1%
I have antivirus software and anti-malware software on my home computer.	1005	50%	33%	13%	5%
I enable multi-factor authentication for online financial accounts whenever possible.	1005	39%	45%	12%	4%
The convenience of saving my account information with an online retailer during checkout outweighs the risk of exposing my information to a data breach.	1005	12%	39%	33%	16%
I don't have strong enough passwords on my online financial accounts.	1005	6%	23%	42%	30%
I often share personal information on social media.	1005	5%	13%	24%	58%

Q9. How often, if at all, do you closely review your financial statements and credit reports for suspicious activity?

	Total
Base: All Respondents	1005
Every day	14%
Every week	28%
Every month	30%
Every 2 to 3 months	9%
Every 4 to 6 months	3%
Once or twice a year	3%
Less often than once a year	1%
Depends – only review when I have a concern.	9%
Never review financial statements	3%



PUBLIC POLL FINDINGS AND METHODOLOGY

Q10. How many retailers have you saved your account information with (i.e., created an account saved with a password)?

	Total
Base: All Respondents	1005
None	24%
5 or less	50%
6-10	12%
More than 10	8%
I've lost count	6%





PUBLIC POLL FINDINGS AND METHODOLOGY

About the Study

These are some of the findings of an Ipsos poll, conducted between September 15 – 18, 2023 on behalf of Wells Fargo. For this survey, a sample of 1,005 adults age 18+ from the continental U.S., Alaska, and Hawaii was interviewed online in English. The sample includes 319 individuals who report experiencing financial cybercrime or online financial fraud and 686 individuals who report not having experienced financial cybercrime or online financial fraud.

The sample was randomly drawn from [Ipsos' online panel](#), partner online panel sources, and ["river" sampling](#) and does not rely on a population frame in the traditional sense. Ipsos uses fixed sample targets, unique to each study, in drawing a sample. After a sample has been obtained from the Ipsos panel, Ipsos calibrates respondent characteristics to be representative of the U.S. Population using standard procedures such as raking-ratio adjustments. The source of these population targets is U.S. Census 2022 American Community Survey data. The sample drawn for this study reflects fixed sample targets on demographics. Posthoc weights were made to the population characteristics on gender, age, race/ethnicity, and region.

Statistical margins of error are not applicable to online non-probability polls. All sample surveys and polls may be subject to other sources of error, including, but not limited to coverage error and measurement error. Where figures do not sum to 100, this is due to the effects of rounding. The precision of Ipsos online polls is measured using a credibility interval. In this case, the poll has a credibility interval of plus or minus 3.8 percentage points for all respondents. Ipsos calculates a design effect (DEFF) for each study based on the variation of the weights, following the formula of Kish (1965). This study had a credibility interval adjusted for design effect of the following (N=1,005, DEFF=1.5, adjusted Confidence Interval=+/- 5.3 percentage points).

The poll also has a credibility interval of plus or minus 6.7 percentage points for individuals who report having experienced financial cybercrime or online financial fraud. The poll has a credibility interval of plus or minus 4.6 percentage points for individuals who report not having experienced financial cybercrime or online fraud.

For more information on this news release, please contact:

Mallory Newall
Vice President, US
Public Affairs
+1 202 374-2613
mallory.newall@ipsos.com





PUBLIC POLL FINDINGS AND METHODOLOGY

About Ipsos

Ipsos is one of the largest market research and polling companies globally, operating in 90 markets and employing over 18,000 people.

Our passionately curious research professionals, analysts and scientists have built unique multi-specialist capabilities that provide true understanding and powerful insights into the actions, opinions and motivations of citizens, consumers, patients, customers or employees. Our 75 solutions are based on primary data from our surveys, social media monitoring, and qualitative or observational techniques.

Our tagline "Game Changers" sums up our ambition to help our 5,000 customers move confidently through a rapidly changing world.

Founded in France in 1975, Ipsos has been listed on the Euronext Paris since July 1, 1999. The company is part of the SBF 120 and Mid-60 indices and is eligible for the Deferred Settlement Service (SRD). ISIN code FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP www.ipsos.com

